USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Smart Spaces, Private Lives: A Culturally Grounded Examination of Privacy Tensions in Smart Homes

Yara Alsiyat, *University of Oxford and King Abdulaziz City for Science and Technology;* Yuanhaur Chang and Ning Zhang, *Washington University in St. Louis;* Ivan Flechais, *University of Oxford*

https://www.usenix.org/conference/soups2025/presentation/alsiyat

This paper is included in the Proceedings of the Twenty-First Symposium on Usable Privacy and Security.

August 11–12, 2025 • Seattle, WA, USA

ISBN 978-1-939133-51-9

Open access to the Proceedings of the Twenty-First Symposium on Usable Privacy and Security is sponsored by USENIX.

Smart Spaces, Private Lives: A Culturally Grounded Examination of Privacy Tensions in Smart Homes

Yara Alsiyat[1,2], Yuanhaur Chang[3], Ning Zhang[3], Ivan Flechais[1]
[1] *University of Oxford, Oxford, UK*
[2] *King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia*
[3] *Washington University in St. Louis, Missouri, USA*

Abstract

Smart home technologies offer convenience and security, but also raise privacy challenges shaped by cultural norms and household dynamics. We conducted an iterative Grounded Theory study using semi-structured interviews to examine how privacy is understood and managed in smart homes. Our initial data collection included participants from both the U.S. and Saudi Arabia, which highlighted a range of privacy tensions influenced by cultural expectations. Based on these insights, we focused subsequent data collection on Saudi households to explore how privacy concerns are navigated in specific religious and social contexts. Our findings show that privacy in Saudi homes is collectively negotiated and shaped by factors such as family hierarchies, interpersonal roles, and cultural obligations. Cameras, in particular, are perceived not merely as tools, but also as socially present entities, leading to behavioral adaptations and negotiated device usage. These insights underscore the importance of designing culturally responsive smart home technologies that align with local norms while supporting privacy and usability. By situating privacy within everyday household practice, this study contributes to broader discussions on culturally embedded design and privacy-aware innovation for smart homes.

1 Introduction

The widespread adoption of smart home technologies has raised critical questions about their impact on privacy and family dynamics, particularly in culturally diverse settings [22,58]. Although these technologies promise to improve convenience, security, and energy efficiency, their poorly aligned designs can exacerbate tensions by conflicting with deeply held cultural norms [36,42]. Understanding how these technologies are perceived and integrated in different cultural contexts is essential to address fundamental issues such as privacy protection, responsible innovation, and ethical technology design.

Recent research highlights the complex interactions between smart home devices and their users, particularly when cyberspace and physical spaces converge [3,11,32,62,79,81]. Studies have examined privacy tensions between different entities, such as homeowners and nannies [24], device owners and bystanders [11, 18, 32, 62, 89], or Airbnb hosts and guests [61]. While some studies have explored these conflicts within family settings [13,20,26,43,52,56,63], family structures and values vary significantly across cultures, and more research is needed to understand diverse cultural perspectives. For example, Saudi families [12,34] who use smart devices commonly need to accommodate the privacy concerns of their female guests [23]. In contrast, such concerns are much less widespread in Western cultures [11]. While there is growing work examining privacy in Muslim-majority and non-Western contexts, such as online visibility and honor in Muslim-American communities [2], gendered device access in Pakistan [54], and domestic surveillance in Jordanian homes [10], the everyday negotiation of smart home privacy within culturally conservative households remains underexplored. Additionally, survey studies across Middle East and North Africa (MENA) countries highlight significant variation in privacy norms tied to religion, gender, and regulation [40], reinforcing the need for localized research. Despite substantial research into privacy in Western settings, limited attention has been given to how cultural norms shape privacy practices in non-Western contexts, such as Saudi Arabia.

To explore this gap, our overarching research question is: *To what extent do cultural perspectives shape device usage, privacy perceptions, and conflict resolution in smart homes?*

To address our research question, we used an iterative Constructivist Grounded Theory (GT) study [28,30,31,46,47]. We began with semi-structured interviews [33] with 40 par-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

ticipants from Saudi Arabia and the United States to identify broad cultural influences on smart home adoption and privacy practices. Based on early insights, we refined our focus and conducted additional interviews with 15 Saudi households. This deeper engagement provided a detailed understanding of how privacy tensions are experienced and negotiated in Saudi homes, where family hierarchies, social customs, and religious expectations intersect with technological use.

Our findings reveal that privacy in Saudi homes is not treated as an individual boundary but is collectively negotiated with smart devices. For example, cameras are often perceived as having a social presence similar to that of a non-mahram (male stranger), profoundly influencing interactions and privacy dynamics. These perceptions highlight the importance of culturally sensitive designs that respect religious and social values while maintaining the benefits of modern technologies. Saudi families adopt various strategies to balance privacy protection with technological convenience.

This study presents an iterative investigation that begins with broad cultural patterns and develops a grounded theory rooted in Saudi households. We offer a culturally grounded perspective on privacy tensions by treating culture not as background, but as the lens through which privacy is understood and enacted. Our findings highlight how social norms, religious values, and household dynamics shape not only privacy perceptions but also how devices are used, shared, or resisted. The resulting theory—Culturally Negotiated Privacy Management in Saudi Smart Homes—demonstrates how privacy emerges from negotiation between cultural values, interpersonal roles, and technology design. These insights inform the design of smart home technologies that are culturally respectful, inclusive, and usable.

2 Background and Related Work

2.1 Definitions

We define several key terms and concepts we use in this paper:

Smart Home. According to the definition by Alam et al. [8] and Madakam et al. [60], smart homes are cutting-edge living environments that seamlessly integrate multiple systems to offer automated services, bolstered security, and an elevated quality of life for residents. These homes utilize various advanced technologies for convenient remote management and oversight of household appliances and systems.

Smart Devices. Smart devices are household appliances that has the ability to connect to networks [49], commonly describing components of the Internet of Things (IoT) [77]. The distinguishing characteristics of these devices are their proficiency in perceiving environment, functioning autonomously, and establishing connections with other devices.

Sharing Dynamics. According to Alghamdi et al. [15], sharing smart home devices within households or with guests involves a complex interplay of benefits, privacy concerns, and user dynamics over the use and control of these devices.

Privacy Perception. This refers to an individual's subjective comprehension of privacy within a specific setting, including sentiments of trust, security, and autonomy about personal data [78]. In contrast to privacy behavior, which includes activities aimed at protecting privacy (such as deactivating devices) [25], privacy perception is shaped by cultural norms, understanding of technology, and prior experiences.

Privacy Tension. This involves the challenges and compromises that emerge when diverse privacy requirements, cultural norms, or technology objectives intersect within the same context [70]. In smart homes, this concept refers to scenarios when privacy expectations conflict, such as balancing security benefits with cultural norms of modesty or addressing varying privacy perspectives among residents and visitors [91].

Mahram and Non-Mahram. In Islamic and Saudi Arabian culture, the term mahram has a strong foundation in religious teachings and cultural practices. It describes a male with whom marriage would be considered permanently unlawful, such as a father, brother, or son [1]. The idea of mahram and non-mahram is deeply rooted in Islamic laws and societal norms related to gender interactions and permissible relationships, such as requiring women's body parts to be covered in the presence of non-mahram men [86].

2.2 Privacy Tension in Smart Shared Spaces

A distinctive challenge in smart shared spaces lies in the intersection of cyberspace and physical space. Unlike purely digital interactions, sharing smart devices within households creates unique scenarios where privacy tensions can escalate. These challenges arise not only from technological factors but also from interpersonal dynamics within shared spaces as users try to navigate varying perceptions and approaches to protect personal information. For example, conflicts between parents and caregivers about the use of smart home cameras with audio recording capabilities have been reported [24, 41]. Similarly, privacy concerns extend to interactions between Airbnb hosts and guests [61], and between device owners and incidental users [18, 32, 48, 55, 65]. Moreover, smart technology users often lack awareness of their privacy rights [72]. Technological complexity also makes it challenging to manage privacy effectively, aligning with Altman's theory [19], which suggests that individuals consistently aim to regulate their privacy, but fail to do so optimally. A recurring theme in the literature is the trade-off between the benefits of smart technologies and their potential privacy intrusions. Devices that capture audio-visuals are frequently perceived as intrusive [24]. This tension is particularly pronounced in culturally conservative societies, where privacy expectations are shaped by social and religious norms, as noted by Yao et al. [88]. Studies show that users are more willing to share sensitive in-

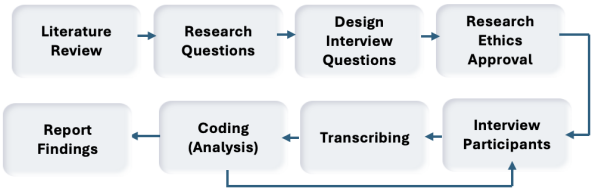

Figure 1: Research Process and Methodology.

formation when clear financial or environmental benefits are evident [38], but this willingness varies significantly based on the nature and purpose of the data being shared [53]. On the other hand, Alghamdi et al. [14] showed that users prioritize privacy when managing IoT devices. Participants expressed higher satisfaction with devices that provide strong privacy controls, even if these controls made the devices slightly more challenging to use. Despite the prevalence of these tensions, limited research has explored how users navigate and resolve them in household settings. Addressing this gap requires an understanding of the social dynamics influencing privacy decisions. By linking privacy tensions to cyber-physical sharing, we aim to uncover strategies that help designers reduce conflicts and improve the usability of smart home technologies.

