Exploring Bystanders’ Privacy Concerns with Smart Homes in Jordan

Wael Albayaydh
wael.albayaydh@cs.ox.ac.uk
University of Oxford
Oxford, UK

Ivan Flechais
ivan.flechais@cs.ox.ac.uk
University of Oxford
Oxford, UK

ABSTRACT

Smart homes continue to raise concerns about privacy and encroachment of businesses into intimate spaces. Prior research has focused on families and device owners in western contexts (Europe and North America), and has identified the importance of bystanders: individuals who are subjected to smart device use of others. Given the cultural and contextual aspects of accommodating bystanders, we identify a gap where bystanders in non-western societies have been insufficiently researched.

To address this we conduct 20 interviews with domestic workers and household employers in Jordan, exploring privacy attitudes and practices. Our analysis uncovers a complex interplay between religious and social norms; legal and regulatory perspectives on privacy; and tensions between households and their domestic workers. We explore issues arising from smart homes coexisting as a residence and workplace, and highlight how workplace protections are ill-suited. We structure our findings to help inform public awareness, policy makers, manufacturers, and future research.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; **Human and societal aspects of security and privacy**.

KEYWORDS

Smart Home, Smart Device, Privacy, Bystanders

ACM Reference Format:
Wael Albayaydh and Ivan Flechais. 2022. Exploring Bystanders’ Privacy Concerns with Smart Homes in Jordan. In *CHI Conference on Human factors in Computing Systems (CHI ’22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3491102.3502097

1 INTRODUCTION

Smart devices can live stream information, or collect and store data (e.g., information, audio, and/or video) about home residents and bystanders who are in range. These capabilities and unprecedented levels of data collection from inside the home are raising concerns about privacy and security, including for example issues surrounding consent practices for data collection and use (e.g. dark patterns and persuasive design practices to gain consent), how personal data is protected by companies and third parties (e.g. smart CCTV or nanny-cams being breached to stream video outside the home), or even how smart technology can be misused by users against other members of the same household (e.g. intimate partner or domestic abuse). This is further complicated by the fact that homes are private spaces in which the privacy rights of smart home users and bystanders are not clearly established, and also where culturally and socially acceptable privacy norms and practices are continually evolving in the face of highly innovative and changeable technology.

The vast majority of privacy research in the smart home has focused on western contexts (e.g., Europe, and North America) however, as smart technology becomes more ubiquitous, we argue that non-western perspectives have been overlooked and require close attention in order to provide more suitable privacy solutions that fit the contextual needs more closely. In this paper, we report on the results of a qualitative study aimed at exploring the privacy concerns of domestic workers in smart homes in Jordan, which is a country that has a middle-eastern social norms and a moderate Islamic background [56]. We have examined smart homes to explore privacy attitudes and practices, focusing on public awareness of smart devices, worker privacy concerns and expectations, aspirations for privacy control in smart homes, perceptions and expectations of privacy rights, and contextual influences (i.e., social norms, customs, and religious background).

We interviewed a total of 8 families ("employers"), and 12 domestic workers ("workers") from Jordan using semi-structured interviews, which we then translated, transcribed, and analysed using Grounded Theory. We identified 5 themes: a) Weak public awareness of smart technologies and basic understanding of user privacy in the smart home; b) Privacy concerns, and expectations – highlighting that cameras are reported to be the most concerning devices; c) Perceptions that worker privacy rights are limited and power dynamics between workers and employers are asymmetric, which leaves workers with no choice other than accepting situations where employers use smart devices to monitor them; d) Contextual, social, and religious influences on privacy concerns, practices and rights; and e) Aspirations for innovative privacy control features to compensate for perceived problems with existing solutions. The paper concludes with some recommendations to mitigate the impact of smart home devices on

CHI ’22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3502097

bystander privacy in Jordan and similar contexts, and discusses future research avenues.

2 BACKGROUND AND RELATED WORK

This research study has been conducted in the middle eastern country of Jordan. The Jordanian constitution declares Islam [2] as the country's official religion, and the country is considered a moderate Muslim country.

2.1 Definitions

for clarity, we highlight here the definitions of some key terms that we will use in this paper:

Smart Device: Drawing from existing definitions in the literature [88, 95], a smart device is a controllable device that is equipped with an embedded processor, memory, sensors, and a network connection to connect to other devices or to the internet to provide useful services to the users and can store or share data on a local storage-device or over the internet.

Smart Home: Drawing on existing defnitions in the literature [17, 19], a smart home is a dwelling that is equipped with smart devices that provide the inhabitants with useful services and benefits. The smart devices in the smart home can connect to other devices and/or to the internet and can be either locally or remotely accessed, controlled and/or monitored, and can collect, store, or share data on local storage device or over the internet.

Smart Home Bystanders: We will use the definition by Yao et al. [108] which states that *"smart home bystanders refer to people who do not own or directly use the smart devices, but they are potentially involved in the use of smart home devices, such as other family members who do not purchase the devices, guests, tenants, passersby"*. Under this definition, we assume that the smart home bystanders can be subject to data collection, and they may not be aware of the installed smart devices, or the functions of these devices. In this paper, we will focus on domestic workers as a group representing smart home bystanders and we may use the term "workers" to refer to this users group.

2.2 General Overview

Smart devices can collect sensitive information from the context of the smart home all the time, which raises concerns about residents' privacy and security. Some risks arising from this include misuse of data, data leakage, cyber-attacks using compromised devices, burglary facilitated from compromised devices, and many more associated threats. Such risks are further exacerbated as many residents are not aware of the security and privacy consequences of smart devices, and the devices themselves are prone to significant usability issues that can hinder the efforts made by the inhabitants to protect their security and privacy [22, 110].

2.3 Smart Homes

The ubiquity of smart home devices and platforms has enabled applications that adapt to user's preferences and interests. Smart devices are either standalone devices that connect to the internet through existing Wi-fi networks, or devices that communicate to the internet using a bridge, like Zigbee and Z-Wave. There are two main types of smart home platforms: The Hubs, such as Wink [20], and Samsung Smart Things [110]. These central devices are designed to communicate with and control other smart devices. Similar to these hubs, the smart personal assistants, such as Google Home and Amazon Echo/Alexa, which can communicate with other smart devices, allowing users to use predefined controllers to control other smart devices. The other type makes use of cloud-hosted services instead of connecting to central hub, to enable the control of other smart devices. This is accessed via a variety of means e.g., web browsers, and smartphone applications.

2.4 Privacy

According to the Oxford English Dictionary, Privacy is the state of being alone and not watched or interrupted by other people [13]. Altman's theory of boundary [16] states that privacy is a temporal dynamic process of interpersonal boundary: a process for regulating interactions with others which indicates how open or closed we are in response to changes in our internal states and external conditions. Due to the proliferation of smart-home devices, surveillance cameras and other smart devices have become expected devices in many environments [5, 8, 50] which in turn has driven a number of privacy concerns.

2.4.1 ***Brief History of Privacy***. In 1891, Warren and Brandeis [102] published their seminal work 'The Right to Privacy', where they argued about protecting oneself from others. In 1967, Westin [103] published 'Privacy and Freedom' where he defined privacy in terms of self-determination: *"privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is shared with others"*. There is a strong relationship between technology evolution and privacy, as seen for example in the privacy concerns arising in the late 19th century from the use of cameras in public, which continues to this day shaping discussion about data use and concerns arising from the proliferation of smart devices.

2.4.2 ***Privacy Design***. Privacy in the context of smart homes has been tackled from two angles: the first by focusing on the home, its inner workings and the norms, practices and values of inhabitants; and the second by focusing on the smart devices, their technical capabilities, design characteristics, and data flows. Bridging these two perspectives, the theory of Contextual Integrity (CI) [7, 14] argues that privacy is dependent on context, which consists of two norms: the norm of appropriate data collection, and the norm of appropriate data flow. A privacy breach is considered to have occurred when either of the two norms is broken.

This perspective shows the importance of understanding privacy norms in context and prior research has aimed to do this. Apthorpe et al. [29] studied privacy norms in smart homes as a whole unit, with the aim to support designing new smart devices that users want to buy and feel secure using in their homes. On the device level, Lau et al. [63] studied voice assistants, focusing on the privacy concerns of bystanders arising from the actions of device owners. They recommended new design features to improve privacy with smart speakers such as guest mode or a voice command mute option. Yao et al. [107] studied both device owners and the bystander concerns to incorporate them in the design process and discussed how future practitioners and researchers can incorporate the findings in privacy designs.

2.5 Smart Home Privacy Concerns

Choe et al. [42], Brush et al. [36], and Worthy et al. [105] identified concerns about security and privacy risks from smart homes. Further findings from research of smart home platforms and devices [60] have identified vulnerabilities in both smart home platforms and devices, for example enabling smart TVs to record conversations [104].