2.3 Cultural Impact on Smart Home Privacy

Cultural, religious, and social factors influence the adoption and use of smart home technologies, shaping privacy expectations and how users navigate privacy in shared spaces [35, 87, 90]. Our research involves participants from the U.S. and Saudi Arabia, two regions with distinct cultural and societal backgrounds. In the U.S., the adoption of smart home technologies [71] is primarily driven by convenience, efficiency, and security. Users in Western countries typically prioritize features that streamline daily tasks, enhance home automation, and ensure security [84]. This approach reflects broader societal values, such as individual autonomy and control, that dominate Western societies [82]. In contrast, Saudi Arabia's adoption of smart home technology is profoundly shaped by Islamic principles and cultural norms, as shown by Albayaydh et al. [11] and Alkahtani et al. [17]. The Holy Qur'an [16] and the Shari'ah law [85] serve as guiding frameworks for daily life and governance, deeply influencing household dynamics and privacy expectations [75]. Cultural values, such as gender segregation and family honor, further shape the adoption and use of smart home technologies [26, 64]. For instance, women traditionally observe practices like wearing hijab and abaya in the presence of non-mahram men [34]. These differences highlight the importance of culturally tailored solutions to address privacy tensions in diverse contexts. Cultural differences in security and privacy behaviors are not unique to Saudi Arabia. Previous studies have shown that cultural background significantly influences how individuals perceive and approach privacy and security [76]. Research comparing Western populations with other cultural groups [6, 26, 51, 57, 64], and studies focusing on non-Western countries [7, 37], have highlighted substantial variations in privacy expectations. Hofstede's cultural dimensions [50, 59] have proven to be an effective model for representing key differences across cultures. The theory has been used to model user privacy behavior [59], and addresses different factors such as power distance, masculinity vs. femininity, and individualism vs. collectivism. Given these complexities, we aim to bridge the gap in understanding how culture shapes smart home privacy practices. By examining the needs and challenges faced by Saudi and U.S. users, we provide insights to guide the development of culturally sensitive solutions.

3 Methodology

Overview. We adopted an iterative Constructivist Grounded Theory (GT) approach [29] to explore how cultural perspectives shape privacy perceptions, device usage, and conflict resolution in smart homes. Our study was structured as a single evolving investigation, where each stage of data collection and analysis informed the next. Initial interviews with participants from culturally diverse backgrounds provided broad insights into privacy practices, highlighting key tensions shaped by cultural norms. These preliminary findings underscore the need for a deeper examination of privacy negotiation within Saudi households, leading to further data collection focused exclusively on this context. This iterative process allowed us to refine our research focus, ensuring that emerging themes and privacy concerns were thoroughly explored. Ethical approval was obtained from our university's ethics committee. An overview of the research process and the applied methods is shown in Figure 1.

Recruitment and Sampling. We employed purposive sampling to recruit participants [66], providing rich insights into the dynamics of privacy and sharing practices associated with smart home technologies. Participants were recruited primarily through WhatsApp groups, social media networks, and referrals. The study was advertised as exploring the use of household technology, without explicitly mentioning privacy, to minimize self-selection bias [9] and encourage a wider range of participant experiences. Initial data collection included 40 participants (20 from Saudi Arabia and 20 from the U.S.), capturing a wide range of cultural perspectives on smart home privacy and device adoption. Participants were selected to represent varying household compositions, technology experience levels, and demographic backgrounds. Interested individuals completed a screening questionnaire to confirm eligibility, which required participants to be over 18, fluent in English or Arabic, and have experience with smart home devices. In addition, we expanded our pool with subsequent recruitment focused exclusively on Saudi households, selecting 15 participants from different income levels, educational back-

Table 1: Participant Demographics

Category	Sub-category	SA (n=20)	US (n=20)
Gender	Man	30%	45%
	Women	70%	55%
Age	18-24	10%	25%
	25-34	50%	35%
	35-44	10%	15%
	45-54	15%	5%
	55 or older	15%	20%
Education	High school or less	0%	10%
	Some college	20%	30%
	Trade/technical/vocational training	0%	0%
	Bachelor's degree	50%	30%
	Master's degree	30%	20%
	Professional degree or Doctorate	0%	10%
Employment	Full-time employment	40%	40%
	Part-time employment	10%	20%
	Self-employed	25%	10%
	Unemployed	10%	10%
	Other	15%	20%
	Prefer not to answer	0%	0%
IT Background	Yes	60%	30%
	No	40%	70%

Table 2: Participant Demographics (Expanded Pool)

Category	Sub-category	Percentage (%)	Participants (n)
Gender	Women	46.7	7
	Men	53.3	8
Age	21-29 years	33.3	5
	30-49 years	33.3	5
	50 years or older	33.3	5
Education	Bachelor's Degree	53.3	8
	Graduate Degree	46.7	7
Employment	Employed	73.3	11
	Retired	13.3	2
	Student	13.3	2

grounds, and geographic regions. Given the unique structure of Saudi households, often with multiple generations living together, our sampling strategy aimed to capture variations in privacy practices based on household composition provided in Appendix C and decision-making hierarchies. Theoretical sampling guided our analysis, with interviews continuing until no new themes emerged, ensuring data saturation was reached. A detailed overview of the demographics of the participants is presented in Table 1 and Table 2.

Interviews Procedure. Interviews were conducted remotely through Microsoft Teams in private settings in either English or Arabic, depending on participant preference. The lead author, a bilingual Arabic-English speaker trained in qualitative methods, conducted all interviews. Ten Arabic interviews were conducted in Arabic, transcribed and translated into English, and reviewed by a professional translator to ensure cultural and emotional nuance was preserved. To promote participant comfort and minimize social or family pressure, no two individuals from the same household were interviewed. Participants were encouraged to speak openly, and interviews were scheduled at times of their choosing to ensure privacy. We used a semi-structured interview approach. Semi-structured interviews explored (i) Household Sharing Practices, (ii) Perceptions of Smart Devices, and (iii) Privacy Concerns. Initial interviews provided broad insights into cultural influences on smart home privacy. Consistent with Constructivist GT, interview questions evolved iteratively alongside data analysis. Early interviews offered broad insights into cultural influences on smart home privacy. As analysis progressed and theoretical insights deepened, later interviews focused more explicitly on (i) Family privacy dynamics, (ii) Religious and cultural norms shaping device usage, and (iii) Conflict resolution strategies within smart homes. Interviews ranged from 30 to 70 minutes, generating over 1340 minutes of audio and 420 pages of transcripts. Our iterative approach refined the interview guide based on ongoing analysis, ensuring comprehensive exploration of key themes. Final interview guides are provided in Appendix A and Appendix B.

Data Analysis. We followed Constructivist GT [29], an iterative and data-driven methodology well suited to exploring complex, situated privacy dynamics in smart homes. Interviews were transcribed and analyzed using NVivo 14 Pro, with data collection and analysis proceeding in parallel. Interviews were conducted in batches of 5–7, allowing us to refine the interview guide and sampling strategy based on ongoing analysis and theoretical sensitivity.

We began with open coding, applying line-by-line analysis to surface key actions, concerns, and interpretations related to privacy, technology adoption, and cultural expectations. This stage produced over 200 initial codes across both cultural contexts. These were grouped into focused codes representing recurring behavioral and perceptual patterns, forming the foundation for deeper conceptual analysis. We then engaged in axial coding, examining relationships between these focused codes to develop broader thematic categories. This phase illuminated how social norms, family structures, and religious values influenced privacy negotiations, especially in Saudi households. We used memo-writing throughout to document evolving insights, tensions, and conceptual linkages. To support our analysis, affinity diagramming was employed to organize emerging themes and visualize relationships between cultural, interpersonal, and technological factors. These visual models enabled us to map how privacy tensions were collectively negotiated and managed in context-specific ways. In the final stage of selective coding, we identified a unifying theoretical concept—Culturally Negotiated Privacy Management in Saudi Smart Homes—that integrated the most salient themes. This core category reflects the dynamic process by which privacy is shaped and reshaped through the interaction of cultural values, household relationships, and device features. To ensure credibility, we conducted member checking with four participants (two men and two women), who affirmed that our interpretations accurately represented their lived experiences. Finally, we compared our emerging theory with existing literature to contextualize our findings and highlight points of alignment and divergence. The final codebooks are provided in Appendix D and Appendix E.

Ethical Considerations. This study was reviewed and approved by our university's ethics committee, ensuring compliance with established research ethics guidelines. Before each interview, participants were provided with a detailed

study information sheet explaining the research objectives, procedures, data handling, and their rights, including voluntary participation and the option to withdraw at any stage. Participants provided written informed consent before participation, explicitly agreeing to the video recording of interviews while being assured that all identifying information would remain confidential and never be disclosed. To enhance participant comfort and privacy, they were given the option to turn off their cameras during the interview sessions. Following transcription and analysis, data were securely stored, and the transcripts were fully anonymized.

Limitations. This study aimed to explore how cultural factors shape smart home adoption and privacy dynamics, but we acknowledge certain limitations. First, our sampling was based on country-level differences (Saudi vs. U.S.) rather than direct cultural measurement. While our findings highlight broader cultural influences, they do not provide quantifiable cross-cultural comparisons. Future studies could incorporate quantitative approaches to measure these influences more systematically. Additionally, we did not explicitly test cultural constructs at the individual level. As previous research by Ghaiumy Anaraky et al. [44] has noted, culture is complex and varies within populations, and our findings may not fully capture all intra-cultural differences. Future research should expand to include additional cultural contexts beyond the U.S. and Saudi Arabia to develop a more comprehensive understanding of global smart home privacy dynamics. Finally, while GT ensures rich, qualitative insights, it does not claim generalizability beyond the sampled population. Our findings offer theoretical contributions that can guide further empirical studies, rather than providing universal conclusions about cultural privacy practices.

4 Conceptual Foundations: Insights from Open and Axial Coding

In this section, we present the key patterns and tensions that emerged through open and axial coding of the initial interview data. Drawing on Constructivist GT, we began by analyzing interviews with participants from both U.S. and Saudi households to identify context-specific interpretations of privacy, perceptions of smart technologies, and strategies for resolving emerging conflicts. While cultural differences were particularly salient in early coding, we found that further data collection from Saudi participants was needed to deepen our understanding of culturally embedded privacy negotiation. The categories outlined here represent conceptual groupings developed through early coding stages, which later informed the construction of our theoretical model in Section 5. The study codes from this stage are included in Appendix D.

4.1 Cultural Perspective in Privacy Perception

Unauthorized public disclosure of private life. Participants expressed different levels of concern about unauthorized public disclosure through physical surveillance. For physical surveillance in the household, the opinions of U.S. participants are divided between having no concerns: *"We have no concerns. It was my parents' decision. And it was for safety, just to keep an eye out"* (US8) and some concerns: *"I feel like there's no privacy, as much as [the camera] companies say that you do"* (US3). In contrast, camera surveillance has frequently been raised as a point of contention by Saudi participants, who fear that personal moments may be unintentionally exposed. SA4, who has a brother aspiring to become a social media influencer, stated, *"He literally opens his live stream all the time, and I'm worried that one day I will just walk, or pass, or talk, and I'd be on his live."* Meanwhile, SA2 had arguments with her husband regarding her desire to use household security cameras: *"He doesn't want us to use them because he thinks it is scary if someone else could watch us or publish our private lives; I believe it is essential."* This conflict is reinforced by the social stigma associated with the disclosure of personal or family matters without permission, especially those involving women, in Saudi culture. Similar tensions have also been observed in diaspora contexts. For example, Afnan et al. [2] highlights how Muslim-American women navigate strict cultural and religious expectations related to visibility, modesty, and public exposure. Their concerns about unauthorized image capture or sharing are deeply intertwined with notions of honor and family reputation, echoing the anxieties raised by Saudi participants in our study.

Privacy leak from browsing histories and recommendations. Much tension manifested in smart homes comes from privacy leakage due to browsing history and recommendations on shared smart devices becoming visible to other sharers. Participants were concerned that their family could see what they did or know what they liked, as US1 said: *"We share things that only make things convenient for us both. However, a lack of privacy between both parties can be inconvenient. I have to be more careful when searching for things in case my dad sees."* The appropriateness of the recommendations also worries some participants. US9 mentioned that these suggestions may not set a good example for their youngster: *"I could be looking up something that wouldn't be mother-appropriate, and it might be embarrassing"*. For Saudi users, the affected recommendation system could suggest things that are *"extreme for our culture or not moral"* (SA17). One observation is that when it comes to shared browsing histories and recommendations, US participants tend to complain more about personal privacy, while Saudi participants approach them with consideration for cultural and religious appropriateness.

Unauthorized expansion of shared space's boundaries. In shared smart home environments, streaming services like Netflix or Amazon Prime Video are often accessed via smart TVs

Table 3: Themes and Codes Summary

Themes	Sub-Themes
Sharing Dynamics	• Reasons for adoption • Hierarchical control delegation • Risk and benefit assessment of sharing • Scenarios of sharing
Camera Identity	• Cameras as non-mahram • Shifting perception
Interpersonal Dynamics	• Impact of camera on family dynamics • Impact of camera on host-guest dynamics
Cultural and Religious Influences	• Cultural influences on personal, familial, and guest privacy • Genders factor in privacy concerns and device sharing • Impact of cultural background on technology adoption and usage • Perception of smart home technology's suitability to cultural expectations • Religion impacting culture
Privacy Concerns and Conflicts	• Chances of something bad to happen (attack, leakage) • Data collection • Recording
Resolving Privacy Issues	• Adjustments and compromises through camera placement • Enhance privacy through technological means • Reduce shared access • Trade-off between privacy and convenience

using a single household account. However, this convenience can lead to unintentional boundary violations when login credentials are shared across family members or devices. SA14 described how account sharing compromised her privacy: *"I never change my password, and I use the same among all my accounts. My sister was able to access my private accounts."* Although such sharing may begin with trusted users, access can extend to guests or extended family, raising concerns about privacy and control. US12 shared: *"I don't know them well. My account information could be changed without consent. My passwords could be compromised. My card information could be taken."* These concerns illustrate how smart TVs, as shared access points, can expose users to unintended risks, particularly when media accounts are linked to personal or financial data. Cultural dynamics further shape how such risks are perceived and tolerated between households.

4.2 Conflict Resolution Strategies

Coordination through spatial separation. Several spatial separation schemes were used to resolve privacy conflicts. Participants decided to remove themselves from the shared space and not approach certain areas, US6 mentioned: *"We have security cameras facing the front door and backyard that send a notification to my mom when any person is detected. It works great for safety purposes, but I would not go near them, as I always feel like being monitored."* Dividing shared physical space was also used to mitigate tension. When asked what action she would take if her roommate started streaming in their shared home, SA14 stated, *"Do not share much of the inside of the house. Create a separate workspace so I don't need to change my daily routine."*

Coordination through temporal separation. Apart from spatial separation, participants also coordinated their actions through temporal separation of the shared spaces. US16 stated, *"As my parents work during the day, I usually use those accounts during the afternoon along with my brother. At night time, I usually have classes and it is when my parents enjoy the referred accounts."* Several participants preferred knowing when privacy-intruding activities would happen ahead of time, as SA15 mentioned, *"Let me know the specific time and how long it will be used."* This way, they can plan ahead and protect their privacy by steering clear of the situation.

Shifting responsibility onto oneself. More proactive methods may be chosen as tension builds up. Oftentimes, one sharer would become a dominating user governing the other sharers and taking responsibility because they are more experienced: *"I take charge of these devices since I'm more tech-savvy."* (US5) or *"I make the decisions. They have no background in protecting themselves"* (SA7). This tendency, when combined with the existing power dynamics in the household, may further exacerbate the power difference between family members, particularly in the case of Saudi Arabian culture, which is more masculine-oriented.

5 Theoretical Integration: Culturally Negotiated Privacy Management in Saudi Smart Homes

Building on the conceptual categories developed through open and axial coding (Section 4), this section presents the results of our selective coding stage, where we synthesized the most significant and interrelated concepts to develop a grounded theory. This theory centers on the core category: *Culturally Negotiated Privacy Management in Saudi Smart Homes*, capturing how privacy is continuously reshaped through everyday negotiation across technological, cultural, and interpersonal dimensions. Our analysis focused on the experiences of Saudi households, revealed how families use smart home technologies not only for convenience and safety, but also as instruments for regulating domestic visibility and social boundaries. Table 3 summarizes the six key themes that support the core category. These themes were refined through selective coding and are explored in greater detail below. We describe how the themes relate to one another and to the core category in our grounded theory model (Figure 2). The model shows how, for example, *Camera Identity* reshapes privacy norms within the context of *Cultural and Religious Influence*, giving rise to specific privacy concerns and prompting resolution strategies. Cultural and religious values pervade each theme, shaping acceptable sharing practices, modifying interpersonal dynamics, and ultimately structuring how privacy is managed in smart Saudi homes.

5.1 Sharing Dynamics

Adoption for monitoring & quality-of-life improvement. Participants emphasized the benefits of smart home devices for monitoring purposes, such as helping law enforcement, child supervision, or simply as a reassurance measure. SA26

illustrated: *"I keep checking that camera every single time to see my baby in a safe place; I open the app from my phone and try to observe my little child because one day she fell from the chair, so I worry about her."* We also found that participants prefer digital access for convenience or luxurious experiences. SA29 shared: *"It is a big comparison between digital and traditional access, I used to have lots of problems forgetting my keys, the digital one is easy to get in, you do not need to carry the key with you even mentally."*

Seniority-based control delegation. It is not uncommon for a typical Saudi family to have multiple generations living under one roof. Family hierarchies and relationships often influence control delegation regarding smart home technologies. Our interviews show that the eldest family members frequently control access to smart home devices, while children or teenagers often have less influence. For example, SA22 illustrated: *"If it's specific to our villa, then my parents would discuss it and decide. Otherwise, the most senior family member, which is my grandfather, has the biggest say."* This has resulted in a blend of generational and technological seniority-based control delegation in Saudi households, as SA23 mentioned: *"Me and my husband and my older son have access to the camera since he knows more about it."*

Perceived benefits & risks of sharing. Our findings show that sharing access can increase peace of mind and facilitate household management, as SA25 illustrated: *"I feel more comfortable when I share my camera or sometimes door lock while I am not home or traveling and I do not have time or internet to check my home."* However, despite the benefits, sharing access has its challenges. These are often associated with negative experiences with shared access, such as unintentional privacy intrusion or misusing the shared device, SA26 shared:*"My sister was traveling and permitted me to access the camera in her house. At one point, I opened the camera to check on her children and see if I could go to their house. I opened the camera and observed a private matter."*

Conditional sharing based on necessity & device sensitivity. Participants showed flexibility in sharing access to their devices when necessary or beneficial to themselves, particularly when they were away from home or when family members needed specific access. For example, SA28 illustrated: *"Regarding safety and security or mutual advantage, it's OK to share, but I exclude certain functionalities using a secret code."* Participants were also more comfortable sharing access to non-sensitive devices, especially those that do not contain or control sensitive information. As SA27 mentioned: *"[I share] the speaker and the light, even with my family member, since it has no access to my personal information or my daily habits, there is no harm in that regard."*

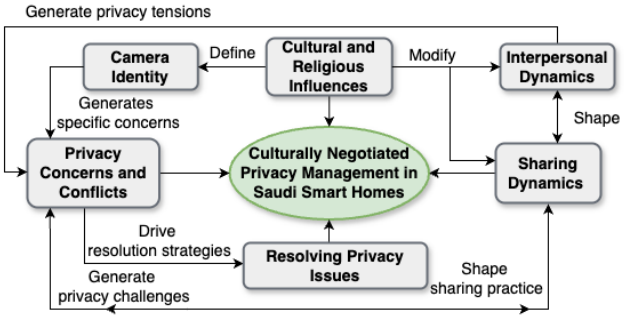

Figure 2: Grounded Theory Model – Culturally Negotiated Privacy Management in Saudi Smart Homes.

5.2 Camera Identity

Our findings show that while participants recognize the value of smart cameras for security, they often perceive these devices as more than just tools. They are frequently treated as if they are non-mahram (stranger men not related by blood). This perception, influenced by personal beliefs and social norms, changes as time progresses.

5.2.1 Cameras as Non-Mahram

Considering camera as stranger man. We found that participants perceived the cameras as unfamiliar individuals. SA21 expressed discomfort without being fully dressed when a camera was present: *"The places with cameras make me afraid to go without dressing, because whatever is in the cloud, I don't know who has access; it's scary."* The presence of a camera makes people more self-conscious, even in places that are usually private. This concern also affects how people interact with their homes and surrounding areas. For instance, SA24 sacrificed his security by removing the outdoor camera for his neighbors' comfort: *"I removed the outside cameras because I don't want to film the neighbor's mother or daughters, and their father will not agree. I don't want my neighbors to see my family and girls coming and going."* The way cameras are seen as similar to the eye of a non-mahram is indicated in SA25 observation: *"My husband doesn't want anyone to see me without my hijab and abaya. I must dress when we go out, and the same goes for my pictures in the camera."* This direct application of public dress codes within private spaces shows how the presence of cameras significantly alters notions of privacy and modesty in Saudi homes.