User perceptions and concerns of smart devices have been studied in the literature [27, 29, 35, 72]. Naeini et al. [80] argued that privacy perceptions are context dependent, as for example people are less concerned about data collection in public places. Also, Naeini et al. [80, 113] found that users may compromise privacy for using the services and the perceived benefits. This was confirmed by Zheng et al. [113]. Also, Zeng et al. [110] found that smart homeowners in general are not concerned about potential threats. Rodden et al. [91] found that users have low concerns about data content, and instead are strongly concerned about the processing of their own data. Another study also showed that lay smart homeowners were not able to state specific threats of sharing their own data [52].

In general, smart homeowners need to be aware of the potential threats in order to be motivated to configure their smart devices to match their privacy requirements [52], [94]. Several studies have shown that smart homeowners prefer to be aware of the data collected about them [57, 76, 80]. From another perspective, Tabassum et al. [99] confirmed that smart homeowners were uncertain about how their data is used, and they expressed a wish for more transparency and control. Another study by Baldini et al. [30] showed that owners are keen to be informed about the smart device's privacy aspects before purchase. From a smart device perspective, the concerns about smart TVs have been studied by Ghiglieri et al. [5] who found that users are not aware of the data collected by smart TVs, and that when they were informed, they disconnected their smart TV from the network. Abdi et al. [23] found that some smart speaker users do not use the full functionality of the device as a result of privacy concerns as they do not want these devices to collect more information about them.

2.6 Bystander Privacy Concerns with the Smart-Home

Smart devices are integrated in the smart home social and economic context in a way that makes it difficult to figure out whether these devices are collecting information about residents and bystanders. This unfiltered collection of data is threatening the privacy of these affected populations, particularly bystanders. In many cases, bystanders are not aware of the existence or functions of the smart devices. For example, children in the home can be considered bystanders from a data collection point of view, for example where smart toys [11, 70, 74] are bought and configured without children's awareness of what these devices are, nor what they are doing. Some studies have also explored visitor concerns with shared housing (e.g. AirBnB rentals) [33, 65]. Other research is highlighting a greater awareness of the importance of bystanders [1, 12, 32, 38, 39, 68, 81, 86]. Bernd et al. [32] discussed the impact of smart devices on domestic workers (i.e., nannies) in a western context, and in earlier work [33] discussed that many researchers e.g., [58, 69, 73, 98] have proposed several solutions to privacy challenges in smart environments, such as: a) disclosure of the installed smart devices and their functions, b) improving control mechanisms, and c) adopting conservative defaults. However,the challenge remains significant when we consider that bystanders may not know about the existence of a smart device, may not know what it is doing, and that privacy control mechanisms are largely designed for the use of device administrators and not for random bystanders.

Ahmad et al. [24] argued that *"smart devices should be designed in a way that clearly and unambiguously conveys sensor states to people around them and make actionable design recommendations to provide strong privacy assurances to bystanders"*. Marky et al. [71] discussed that visitors cannot protect their privacy in a foreign smart environment due to a) poor awareness of privacy violations by smart devices, b) lack of knowledge, or c) lack of coping strategies. From this, they outlined five steps for visitors to exert control over their privacy: 1) gaining awareness, 2) gaining knowledge, 3) evaluating data sensitivity, 4) decision making, and 5) decision communication. Given the variety of challenges in this space, it is particularly important to understand the context of use of smart devices, and to understand people's expectations and interests in order to design effective privacy protection mechanisms [21].

Many privacy researchers are working to build a shared knowledge base of smart home devices such as how users understand device functionality, or user expectations in addition to privacy concerns [42, 47, 77, 101, 110]. Asymmetries in people's knowledge and experiences, together with the power dynamics between different user groups can produce a variety of privacy impacts in the context of smart homes [30, 46, 53, 84]. Flechais and Kraemer [62] argued that the control over smart devices is related to socio-cultural dynamics. These issues also extend into more nefarious scenarios, where having control over smart-home devices is an element in domestic abuse [34, 66]. Many researchers have argued that people's concerns about security and privacy in the smart home context are dependent on contextual and situational factors [5, 12, 49, 64, 65, 80], and people are more concerned about data collection in their homes rather than in their work spaces [80].

Bystander privacy can be breached by smart home devices that collect data from the environment [85] but has also been studied in different emerging technologies, such as wearable cameras [15, 59, 87], and augmented reality [39, 44, 45, 85]. These studies found that bystanders would share information if they could exert control over it, and that privacy concerns about the smart device are dependent on the context: whether it is a private or public space, e.g. using the smart device inside a house or in a metro station. Another study found that users aim to protect the privacy of bystanders [87], and there are clear indications that the cultural context plays an important role.