Someone else is watching me. We found that participants' feeling of being watched challenges the idea of considering their home a safe place. SA31 mentioned: *"Cameras are not in the bedrooms, but you still do not feel comfortable in the house."* We found that the discomfort is related to individual concerns and affects family dynamics and decisions. As SA29 shared: *"We wanted to install a CCTV camera in the house, but we decided not to tell our parents because we did not want them to watch us."* This shows how fear of being watched

can create tension and lead to opacity, even within families. The psychological impact of constant surveillance is further emphasized by SA26: *"I don't like to feel being watched, even though no one is doing anything wrong, but the feeling you know!"* This sentiment underscores how the mere presence of cameras can cause discomfort. This tension between security benefits and privacy costs reflects the broader challenges of integrating smart home technologies in culturally conservative societies, as also noted by Yao et al. [88].

5.2.2 Shifting Perception

Are cameras that important? Participants reflected on the importance of cameras, with the reasons for their adoption varying but congregating on similar outcomes. Cameras have become increasingly significant in many households, as illustrated by SA34: *"Having a camera in my house is a must, and I always vote for that."* This sentiment resonates throughout our interviews, showing a growing agreement on the need for home surveillance systems. A significant factor driving camera adoption is the common presence of domestic workers in Saudi homes. As SA27 mentioned: *"[We need cameras] to observe the nanny because the last one we had harmed my baby, hitting her and screaming at her."* Beyond security concerns, cameras are increasingly valued for their practical benefits in daily life. SA24 highlighted how cameras help locate missing items: *"We often lose our stuff. We go back to the camera storage on the application and follow until we find our stuff."* This practical aspect of camera systems demonstrates their evolving role from pure security devices to household management and convenience tools. Interestingly, cameras are also emerging as tools for maintaining family trust or uncovering untruthfulness. SA31 shared a notable example that exposed a husband's attempt to defraud his wife: *"Without the CCTV cameras, she couldn't know that he was playing games on her to get her money."*

Forgetting the existence of cameras. We found that as time passes, members tend to forget the existence of cameras in their homes. The shift in perception reflects a growing sense of comfort and trust in the presence of cameras. However, it also introduces the risk of oversight, which could lead to privacy concerns. SA25 shared: *"The wife forgot that the camera was in the house since she was used to it, her husband listened to her conversation with someone else."* These incidents reveal how the constant presence of cameras can unexpectedly invade privacy, leading to uncomfortable experiences. However, getting used to cameras' presence isn't always a bad thing. SA28 said: *"When my guests or family see themselves looking good in my cameras, they get comfortable with it by the time they even forget I have one."* The shift in how cameras are perceived and used emphasizes the need to remain vigilant about privacy and consistently review boundaries, even as technology seamlessly integrates into homes.

5.3 Cultural and Religious Influences

Cultural influences on personal, familial, and guest privacy. Balancing cultural expectations with modern technology requires careful consideration, especially regarding maintaining privacy. We found that privacy is a complex issue among Saudi family members, influenced by cultural norms that often prioritize communal living and shared spaces over individual privacy. SA24 reflected: *"In our culture, we do not have as much privacy as we would like. We invite our families to our private spaces and tend to share so much with each other."* This communal living approach can lead to complexities in managing privacy, particularly within the Saudi home structure where multiple adults commonly live together. As SA27 mentioned: *"We have more than two adults living under the same roof, like 5 or 6, compared to Western society, where they have mostly two adults."* The presence of many adults in a household can complicate decisions about privacy and the use of smart home technology, as each individual may have different expectations and needs.

Gender factors in privacy concerns and device sharing. Our findings highlight how Saudi societal and Islamic religious expectations place less scrutiny on men in situations regarding visibility and behavior. SA35 illustrated: *"When it comes to guests and cameras inside of the house, I think that for men, it will be different because there's not much concern in our society."* SA24 mentioned a more casual attitude towards being filmed: *"Because I am a guy, it doesn't matter. Who cares if someone sees me?"* This reflects the different levels of concern between genders, where men typically feel less impacted by being on camera. The presence of cameras also creates specific challenges for women, particularly if it involves controversial behaviors. SA31 mentioned: *"When my male friends gather, they do not care if I have the camera on while they smoke here. On the other hand, some of my wife's female friends smoke, but even though they trust her, they do not want to be on camera while smoking because of society's judgment regarding women's behavior."*

Impact of cultural background on technology adoption and usage. We found that cultural background profoundly influences how smart home technologies are embraced and managed in Saudi Arabia. SA28 mentioned: *"Usually, Saudis are a private-oriented people, so they do not like people outside their domain to know about their life, their homes, their family, and their problems."* This critical value of privacy guides many Saudis' cautious approach toward integrating new technology into their lives. Moreover, SA34 observed that economic factors play a significant role in the adoption of smart home devices, suggesting that financial resources can determine how broadly these technologies are integrated into daily lives:*"Adoption of technology in Saudi Arabia depends on how economically wealthy you are, some other poor people know they won't use it."* Social influence is another key driver, as SA31 mentioned: *"When I see one of my best friends*

using these kinds of tech daily, I realize I need to get these devices." Cultural traditions and customs add another layer of complexity as SA23 highlighted concerns about data security and the cultural fit of new technologies: *"Customs and traditions may play a role, considering our information is being recorded in the cloud. Our things are recorded in a place, or someone can access them, which doesn't suit us and is still a concern for our society."* SA22 summarized this cautious approach by stating: *"It's for the individual to use technology based on their cultural expectations, such as certain devices, ideas, or concepts that we just wouldn't do because they're not part of our tradition or affect our beliefs."*

Perception of smart home technology's suitability to cultural expectations. We looked at how participants perceived the suitability between smart home technologies and the cultural expectations in Saudi Arabia. SA24 mentioned: *"Some devices are not well suited in our community because they are designed, built, and manufactured for other cultures."* This highlights a discrepancy between the technology available and the unique requirements of Saudi users. SA27 supported this concern by mentioning: *"There is no clarity or transparency in the applications that are used since the policies imposed on them in their countries are different from those in our countries."* These views express worry about whether current smart home technologies align with local cultural expectations and the country's policies. However, SA22 provided a different perspective: *"Sometimes, certain things might not suit our culture based on how we view privacy and all these modesty. But the way people place technology within the household is not necessarily suited."* This points out that while cultural mismatches exist, how people adapt these technologies into their homes is essential in deciding their suitability.

Religion impacting culture. We found that religion shapes the use and perception of smart home technologies in Saudi Arabia, particularly regarding privacy and adopting new technology. As SA28 mentioned: *"Our religion goes with justice, as we always know. If this sharing brings us justice and comfort to others, it's OK, but I did not think it would be an excellent decision if there were no justice."* Similarly, SA26 mentioned: *"In some of my strictly religious friends' homes, they do not like to give up their privacy because of Islam"*, illustrating the strong link between religious values and everyday practices. SA22 added: *"We've been raised as Muslims in a certain way where right and wrong are clear, and we always want what's best for each other. I think religion and society are always hand in hand, and in Saudi Arabia at least, they always play a role in how people socialize, view modesty, and accept smart devices."* These reflections demonstrate the belief that religion strongly influences the integration of smart home technologies, emphasizing the importance of aligning with cultural and religious expectations.

5.4 Interpersonal Dynamics

5.4.1 Impact of Camera on Family Dynamics

We explored how cameras can influence family dynamics. Our findings show that cameras can create contention, leading to family members' conflicts over their use and control.

Conflicts and disagreements about camera with household. We found that cameras in common areas of the house often cause concern, as family members may feel uncomfortable being watched. SA24 mentioned: *"Some of my family members are uncomfortable when I monitor certain places, especially when the camera speaker is on."* Furthermore, the presence of cameras can lead to conflicts among siblings. SA33 expressed frustrations over unequal access: *"I always discuss with my parents why they gave my sister access to the camera since I am fine with my parents seeing me but not anyone else."* SA33 also mentioned: *"I was against the cameras, but in the end, it's my parent's house, so I must agree with their rules."* Reflecting how the household hierarchy plays a role in forcing the acceptance of these technologies. SA22 emphasized the importance of family discussions when introducing such technology: *"It will affect everyone because you're talking about a camera in places we access every day. Of course, it will affect our lives, and we will discuss it together."*

Family trust with regards to sharing. We found that trust is essential in sharing devices within the family. SA22 emphasized the inherent trust within the family: *"We always want what's best for each other, this trust is always built inside us, we always take into account our opinions and how these things affect us before the sharing decision is made."* However, sharing with extended family or those outside the immediate household can be more complex. SA26 mentioned: *"I negotiated with my husband to share the device with my mom, who doesn't live with us, but we are one family in the end, and we agree that sharing will benefit us."* Participants show that this trust is not always unconditional. As SA24 illustrated: *"If they tell me something and do another, I would be worried and stop the sharing."* This highlights the importance of maintaining trust by respecting agreed boundaries. SA35 summed up the view of many participants: *"I think knowing that my family, my parents, and my siblings always want what's best for each other, we would never put ourselves in any compromising situation."* This deep trust within the Saudi family supports sharing smart home devices, with the understanding that everyone is looking out for each other's best interests. However, this notion of trust was challenged in a previous case, where a participant shared how a camera uncovered her husband's attempt at financial deception. This introduces complexity to the otherwise solid belief in familial loyalty, highlighting the double role that smart technologies play in strengthening and challenging family trust dynamics.

Limited shared access with family members while maintaining control. We found that sharing was often limited and

conditional, even within families. SA28 mentioned: *"It's OK if I am still in control as long as it is one of my family members, but my wife always has control."* This highlights that while sharing with family members is common, many participants emphasized the importance of maintaining control over their devices. SA30 shared a similar perspective: *"I only share it with my mother for a limited time when I am not home."* This slight approach suggests a growing awareness of the need for personal privacy, even within close family circles.

5.4.2 Impact of Camera on Host-Guest Dynamics

Cameras also change how hosts and guests interact, as guests may feel uncomfortable being watched. The trust guests place in their hosts, particularly regarding who controls the cameras, plays a big part in how comfortable they feel. We explored how hosts try to balance addressing their guests' concerns and keeping the security and benefits cameras provide.

Conflicts and disagreements about cameras with guests. Many participants shared the same concerns that cameras can make their guests uncomfortable. SA26 mentioned: *"Some visitors talk about the camera in the living room, and when they saw it, they asked if the recording could be deleted, and I confirmed I would delete it."* SA22 also highlighted this issue: *"Some of my guests feel uncomfortable when they're being recorded, and more than once, we had a long discussion about it. Some of them stopped coming to my home."*

Trustworthiness of host. We found that trust plays a crucial role in how guests perceive cameras in the home. SA30 expressed: *"I am concerned, and the next time I visited them I tried not to be seen in the camera. Even though she said she is not sharing it with others, for sure, her husband has access, and even if I trust her, I won't trust him"*. This highlights the complex trust dynamics that come into play when guests know others might have access to the footage.

Limited sharing of access with guests while maintaining control. Participants were careful about sharing access with anyone outside their immediate family, preferring to limit or avoid it altogether. SA28 captured this: *"Other than family members, I don't think it's a good idea."* However, there were conflicting views on guest access. SA31 believed that guests should have some level of access to the place they stay in: *"I would like people in the guest room to have full access to everything in that room."* He added that this access is temporary and removed once the guest leaves.

Guest comfort. Participants discussed the steps they take to help their guests feel comfortable in the presence of cameras. SA34 shared:*"When my brother comes, I turn off the camera because he's a diplomat and afraid of his privacy."* That leads to the importance of guest background and acceptance of the cameras. SA25 also took steps to reduce discomfort: *"When visitors come, I have cameras on the ceiling I can't take away, so I flip them to the corner of the wall."* SA23 followed the steps by emphasizing the importance of placing cameras thoughtfully: *"I carefully choose where I put the cameras. For example, the guest area has no camera."*

5.5 Privacy Concerns and Conflicts

Participants expressed anxiety over the possibility of something going wrong, such as a security breach or a data leak. There are also notable discomfort and trust issues related to these devices. Participants are worried about the potential for these devices to record private conversations.

Chances of something bad happening. Participants expressed their fears about the possibility of their privacy being compromised, as SA28 mentioned: *"If they have access, they could probably easily hack my Wi-Fi and invade my privacy."* Even within family settings, sharing devices raised concerns, as SA25 explained: *"My husband's privacy that he is on a call that he does not want anyone to hear."*

Data collection. We found that data collection was another primary concern. SA27 shared his ongoing struggle with voice assistants: *"I stuck with Alexa, even though it is terrible, and I think it collects my data. I use it because it's the only device that understands Arabic."* On the other hand, SA24 provided a more resigned view: *"Yes, I know that the data is going somewhere, but they're recording thousands of hours of millions of other humans, who cares? I am not an important person who works on the political side or in the government."* Despite these varied perspectives, SA27 emphasized the lack of privacy assurances: *"There are no promises regarding privacy. No one will stop them if they want to steal all the information. And they are not claiming that they are not. All I want is for them to claim it is private."* SA22 also expressed a need for transparency: *"I always want to know where the data is going."*

5.6 Resolving Privacy Issues

Our analysis shows that participants actively try to take steps to manage privacy issues caused by using smart home devices. Participants adjust the cameras' location and turn them off when needed. Others focus on improving security settings and being careful about who can access these devices. Participants aim to find a balance between privacy and convenience, looking to maintain control of their homes.

Adjustments and compromises through camera placement. The most common method participants mentioned was adjusting the placement of cameras within their homes. SA26 shared: *"I only have a camera in main rooms, like the living room, dining room, and kitchen, and no camera in bedrooms,"* illustrating how selective placement can help protect more intimate spaces. SA21 also emphasized a thoughtful approach to camera placement: *"When I place the camera, I only make it cover the area needed."* This careful consideration extends to SA22's decision to avoid placing cameras in particular

areas where his grandmother stays: *"It wouldn't be where my grandma stays. Because she doesn't like it."* These methods underline a conscious effort to balance security with the need for privacy within the home.

Enhance privacy through technological means. In addition to physical adjustments, participants also focused on enhancing the security settings of their devices to avoid unnecessary data exposure. SA24 mentioned: *"I am not linking it to any of my accounts."* Similarly, SA31 noted the importance of keeping software updated: *"Every time I have this notification about a security update, I update it immediately."*

Reduce shared access. In addition to adjustments and enhancements, participants further described proactive measures to protect their privacy. For instance, SA26 mentioned: *"My father did not want to share the door's secret code with his young grandchildren, fearing the child might pass it on to other people."* This illustrates a cautious approach to sharing access information within the family. SA25 added: *"I put boundaries, to whom I give access, and not all cameras are shared."* Both examples demonstrate a conscious effort to control how and where data is stored and who can access it.

Trade-off between privacy and daily convenience. We found that efforts to maintain privacy often involve a trade-off with smart home devices' convenience. This opinion is reflected by SA29, who remarked: *"The ease of dealing with life overshadows privacy a bit, I can give up privacy,"* and SA21, who openly said: *"We sell our privacy for them because they are convenient."* These statements highlight a common theme: while privacy is highly valued, the convenience of smart home technology can sometimes justify compromising that privacy.

6 Discussion and Recommendations

Our study shows how cultural perspectives play a critical role in shaping privacy practices and the adoption of smart home technologies. We discuss how the interplay between user expectations, social norms, and technological affordances, can offer insights into culturally aware smart home design.

6.1 Summary of Findings

Privacy in Saudi households is not merely an individual concern but a collectively negotiated practice, shaped by family hierarchies, gender norms, and religious values. Our findings extend prior work in smart home privacy [4, 5, 67, 69], emphasizing the limited awareness of the privacy implications of smart technology in non-Western contexts. In contrast to studies such as Zheng et al. [92], which emphasize trade-offs between convenience and data privacy in Western homes, our participants framed smart technologies, particularly cameras, as entities whose presence must align with social and religious values. Although Western users might weigh privacy against convenience or corporate trust, Saudi participants framed privacy as a communal responsibility, negotiated between household hierarchies, and often linked to moral and spiritual obligations. Similarly, while Ur et al. [83] highlight power struggles between teens and parents around surveillance, we found that gender and religious boundaries often dictated who could control or access devices, adding layers of complexity to the governance of smart homes. Moreover, our work builds on Sun et al. [80], who point to evolving privacy awareness among parents using smart technologies, by highlighting how such awareness is not only reactive but embedded in pre-existing cultural anxieties around digital exposure. Our participants described using physical means (e.g., unplugging devices, turning cameras to the wall) to mitigate privacy threats—echoing findings in Afnan et al. [2] about how Muslim women navigate online visibility under conditions of reputational risk and religious scrutiny. However, our study extends that work to the domain of domestic technologies, uncovering how the camera, analogous to the "stranger gaze" or non-mahram male, is perceived as an agent that can violate cultural norms simply by being present. One of our key contributions is the framing of smart cameras not merely as passive surveillance tools but as culturally consequential presences. Participants often described the camera as having a "social role" within the family, affecting behavior and prompting negotiation. This resonates with broader HCI discourse on the agency of technology [27], but our findings localize this in a Saudi context, adding a novel dimension to the conversation on privacy design. In summary, our findings offer three key insights that extend prior research:

Relational Privacy. Privacy is not solely individual but shaped through household negotiation, social expectations, and shared responsibility.

Moral Dimensions. Religious and cultural ethics guide visibility and access, adding moral and spiritual weight beyond usability or risk.

Device as Social Actor. Devices are seen as socially significant entities that can reinforce or violate cultural boundaries, not just tools to be trusted or controlled.

6.2 Understanding the Complexity of Culture

Designing technologies that integrate well into diverse cultural contexts is complicated. As noted by Anarky et al. [44], cultural expectations evolve and vary across geographical regions, within households, and according to individuals. This presents significant challenges in accurately measuring privacy, and makes it difficult to develop universal privacy solutions. Our research supports this view and highlights how deeply embedded cultural values shape technology use, often in ways that technology designers may not anticipate.

6.2.1 The Dilemma of Conflicting Values

One of the key challenges we observed is the conflict between household hierarchies and privacy controls. In many Saudi homes, the decision-making authority over smart home devices is concentrated in senior family members—typically male figures—who determine access, usage, and privacy settings. When smart home technologies reinforce these hierarchies through default control settings or technical complexity, they risk exacerbating existing power imbalances. Furthermore, technological affordances do not always align with household privacy expectations. For instance, some participants noted that the lack of granular control over camera permissions led to unintended visibility for household members, guests, or domestic workers. In such cases, participants resorted to non-digital solutions, such as placing fabric over cameras or positioning devices away from private spaces. This highlights the critical gap between design assumptions and lived experiences, reinforcing the need for technologies that allow adaptive, culturally aware privacy configurations.

6.2.2 Culturally Aligned Design and Affordances

To develop culturally respectful smart home technologies, especially those using cameras, we contend that affordances [45] must be thoughtfully designed to mitigate three acknowledged usability gaps from HCI [73, 74]: the Gulf of Execution [68], Gulf of Evaluation [68], and Gulf of Expectation [39]. Our research indicates that culturally significant affordances [45], those that align with users' social values and religious practices, can mitigate the cognitive and social obstacles to the utilization of privacy-compliant technologies.

We propose three illustrative affordances grounded in the lived experiences of our Saudi participants:

Guest Mode. In the presence of guests, cameras automatically deactivate or transition to a privacy-preserving mode. This mode may be activated manually, through a voice assistant, prompted by doorbell activation, or set up to start from proximity detection of known guests' devices. It tackles the Gulf of Execution by providing an intuitive mechanism that embodies modesty rules and the Gulf of Expectation by conforming device behavior to cultural privacy standards.

Prayer Mode. Cameras and voice assistants suspend data collection during prayer periods, either according to a predetermined schedule or recognized signals. This ensures clarity regarding what is documented and the timing, reducing the Gulf of Evaluation and strengthening cultural practices.

Visitor Notification. Smart home systems alert users and guests when approaching areas equipped with operational cameras, especially in private residences, enabling visitors to make informed decisions (e.g., adjusting attire or behavior). This connects the Gulf of Evaluation and the Gulf of Expectation by revealing underlying risks and fostering trust via respectful transparency.

These examples show that affordances can be designed to suit not only individual preferences but also collective cultural values [21]. Rather than framing privacy solely as a user configuration issue, culturally aligned features enable shared negotiation and improve usability in communal settings. They offer a foundation for integrating religious and societal expectations directly into smart device functionality.