Contextual Integrity (CI) researchers [31, 81] have studied people's multi-context privacy concerns, and have investigated people's view of smart home devices based – in some cases – on privacy norms in smart homes vs other contexts [29, 49, 104]. Researchers found that different contexts overlapping can produce new concerns [37]. Other studies have investigated bystanders' concerns with smart devices to examine the influence of contextual factors (i.e., purposes, mechanisms, and bystanders' ability to control data collection) [45, 61, 89, 90, 90, 92, 96, 97].

More research has focused on the privacy concerns of smart home owners and their families [15, 109] and several studies have addressed multi-user scenarios [48, 51, 109, 111, 112], however not much work has addressed smart home bystanders [75, 100]. Chhetri et al. [41] discussed that the greatest user concerns with the smart devices are: a) Tracking of users, their actions and preferences, b) Storage of conversations and their transcripts (for audio conversations) in the cloud, c) The lack of security of such content in the cloud, d) The potential for private conversations to be hacked, and e) The likelihood of such information to be subject to legal discovery by law enforcement and eventually disclosed publicly. On the other hand. Yao et al. [107] argued that the complex context of smart homes, the social relationships, and power dynamics can complicate privacy aspects. Their study showed that the majority of smart home design tends to protect smart homes owners and their families, with some designs aimed to protect the privacy of bystanders. Other studies showed that some users would like to have a visitor mode of smart devices [39, 40].

2.7 Privacy in Non-Western and Muslim Contexts

The vast majority of privacy research has focused on western contexts with very little research exploring non-western contexts—specifically Muslim contexts. Researchers have argued that the notion of privacy varies substantially across cultures, times, and locations [25, 26, 43, 83, 93] suggesting that outcomes of privacy research conducted in western contexts cannot simply be applied as-is to non-western contexts. Ahmed et al. [25] highlighted the social and cultural factors that impact privacy of populations who practice mobile device sharing in the non-western Muslim context of Bangladesh.

Mustafa et al. [79] argued that understanding Muslim identity is particularly of great importance as, according to the Pew research centre [67]: *"Islam is currently the world's second-largest religion (after Christianity)"*, which makes it imperative for the HCI community to consider privacy concerns of Muslim populations with smart technologies. Norwawi et al. [82] argued that the human rights recognized in modern constitutions, charters and international treaties are embedded in the religion of Islam, as respect for life, privacy, freedom, equality, property and religious belief are an essential features of Islam. Despite the limited amount of research in this space, we found initiatives such as the ArabHCI [28] initiative, which has aimed at tackling HCI issues from Muslim perspective to address the misrepresentation of Muslim populations in HCI research, and to highlight the fact that outcomes from research conducted in western contexts require delicate adaptations to be applicable to the Muslim non-Western contexts.

3 METHODOLOGY AND RESEARCH QUESTION

With approval from the University of Oxford Central University Research Ethics Committee (CUREC) [Approval: CS-C1A-21-001], we have designed and conducted semi-structured interviews with 8 families and 12 domestic workers (nurses, care givers, nannies, babysitters, and in-home maintenance workers). This research project was conducted to address the research question "*What are the privacy concerns of the households and their domestic workers (i.e., the bystanders) in the smart homes in Jordan?"*. Fig-1 (next page) shows the research process and the applied methodology. Since there has been relatively little research exploring the privacy concerns of domestic workers and their employer families in non-western contexts, we chose to use Grounded Theory [4] as a data analysis method for our research study because it has shown to be a well-established methodology for exploring security and privacy, and is particularly suited to areas of inquiry that have not been widely researched. Through a structured process of data collection, data coding and inductive reasoning, Grounded Theory can be used to construct substantive explanatory theories.

3.1 Recruitment and Sampling

We recruited participants by posting on specialized social media groups (e.g. Babysitters Amman, Baby sitting in Jordan, Nurses in Jordan, and Ask Jordan), by directly contacting recruitment agencies, by directly contacting smart device sellers, and by snowball sampling after the candidates agree to share their contact details with us. We asked volunteers to fill a demographic and basic information survey. In the survey we provided a general description of the study, and we asked the participants whether they would like to participate. Those who accepted were asked about their age, gender, household location, education level, purpose of using smart devices, experience with smart homes, employment details, marital status, whether they are an employer or a domestic worker, and to provide their contact details for future communication with the researchers.

27 people filled the survey. After screening the survey results, we identified 20 eligible participants who met our criteria:

- Age should be over 18 years.
- To consent to participating in the interviews.
- To have experience with smart homes and smart devices.
- To be able to give the consent to being audio-recorded.

We managed to recruit and interview 8 individuals who were members of different employer families and 12 workers from different households, see Fig-2, and Table-1 (next page). We refer to the workers and families in the interview transcripts as PW and PE respectively (e.g., PE01 refers to family number 1, and PW01 refers to worker number 1). We explicitly avoided including workers and family members from the same household to avoid any negative effects arising from socio-economic power dynamics, and to enable participants to communicate openly. All participants who met the criteria were contacted to set a date and time for an online interview. The interviews were conducted using Zoom and

Figure 1: Research Process and Methodology

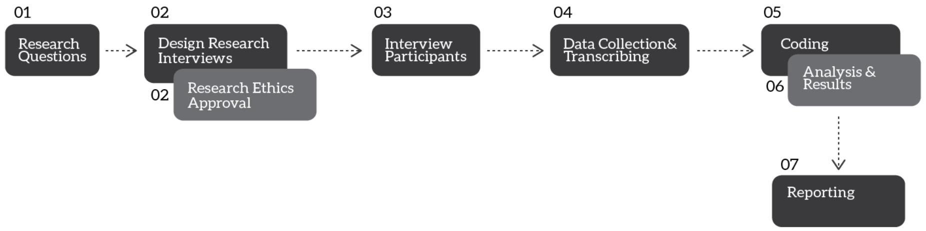


Table 1: Recruitment Channels

Recruitment Channel	Families		Workers(Domestic Workers)	
	Number	%	Number	%
Social Media Pages	2	25%	4	33.33%
Snowball Sampling	4	50%	8	66.66%
Direct Contact (Phone/Email)	2	25%	0	0%

Figure 2: Recruited Participants via Recruitment Channels

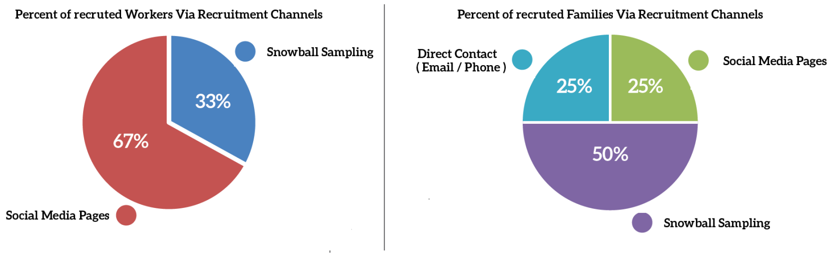


Table 2: Demographic Information of Workers

Characteristics	Number	%
Workers	12	60%
Living with the family	5	42%
Not living with the family	7	58%
Age		
18-34 Years	10	83%
35-64 Years	2	17%
Gender		
Male	2	17%
Female	10	83%
Job Type		
Nanny/Babysitter	6	50%
Nurse	5	42%
Elderly Care Giver	1	8%
Used Smart Devices		
Smart Cameras	12	100%
Smart Speakers	11	91%
Smart Lights	3	25%
Smart Windows/Doors	2	16%
Security System	12	100%
Smart Heating System	2	16%
Smart Home Appliances	7	58%

Table 3: Demographic Information of Families

Characteristics	Number	%
Families	8	40%
Living with the family	5	62.5%
Not living with the family	3	37.5%
Age		
18-34 Years	4	50%
35-64 Years	4	50%
Gender		
Male	5	62%
Female	3	38%
Hired Worker		
Nanny/Babysitter	4	50%
Maid	3	37.5%
Elderly Care Giver	1	12.5%
Used Smart Devices		
Smart Cameras	8	100%
Smart Speakers	6	75%
Smart Lights	3	37%
Smart Windows/Doors	1	12%
Security System	6	75%
Smart Heating System	1	12%
Smart Home Appliances	5	62%

Facebook Messenger, and we used standalone recording devices to audio record the interviews.

Before the interviews with the workers, we asked them explicitly to conduct the interviews outside of the houses they work in and not to use the internet infrastructure of the houses they work in to further ensure that the workers are not put under pressure. Table-2 & Table-3 show the individual characteristics of all participants: job status, technology background, and experience with smart home devices. It is important to mention that the reported smart devices by the workers might not be accurate as they may not be aware of all installed and used smart devices in the home. (See the results of all surveys in Appendix-C).