6.3 Cultural Insights as Drivers of Innovation

Rather than framing these findings as design recommendations, we argue that understanding cultural perspectives can provide novel insights and spur innovation for privacy design. Designers of smart devices need to strike a fine balance: on the one hand, they need to design technologies that are intuitive, usable, and safe for home users. On the other hand, they need to design innovative and desirable features and qualities. Unfortunately, privacy protection is not often seen as a candidate for innovation, and is more commonly addressed through regulation and compliance. This approach has the advantage of being familiar to designers and home users, and is often framed as following "best practice". However, such practices are very strongly tied to the norms and expectations of Western societies, which are typically more regulated and historically have driven the development of smart home technology. We argue that a design approach for smart home devices that draws deeply upon cultural perspectives can provide significant inspiration for future innovations in privacy. Initially, such innovations will provide more appropriate privacy solutions for these specific cultures. However, it is also likely that in doing so, they will provide greater insights into privacy interaction across different cultures, advancing the state of the art of privacy preference and protection.

7 Conclusion

Our study examines how culture shapes privacy practices in smart homes through an iterative constructivist GT approach. Focusing on Saudi households, we find that privacy is not individually defined but collectively negotiated, shaped by family hierarchies, religious values, and social norms. Smart cameras are often perceived as socially present entities, prompting users to create physical workarounds when cultural expectations are not met. These findings call for culturally responsive design approaches that support family-driven privacy strategies. Rather than viewing cultural values as constraints, we highlight their potential to inspire privacy-aware innovation. Our grounded theory of Culturally Negotiated Privacy Management in Saudi Smart Homes contributes to ongoing discussions in usable privacy and security by emphasizing the need for smart home systems that are not only technologically robust, but also socially inclusive and culturally grounded.

Acknowledgments

The authors would like to thank all participants for generously sharing their time and insights. We are also grateful to the anonymous SOUPS reviewers for their thoughtful feedback. Yara Alsiyat is supported by a graduate scholarship from King Abdulaziz City for Science and Technology (KACST).

References

[1] ACAPS. Dynamics and effects of the mahram practice in yemen. Dec 2023.

[2] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. Aunties, strangers, and the FBI: Online privacy concerns and experiences of Muslim-American women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 387–406, Boston, MA, August 2022. USENIX Association.

[3] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–28, 2020.

[4] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. Privacy, security, and surveillance in the global south: A study of biometric mobile sim registration in bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 906–918, 2017.

[5] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Understanding the physical safety, security, and privacy concerns of people with visual impairments. *IEEE Internet Computing*, 21(3):56–63, 2017.

[6] Mahdi Nasrullah Al-Ameen, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna. "we, three brothers have always known everything of each other": A cross-cultural study of sharing digital devices and online accounts. volume 2021, pages 203–224, 2021.

[7] Elham Al Qahtani, Yousra Javed, Heather Lipford, and Mohamed Shehab. Do women in conservative societies (not) follow smartphone security advice? a case study of saudi arabia and pakistan. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 150–159, 2020.

[8] Muhammad Raisul Alam, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali. A review of smart homes—past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 42(6):1190–1203, 2012.

[9] Samuele Alarie and Sonia J. Lupien. Self-selection bias in human stress research: A systematic review. *Psychoneuroendocrinology*, 131:105514, 2021.

[10] Wael Albayaydh and Ivan Flechais. "innovative technologies or invasive technologies?": Exploring design challenges of privacy protection with smart home in jordan. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1), apr 2024.

[11] Wael S Albayaydh and Ivan Flechais. Exploring bystanders' privacy concerns with smart homes in jordan. CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[12] Noura Aleisa and Karen Renaud. Yes, i know this iot device might invade my privacy, but i love it anyway. a study of saudi arabian perceptions. 2017.

[13] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. Security practices for households bank customers in the kingdom of saudi arabia. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 297–308, 2015.

[14] Fatimah Abdulrahman Alghamdi and Abdulrahman Abdullah Alghamdi. Navigating the privacy and cybersecurity risks of smart homes. In *2023 24th International Arab Conference on Information Technology (ACIT)*, pages 1–6. IEEE, 2023.

[15] Leena Alghamdi, Mamtaj Akter, Jess Kropczynski, Pamela J. Wisniewski, and Heather Lipford. Co-designing community-based sharing of smarthome devices for the purpose of co-monitoring in-home emergencies. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[16] Abdullah Yusuf Ali. *The holy Qur'an*. Wordsworth Editions, 2000.

[17] Hend Khalid Alkahtani, Ray J. Dawson, and Russell Lock. The impact of culture on saudi arabian information systems security. 2013.

[18] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. Exploring the privacy concerns of bystanders in smart homes from the perspectives of both owners and bystanders. *Proceedings on Privacy Enhancing Technologies*, 3:99–119, 2022.

[19] Irwin Altman. *The environment and social behavior: privacy, personal space, territory, and crowding.* Brooks/Cole Publishing Company, Monterey, CA, 1975.

[20] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. You, me, and iot: How internet-connected consumer devices affect interpersonal relationships. *ACM Transactions on Internet of Things*, 3(4):1–29, 2022.

[21] Jan Assmann and John Czaplicka. Collective memory and cultural identity. *New german critique*, (65):125–133, 1995.

[22] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. Social barriers to the adoption of smart homes. *Energy policy*, 63:363–374, 2013.

[23] Russell Belk and Rana Sobh. Gender and privacy in arab gulf states: Implications for consumption and marketing. *Handbook of Islamic marketing*, pages 71–96, 2011.

[24] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 687–706, Boston, MA, August 2022. USENIX Association.

[25] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 48(7):953–977, 2021.

[26] Patrick Bombik, Tom Wenzel, Jens Grossklags, and Sameer Patil. A multi-region investigation of the perceptions and use of smart home devices. volume 3, pages 6–32, 2022.

[27] Philip AE Brey. Artifacts as social agents. In *Inside the politics of technology. Agency and Normativity in the Production of Technology and Society.* Amsterdam University Press, 2005.

[28] K. Charmaz. Grounded theory: Methodology and theory construction. 2001.

[29] Kathy Charmaz. Constructing grounded theory, 2014.

[30] Kathy Charmaz. Grounded theory. *Qualitative psychology: A practical guide to research methods*, 3:53–84, 2015.

[31] Ylona Chun Tie, Melanie Birks, and Karen Francis. Grounded theory research: A design framework for novice researchers. *SAGE open medicine*, 7:2050312118822927, 2019.

[32] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. " i would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proc. Priv. Enhancing Technol.*, 2021(4):54–75, 2021.

[33] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Thousand Oaks, California, 3 edition, 2008.

[34] Cultural Atlas. Saudi arabian culture - family, 2023.

[35] Neil Daruwala and Ursula Oberst. A cross cultural investigation of individuals' acceptance of smart home technology: The role of needs satisfaction. *Aloma*, 40(2):33–45, 2022.

[36] Dylan D Furszyfer Del Rio, Benjamin K Sovacool, and Steve Griffiths. Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. *Energy and Climate Change*, 2:100035, 2021.

[37] Jayati Dev, Pablo Moriano, and L Jean Camp. Lessons learnt from comparing WhatsApp privacy concerns across saudi and indian populations. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 81–97, 2020.

[38] Hua Du, Qi Han, Dujuan Yang, Bauke de Vries, and Thomas van Houten. Data privacy and smart home energy appliances: A stated choice experiment. *Heliyon*, 9(11), 2023.

[39] Shamal Faily, David Power, and Ivan Fléchais. Gulfs of expectation: eliciting and verifying differences in trust expectations using personas. *Journal of Trust Management*, 3:1–22, 2016.

[40] Anum Farooq, Joni Salminen, James Martin, Kathleen Aldous, Soon-Gyo Jung, and Bernard J Jansen. Exploring social media privacy concerns: A comprehensive survey study across 16 middle eastern and north african countries. *IEEE Access*, 2024.

[41] Angella Foster. When parents eavesdrop on nannies, Aug 2019.

[42] Radhika Garg and Hua Cui. Social contexts, agency, and conflicts: Exploring critical aspects of design for future smart home technologies. *ACM Transactions on Computer-Human Interaction*, 29(2):1–30, 2022.

[43] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[44] Reza Ghaiumy Anaraky, Yao Li, and Bart Knijnenburg. Difficulties of measuring culture in privacy studies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–26, 2021.

[45] James J Gibson. The theory of affordances:(1979). In *The people, place, and space reader*, pages 56–60. Routledge, 2014.

[46] Barney G. Glaser. *Basics of Grounded Theory Analysis*. Sociology Press, Mill Valley, CA, 1992.

[47] Cassandra Groen, Denise R. Simmons, and Lisa D. Mcnair. An introduction to grounded theory: Choosing and implementing an emergent method. 2017.

[48] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, Baltimore, MD, August 2018. USENIX Association.

[49] Weijia He, Jesse Martinez, Roshni Padhi, Lefan Zhang, and Blase Ur. When smart devices are stupid: Negative experiences using home smart devices. In *2019 IEEE Security and Privacy Workshops (SPW)*, pages 150–155, 2019.

[50] Geert Hofstede. National cultures in four dimensions: A research-based theory of cultural differences among nations. *International studies of management & organization*, 13(1-2):46–74, 1983.

[51] Xuehui Hu, Guillermo Suarez de Tangil, and Nishanth Sastry. Multi-country study of third party trackers from real browser histories. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 70–86. IEEE, 2020.

[52] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. 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*, pages 1–13, 2020.

[53] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. End users' information-sharing behaviours and preferences within a multi-user smart home. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[54] Samia Ibtasam, Lubna Razaq, Muhammad Ayub, Jedidiah R Webster, Syed Ishtiaque Ahmed, and Richard Anderson. "my cousin bought the phone for me. i never go to mobile shops." the role of family in women's technological inclusion in islamic culture. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–33, 2019.

[55] Thorin Klosowski. Your visitors deserve to know they're on camera, Oct 2019.

[56] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. "we just use what they give us": Understanding passenger user perspectives in smart homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

[57] Kat Krol, Muhammad Sajidur Rahman, Simon Parkin, Emiliano De Cristofaro, and E Vasserman. An exploratory study of user perceptions of payment methods in the uk and the us. In *Proceedings of the 10th NDSS Workshop on Usable Security (USEC 2016)*. Internet Society, 2016.

[58] Wenda Li, Tan Yigitcanlar, Isil Erol, and Aaron Liu. Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, 80:102211, 2021.

[59] Yao Li, Alfred Kobsa, Bart P Knijnenburg, M-H Carolyn Nguyen, et al. Cross-cultural privacy prediction. *Proc. Priv. Enhancing Technol.*, 2017(2):113–132, 2017.

[60] Somayya Madakam and Ramesh Ramaswamy. Smart homes (conceptual views). pages 63–66, 2014.

[61] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proc. Priv. Enhancing Technol.*, 2020(2):436–458, 2020.

[62] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. " 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*, pages 1–11, 2020.

[63] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. " she'll just grab any device that's closer" a study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5921–5932, 2016.

[64] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies*, 1:105–125, 2022.

[65] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–29, 2021.

[66] Albine Moser and Irene Korstjens. Series: Practical guidance to qualitative research. part 3: Sampling, data collection and analysis. *European Journal of General Practice*, 24(1):9–18, 2017.

[67] Maryam Mustafa, Shaimaa Lazem, Ebtisam Alabdulqader, Kentaro Toyama, Sharifa Sultana, Samia Ibtasam, Richard Anderson, and Syed Ishtiaque Ahmed. Islamichci: Designing with and within muslim populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI EA '20, page 1–8, New York, NY, USA, 2020. Association for Computing Machinery.

[68] Donald A. Norman. *The Design of Everyday Things*. London : MIT, 1998.

[69] Norita Md Norwawi, Najwa Hayaati Mohd Alwi, Roesnita Ismail, Fauziah Wahid, and Nader M Alkaenay. Promoting islamic ethics on privacy in digital social network for user data protection and trust. *Ulum Islamiyyah Journal*, 197(1979):1–23, 2014.

[70] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, page 129–136, New York, NY, USA, 2003. Association for Computing Machinery.

[71] Eunil Park, Sunghyun Kim, YoungSeok Kim, and Sang Jib Kwon. Smart home services as the next mainstream of the ict industry: determinants of the adoption of smart home services. *Universal Access in the Information Society*, 17:175–190, 2018.

[72] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. A survey of user perspectives on security and privacy in a home networking environment. *ACM Comput. Surv.*, 55(9), jan 2023.

[73] Michael J. Quinn. *Ethics for the Information Age*. Pearson, 6th edition edition, 2015.

[74] James Rachels and Stuart Rachels. *The Elements of Moral Philosophy*. McGraw-Hill Education, 9th edition edition, 2018.

[75] Royal Embassy of Saudi Arabia. Islam, 2023.

[76] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214, 2017.

[77] Manuel Silverio Fernandez, Suresh Renukappa, and Subashini Suresh. What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Vizualization in Engineering*, 6, May 2018.

[78] Wouter MP Steijn and Anton Vedder. Privacy under construction: A developmental perspective on privacy perception. *Science, Technology, & Human Values*, 40(4):615–637, 2015.

[79] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. "it's the equivalent of feeling like you're in Jail": Lessons from firsthand and secondhand accounts of IoT-Enabled intimate partner abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 105–122, Anaheim, CA, August 2023. USENIX Association.

[80] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. Child safety in the smart home: parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–41, 2021.

[81] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "it would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, 2022.

[82] Harry Triandis. Collectivism v. individualism: A reconceptualisation of a basic concept in cross-cultural social psychology. In *Cross-cultural studies of personality, attitudes and cognition*, pages 60–95. Springer, 1988.

[83] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 129–139, 2014.

[84] Alejandro Valencia-Arias, Sebastian Cardona-Acevedo, Sergio Gómez-Molina, Juan David Gonzalez-Ruiz, and Jackeline Valencia. Smart home adoption factors: A systematic literature review and research agenda. *Plos one*, 18(10):e0292558, 2023.

[85] Esther Van Eijk. Sharia and national law in saudi arabia. *Sharia incorporated: A comparative overview of the legal systems of twelve Muslim countries in past and present*, pages 139–180, 2010.

[86] Women's Studies in Religion Program, Harvard Divinity School. What is 'awra? women, gendered space, and islamic law. 2022.

[87] Mikołaj P Woźniak, Sarah Vöge, Ronja Krüger, Heiko Müller, Marion Koelle, and Susanne Boll. Inhabiting interconnected spaces: How users shape and appropriate their smart home ecosystems. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2023.

[88] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[89] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[90] Xiaojun Zhang and Likoebe M Maruping. Household technology adoption in a global marketplace: Incorporating the role of espoused cultural values. *Information systems frontiers*, 10:403–413, 2008.

[91] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[92] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20, 2018.

A Initial Interview Questions

Characteristics of Device and Service Sharing

- How many people are there in your house?
- What is each person's relationship with you? How about their age and gender?
- What kind of digital service do you own or use in your house?
- Were you ever asked to share your information with others in your home? What was it for?

Conflicting Privacy Practices

- What factors do you consider or care about when using digital services in your home?
- Which digital service do you have the most concern with? Why is this the case?
- In your own words, please tell me your interpretation of digital privacy.
- Are there any particular privacy issues in the household you are worried about?
- Are there any particular privacy issues in the household you are aware of, but are not worried about?
- Have your housemates unexpectedly breached your privacy due to privacy leakage from digital services?
- Have you ever unexpectedly learned something about your housemate due to privacy leakage from digital services?
- Is there any specific piece of information you try your hardest to avoid giving up to the people you live with? Why?
- Are there times when you wished you could interact with those digital services without your housemate knowing? What are they? Why?

Resolving Privacy Conflicts

- How much control do you feel you have over the privacy settings of the digital services in your house?
- Who usually makes the last call in the matter? Why? Does everyone in the house agree? Please describe an incident to illustrate this.
- Is there any specific digital service that you seized using due to privacy concerns, but your housemate continues to use it? Why?
- Is there any specific digital service for which your housemate has privacy concerns, but you continue using it? Why?
- What measures do you take, if any, to work around privacy conflicts?

B Expanded Pool Interview Questions

Device and Service Sharing Dynamics

- Can you describe a typical situation in your daily life where you interact with smart home technology? What device do you use?
- How is access to or control over smart home devices managed in your household? Who typically has control, and how is this decided?
- Can you describe the different ways you share access to smart home devices? For example, do you share control differently with family members versus guests?
- Are there specific devices or services you are more comfortable sharing access to? Which ones, and why?
- How do you feel about the effects of sharing smart home technologies on aspects like privacy and daily convenience?
- Could you describe different scenarios where you might share access to your smart devices?
- Can you discuss some concerns or benefits of sharing smart home technologies?
- Can you describe specific practices or traditions that come into play when deciding/managing who gets access to these technologies?
- How do you compare managing physical access through traditional means, like keys, with managing digital access, such as through app permissions, for your smart home? What are some differences in how you handle these types of access?
- Have any personal or historical experiences shaped your approach to sharing devices and services in your smart home? Could you describe how these experiences have influenced your digital and physical sharing preferences?

Identifying Problems with Sharing Practices

- In your experience, what are the main benefits and drawbacks of sharing data or access within smart home environments?
- Can you tell me about any times when sharing control or access to your smart home devices made you or someone else in your household feel uncomfortable or uneasy? What happened?
- Have there been any disagreements or issues in your household about how smart home devices should be used or who should access them? Can you share an example of such a situation?
- How has sharing access to your smart home devices changed how you think about your safety or privacy at home? Do you feel more or less secure? and why?
- Do you find keeping things private or safe at home more challenging when others can use your smart devices? Can you describe a situation where this was the case?
- In what ways do you think sharing smart home controls could impact relationships within the household or with visitors?

Resolving Conflicts Arising from Sharing

- What steps have you taken to resolve conflicts or issues that arise from sharing access to your smart home devices? If not? What happened?

- Can you describe any methods or rules you've implemented to feel more comfortable when others use your smart home devices? What do you do to make sure everything stays safe and private?
- Have there been times when you decided to change or stop letting others use your smart home devices? Can you explain what led to that decision?
- How do your family traditions or cultural background affect how you handle disagreements or issues related to smart home device usage?
- In your experience, how is trust built and upheld when you share smart home devices with others, especially considering the cultural expectations in your community?
- Can you walk me through how you discuss and decide on technology usage and sharing rules with your family or guests in your home? What does that negotiation look like?
- Can you describe any adjustments you've made to how you use smart home devices to keep everyone comfortable and still maintain some control? What kind of compromises have you made?
- Do you think the smart home technologies available today are well-suited to the privacy and safety expectations of people in your community? Why or why not?
- How do you manage the trade-offs between making things easier and keeping things private or safe when using smart home devices with others?

C Household Composition

Table 4: Initial Data Collection - Saudi Participants

ID	Household Composition	Size	Role
SA1	Parents, 2 brothers, 2 sisters, grandmother, housekeeper	9	Daughter
SA2	Husband, 3 daughters, 2 housekeepers, son, driver	9	Wife
SA3	Mother, brother, sister, housekeeper	5	Daughter
SA4	Parents, 2 brothers, 2 sisters, grandparents, housekeeper	10	Daughter
SA5	Wife, son, housekeeper	4	Husband
SA6	Husband, daughter, housekeeper	4	Wife
SA7	Wife, son, daughter, housekeeper	5	Husband
SA8	Husband, housekeeper	3	Wife
SA9	Husband, 4 sons, 4 daughters, 2 housekeepers, 2 mothers	14	Wife
SA10	Parents, 2 brothers, 3 sisters	8	Daughter
SA11	Mother, 2 brothers, sister, housekeeper	6	Daughter
SA12	Husband, son, daughter, housekeeper	5	Wife
SA13	Parents, 3 brothers, sister, grandmother, housekeeper	9	Daughter
SA14	Parents, 3 sisters, 3 brothers, grandparents, 2 housekeepers	13	Daughter
SA15	Wife, son, daughter, housekeeper	5	Husband
SA16	Mother, 2 brothers, 2 sisters, housekeeper	7	Daughter
SA17	Wife, 2 sons, 3 daughters, housekeeper	8	Husband
SA18	Husband, 3 daughters, housekeeper	6	Wife
SA19	Parents, brother, housekeeper	5	Son
SA20	Wife, housekeeper	3	Husband