3.2 Interviews

We designed semi-structured interviews using Grounded Theory [4, 6], and informed from the literature review in order to help identify potential topics of interest. Prior to the real interviews, we conducted 4 pilot interviews to test for clarity of the questions. Adjustments were done based on the results of the pilot interviews. The pilot interviews were not included in the analysis of the research study. We transcribed and analyzed all the 20 interviews using Grounded Theory procedure [6]. The Grounded Theory has helped us examining bystanders privacy concerns with smart homes, and understanding deeply the many issues around research topic. The Grounded Theory has helped us understanding people's behaviors and attitudes, through examining both rational and irrational aspects of behaviors [106]. In the beginning of each interview, we described the research topic and asked participants to give us their permission to start the interview and to audio record it. We assured the participants that all their individual identifiable information would be kept confidential and would not be shared with any party, and we assured them that all identifiable information would be deleted after we finished the analysis of the interview transcripts. The interviews lasted between 30 to 91 minutes with an average of 41 minutes for all interviews, 35 minutes for the workers' interviews, and 52 minutes for the family interviews. We began with general questions to gather information about the participants' background, experiences, how they view and understand smart homes and smart devices, and about the relations between the families and the workers. After these warm-up questions, we went through more detailed questions, being careful not to interrupt the participants and trying to avoid influencing them or their answers.

The interviews were conducted in English with participants who could speak English language proficiently, and in Arabic with those who were not able to speak English. The main researcher translated the Arabic interviews and made efforts to avoid altering or making any changes to the participants' comments during the translations.

3.3 Analysis

After transcribing the interviews, we used the inductive grounded theory approach to analyze the transcripts. The primary researcher conducted, transcribed and translated the interviews, and performed the initial coding of all interview transcripts. Then two researchers grouped the codes into themes (axial coding) and categories (selective coding). We observed data saturation between the 19th and the 20th interview; (i.e., no significant new codes emerged in interviews 19–20).

After we completed our initial analysis (see Appendix-B), we tested the codes and themes for reliability and credibility. We used the grounded theory triangulation method by selecting randomly 7 participants (i.e., 4 workers, and 3 families) and asked them to comment on the generated codes and themes and to determine whether they agreed with the analysis output. We found consensus between the participants on the generated codes and themes. Some additional codes were identified and added to the code-book as a result of the verification process, but the new codes did not generate new themes and were linked to the existing themes.

4 RESEARCH FINDINGS AND RESULTS

The study focused on the privacy of populations in the smart homes, specifically domestic workers and employer families in smart homes in Jordan. The study showed that families use different types of smart devices such as security systems, smart cameras, smart speakers, and smart lights. Using the Grounded Theory approach described above, we used NVivo 12 Pro to code the interview transcripts and we identified 220 codes (see Appendix- B) which we organised into themes. In the following sections we will explain the identified themes.

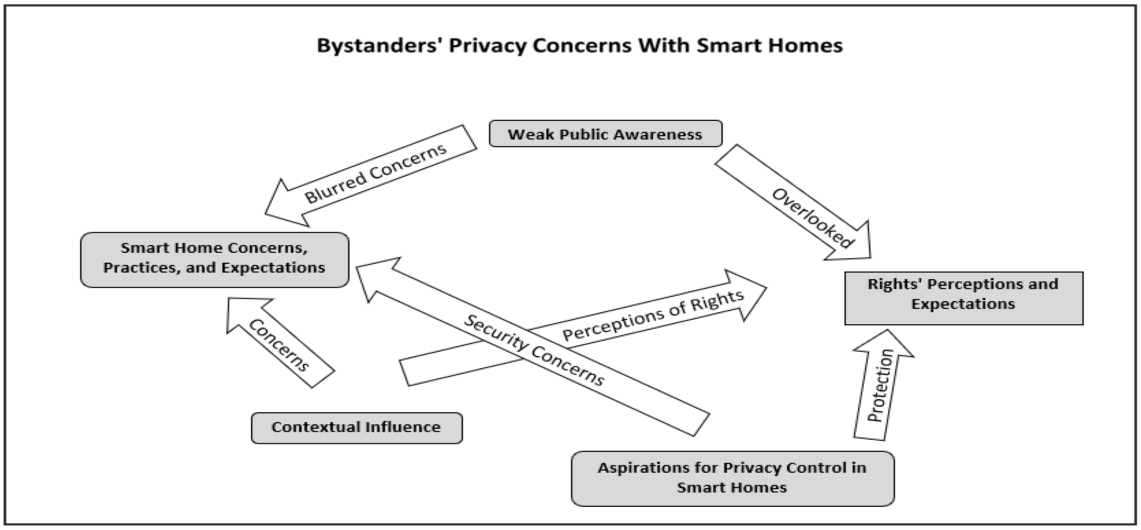
4.1 Themes

We identified 5 themes that are summarized in Table-4, and Fig-3.