Table 5: Initial Data Collection - U.S. Participants

ID	Household Composition	Size	Role
US1	Parents	3	Son
US2	Mother, father, 2 brothers	5	Daughter
US3	Partner	2	Partner
US4	Wife, 2 daughters	4	Husband
US5	Mother, brother	3	Son
US6	Parents, sister	4	Daughter
US7	Parents, 2 brothers	5	Daughter
US8	Parents	3	Daughter
US9	Husband, daughter, son	4	Wife
US10	Parents	3	Son
US11	Husband	2	Wife
US12	Wife, daughter, son	4	Husband
US13	Mother	2	Daughter
US14	Father, mother, sister	4	Daughter
US15	Wife, son	3	Husband
US16	Father, mother, 2 brothers	5	Daughter
US17	Husband	2	Wife
US18	2 sisters	3	Son
US19	Husband, daughter	3	Wife
US20	Girlfriend	2	Partner

Table 6: Subsequent Data Collection - Saudi Participants

ID	Household Composition	Size	Role
SA21	Mother, brother, sister, housekeeper	5	Daughter
SA22	Mother, 3 brothers, 4 sisters, grandparents, housekeeper	12	Son
SA23	Husband, 5 sons, 4 daughters, 2 housekeepers, grandparents	15	Wife
SA24	wife, 2 daughters, son, housekeeper	6	Husband
SA25	Husband, housekeeper, daughter, son	5	Wife
SA26	Husband, son, housekeeper	4	Wife
SA27	Wife, 3 daughters, housekeeper	6	Husband
SA28	Wife, son, daughter, housekeeper	5	Husband
SA29	Parents, 3 brothers, grandparents, housekeeper	9	Son
SA30	Husband, son, daughter ,housekeeper	5	Wife
SA31	Wife, 2 daughters, housekeeper	5	Husband
SA32	Parents, 2 sisters, 3 brothers	8	Daughter
SA33	Parents, brother, sister, housekeeper	5	Daughter
SA34	Wife, 2 sons, 3 daughters, housekeeper	8	Husband
SA35	Mother, 2 brothers, 3 sisters, housekeeper	8	Son

D Study Codes from Conceptual Foundations

Table 7: Tension Manifestation Categories

Category	Subcategory
Misalignment	• Account usage • Privacy habits
Untrusting sharer	• Due to unfamiliarity • Believing sharer is dependent
Mistakes	• Accidental login • Accidental usage/modification
Unauthorized expansion	• Space • Sharer
Service feature	• Authentication • Notification
Leak from history	• Activities • Preferences • Buying gifts
Untailored recommendation	• Misunderstanding • Appropriacy

Table 8: Tension Mitigation Categories

Category	Subcategory
Inaction	• Nothing to do • Power difference • Trust • Expect to resume normal usage
Adopting new habits	
Alter trail of usage	
Coordination	• Spatial separation • Temporal separation • Temporal aggregation
Shifting responsibility onto oneself	
Revoke access	

E Refined Study Codes from Subsequent Data Collection

Table 9: Sharing Dynamics

Sub-Theme	Category	List of Codes
Reasons for Adoption	For monitoring	• Remote monitoring of home • Child supervision and safety • Monitoring household staff • Smart cameras for surveillance • Smart locks for access control • Outdoor cameras at main entrances • Cameras in children's areas • Assistance in law enforcement
	For quality-of-life improvements	• Convenience in daily tasks • Cost-effectiveness and accessibility • Luxury and modern living experience • Emotional comfort for parents • Smart lights for efficiency • Voice-controlled devices for ease of use • Smart TVs for entertainment • Devices in communal areas for shared benefits
Hierarchical Control Delegation	Generational seniority-based	• Parental control over device access • Grandparents given priority access • Adult children with secondary access rights • Young children with limited/supervised access
	Technological seniority-based	• Tech family members managing device setups • Younger generations teaching older members • Access rights based on technical proficiency • Tech-confident members as family IT support
Risk and Benefit Assessment of Sharing	Benefits of sharing	• Enhanced home security • Improved communication & coordination • Convenience in managing household tasks • Shared responsibility for home management
	Problems of sharing	• Privacy concerns within family members • Potential for misuse of access privileges • Challenges in maintaining individual privacy • Unauthorized access to sensitive information • Disagreements over device settings and usage
Scenarios of Sharing	Conditional sharing based on necessity	• Temporary access given during emergencies • Limited access for household staff or caregivers • Time access for visiting family members • Shared access during family gatherings
	Conditional sharing based on device sensitivity	• Sharing of non-security-related devices • Restricted access to security cameras and locks • Full family access to entertainment systems

Table 10: Camera Identity

Sub-Theme	Category	List of Codes
Cameras as Non-Mahram	Considering camera as stranger man	• Perception of cameras as non-family members • Discomfort with camera in private spaces
	Someone else is watching me	• Feeling of constant surveillance • Challenges "home as a safe space"
Shifting Perception	Are cameras that important?	• Balance between security and privacy • Reassessing the role of cameras in daily life
	Forgetting the existence of Camera	• Incremental normalization of camera presence • Unintentional effects of camera habituation • Evolving comfort levels with surveillance

Table 11: Cultural and Religious Influences

Sub-Theme	Category	List of Codes
Cultural Influence on Personal, Familial, and Guest Privacy	Cultural and personal privacy expectations with guests	• Heightened privacy concerns when hosting guests • Explain privacy measures to international visitors • Adjust camera use during guest visits • Balance hospitality with privacy preservation
	Cultural norms limiting personal privacy within family settings	• Acceptance of shared living spaces in Saudi culture • Limited expectation of individual privacy within family • Communal approach to family living and technology use • Negotiate privacy in multi-generational households
Genders Factor in Privacy Concerns and Device Sharing	Gender-specific privacy considerations	• Stricter control over recordings of women • Different levels of concern between genders about being on camera • Impact of gender on comfort with smart home devices
	Gender roles in device management	• Gender differences in device control/access • Influence of traditional gender roles on technology adoption • Gender-based restrictions in device sharing
Impact of Cultural Background on Technology Adoption and Usage	Cultural influence on adoption patterns	• Privacy-oriented approach in Saudi culture • Influence of wealth on technology adoption • Role of social influence in smart home acceptance
	Cultural adaptation of technology	• Adapt smart home use to fit Saudi customs • Concerns about data security in relation to cultural norms • Balance modernization with traditional values
Perception of Smart Home Technology's Suitability to Cultural Expectations	Cultural fit of smart home technology	• Evaluate technology alignment with Saudi values • Concerns about cultural mismatch in device design • Adapt technology to meet cultural expectations • Balance innovation with cultural preservation
Religion Impacting Culture	Religious principles in technology use	• Align smart home use with Islamic principles • Consider religious views on privacy and modesty • Impact of religious beliefs on technology acceptance
	Religious influence on decision-making	• Consult religious guidance for technology decisions • Balance religious values with technological benefits • Influence of religious norms on sharing practices

Table 12: Interpersonal Dynamics

Sub-Theme	Category	List of Codes
Impact of Camera on Family Dynamics	Conflicts and disagreements about camera with household	• Family members' discomfort with being monitored • Disagreements over camera placement in shared spaces • Tensions arising from unequal access to camera footage • Debates over the necessity of indoor cameras
	Family trust in regard to sharing	• Concerns about potential misuse of footage by family • Balancing trust and privacy within family units
	Limited sharing of access with family members while maintaining control	• Selective access to camera footage for different family members • Parental controls on camera access • Negotiating camera control among adult family members • Strategies for maintaining privacy while sharing access
Impact of Camera on Host-Guest Dynamics	Conflicts and disagreements about camera with guest	• Discomfort with visible cameras • Discussions on camera presence during visits • Guests requesting footage deletion after visits • Reduced visitation due to camera presence
	Trustworthiness of Host	• Concerns about who can access guest footage • Guests' anxiety about potential misuse of footage • Impact of trust on guest comfort levels • Host's standing regarding privacy respect
	Limited shared access with guests while maintaining control	• Restricting guest access to certain camera feeds • Time-limited access for guests • Protocols for managing guest access
	Guest Camera Comfort	• Informing guests about camera presence beforehand • Offering to turn off cameras in guest areas • Explaining camera usage and access policies to guests • Adjusting camera angles to respect guest privacy • Providing options for guests to control cameras in their space

Table 13: Privacy Concerns and Conflicts

Sub-Theme	Category	List of Codes
Chances of Something Bad to Happen (Attack, Leakage)	Security vulnerabilities	• Fears of hacking into smart home systems • Concerns about unauthorized access to camera feeds • Worries about data breaches in cloud storage
	Potential misuse of data	• Concerns about blackmail using recorded footage • Fears of identity theft through stolen smart home data • Worries about location data being used for burglary
Data Collection	Types of data collected	• Awareness of audio data collection by voice assistants • Concerns for video data from smart cameras • Tracking of daily routines and habits
	Data usage and storage	• Uncertainty about how collected data is used • Concerns for long-term storage of personal data • Lack of transparency in data handling policy
Recording	Continuous surveillance	• Discomfort with constant video recording • Concerns about audio recording of private conversations • Feeling of being constantly watched in one's own home
	Control over recording	• Desire for more control over when devices record • Concerns about inability to truly 'turn off' smart devices • Difficulties in managing recording settings

Table 14: Resolving Privacy Issues

Sub-Theme	Category	List of Codes
Adjustments and Compromises Through Camera Placement	Physical adjustments	• Reposition cameras to cover only necessary areas • Turn cameras to face walls when not in use • Install privacy screens or covers for cameras
	Usage adjustments	• Limit camera operation to specific times of day • Turn off cameras during private family moments • Adjust camera settings to blur or mask certain areas
Enhance Privacy Through Technological Means	Technical solutions	• Regularly updating device firmware and security settings • Use strong, unique passwords for each device • Enable 2-factor authentication where available
	Behavioral changes	• Being mindful of conversations around voice-activated devices • Regularly reviewing and deleting stored data • Educating family members about privacy best practices
Reduce Shared Access	Ongoing management	• Regularly audit device access and permissions • Create separate networks for smart home devices • Implement parental controls for children's device usage
Trade-off Between Privacy and Convenience	Balancing act strategies	• Selectively enabling features based on privacy-convenience trade-offs • Using privacy-enhancing modes during sensitive times • Accepting some privacy risks for significant convenience gains
	Decision-making process	• Weighing privacy concerns against practical benefits • Involving family in decisions about device usage and settings • Periodically reassessing the balance between privacy and convenience