Table 4: Summary of Themes and Codes

No	Themes	Sub-Themes
1	Weak Public Awareness	Weak Awareness of Smart Home and Smart Devices
		Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies
		Weak Competence of Managing Smart Devices
2	Smart Home Concerns, Practices, and Expectations	People are Mostly Concerned about Data Collection in the Home more than in the Workplace.
		People are Mostly Concerned about Audio/Visual Data Collection
		Families Have Concerns with Informing Workers about the Smart Devices
		Workers Presence in the Home Negatively Impacts Family's Privacy
		Smart Devices Drive Workers to Adopt Disciplined Practices
		Families Do Not Inform Workers About Devices
		Families Presume Workers are Aware of the Devices Existence
		Workers Should Respect the Rules of the Blended Context Of the Home
		Perception of Dis-Trusting Workers
3	Rights Perceptions and Expectations	Family's Autocratic Rights
		Perception of Dis-Respecting Workers' Privacy Rights
		Perceptions of Privacy Rights
		Absence of Privacy Rights and Policies in Jordan
		Effect of Power Dynamics and Privacy Trade Offs
		Trust Vendors' Privacy Policies
4	Aspirations for Privacy Control in Smart Homes	Improve and Ensure Awareness of Smart Devices' Existence in the Home
		Novel Applications could Utilize Recognition Technologies
		Concerns With Novel Applications
5	Contextual Influence	Religious Background , Social Norms, and Customs Influence Privacy Concerns, Practices, Expectations, and Rights.
		Religious Background is Presumed to Ensure Privacy Rights
		Religious Background and Social Dynamics Drives Positive Privacy Practices
		Workers are Presumed to Trust Religiously Committed Families

Figure 3: Visual Representation of Themes and Codes


Bystanders' Privacy Concerns With Smart Homes
Weak Public Awareness
Blurred Concerns
Overlooked
Smart Home Concerns, Practices, and Expectations
Rights' Perceptions and Expectations
Perceptions of Rights
Security Concerns
Concerns
Protection
Contextual Influence
Aspirations for Privacy Control in Smart Homes

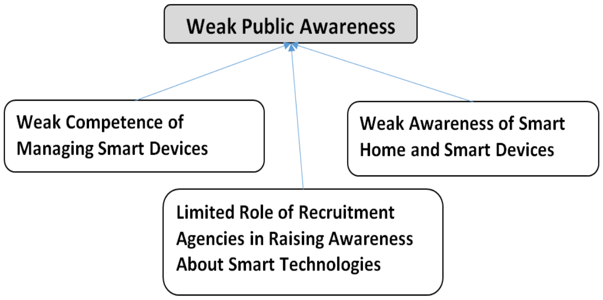
The identified 5 themes are: a) Weak public awareness of smart technologies, b) Privacy concerns, and expectations, where we found that cameras are the most concerning devices, c) Perceptions of Privacy rights, and expectations, where we highlighted the lack of privacy regulations in Jordan which has left workers with no choice other than accepting the situation as is and remaining subject to the asymmetric power dynamics between workers and their employers (i.e., the families), d) The contextual influence on privacy concerns, practices and rights, and e) The aspirations for new innovative privacy control features.(See Appendix-A, and Appendix-B for more details of all the themes and codes).

In summary, Fig-3 shows that a) Weak public awareness about smart devices causes people to overlook associated privacy rights, and is raising blurred privacy concerns about smart technologies, b) The contextual influences raise some privacy concerns, practises, and expectations, and create a goodwill perception of privacy protection and rights, c) The users' aspirations for privacy control create new security and privacy concerns, in addition to expectations of improved privacy protection features in smart home's devices.

4.1.1 ***Weak Public Awareness.*** We found weak levels of knowledge, skill, and awareness of smart technologies and smart homes, which we further break down into the following sub-themes(see Fig-4):

Weak Public Awareness of Smart Homes. When we asked participants about how they understand smart homes and smart devices, they were not able to demonstrate a strong understanding of the technology; most of the answers focused on the names and brands of the technology, with some discussion of the functionality. Only one participant mentioned that they had read the documentation and had also contacted the vendor to understand more about how to use their smart speaker (an Amazon Alexa). Most of the participants said that they do not have a clear idea about where the data is stored: some of them thought it was stored on a local hard drive inside the device, and others mentioned that they had never thought about that, but they thought the data might be stored over the cloud. PE05 said: *"I think the data is stored on a small chip inside the devices, and really, I do not know. Maybe it is online. I have never thought about that"*.

Figure 4: Weak Public Awareness


Weak Public Awareness
Weak Competence of Managing Smart Devices
Weak Awareness of Smart Home and Smart Devices
Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies

When we asked participants about how they understand privacy in the smart home, most of them said that it is mainly about audio and/or video recording them while they are inside the home, and none mentioned other types of data the smart devices might be collecting bout them (e.g., attendance patterns, daily activities, personal habits, voice print, etc.) [41].

Weak Competence of Managing Smart Devices. When we asked participants about how long data is stored for, most of them did not know. PE01 said: *"I do not know, but may be they store the data for 372 days"*. And when we asked them what vendors might be doing with their data, and how they could use it, the majority said they do not know, although a few of them mentioned that vendors could use it for advertisement, and some of them mentioned that nobody can access their data or use it. PE08 said: *"Yes, I think they use it for advertisement"*. When we asked participants about whether devices are connected to the internet, most of them said yes, and when we asked them about who can access the data and view logs, most of them said family members can. PW07 said: *"Only the family and the experts from the company can access the data"*. None of the interviewed workers or families said that workers can access the data. However, most of them said that workers can use the smart devices.

Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies. We found that participants use recruitment agencies to help them with their recruitment and employment needs, and when we asked participants whether recruitment agencies or public organizations provide any information about smart devices, most said that agencies do not provide any kind of information. Two participants mentioned that agencies had informed them that the homes they are going to work in might have smart devices like cameras and smart speakers without giving them additional details. Some participants mentioned that sometimes the recruitment poster mentioned that the home has smart devices. Additionally, it was interesting to note that some domestic workers share information on specialized social web pages about the homes they have worked for before, thus, new workers could know whether the homes they are going to work in have smart devices or not, and what type of devices are used. PW12 said:*" Not exactly, but they told us that there will be smart devices in the homes that we will be working in, and in some cases when I get my job directly through an advert, some times that advert says clearly that there are cameras or smart devices, and on the other side, we -as a group of care givers- we tell each other about the homes that we have worked in before, and whether they use smart devices or not, so the worker who will be going to that home, will be aware of the smart devices, and will take care and behave in good manner"*.

When we asked participants whether the recruitment agencies got involved in the worker-employer contract negotiations, and specifically about issues related to smart home and using smart devices in the home, all participants said agencies do not get involved in such negotiations. PW12 said: *"No, they do not get involved in contract negotiation in general."*. And when we asked participants whether they thought it would be good if agencies provided information and advice about smart devices to families and workers, they all approved of the idea. PW06 said: *"It would be good if they tell us about the smart devices and how to deal with them"*.

4.1.2 *Smart Home Privacy Concerns, Practices, and Expectations.*

We identified several privacy concerns, practices, and expectations with the smart home in Jordan.(See Fig-5):

People are Mostly Concerned about Audio/Visual Data Collection The analysis has shown that Audio/Visual data collection is the most concerning function of smart devices. PW06 said: *"I am concerned about posting video or audio file about me on social media."*. We also found that people are concerned about data collection inside the home more than in their workplace. PW12 said: *"No, as this is my workplace and I have to respect its rules"*. This makes the smart home an interesting environment given it is both a home (for employers) and a workplace (for domestic workers). We also asked participants what kind of smart devices are most used in the home, all participants commented that cameras are used the most; PE05 said: *"I use cameras to check on my mom"*. In reviewing this finding, we suspect that the responses were primed due to the earlier question about privacy concerns, and it is likely that the question was interpreted as "what kind of privacy concerning devices are most used in the home".

From the perspective of workers, some thought that they were the primary targets of smart devices data collection, while others did not feel targeted and considered themselves as bystanders to these smart devices. When we asked whether workers know if they are monitored, PW08 said: *"Yes, I know"*, while PW10 said: *"They do not use them to monitor me"*. When we asked participants about how they understand privacy in the smart home, many of them gave answers around the idea of not being monitored and recorded, and not to share data about them on social media. PE01 said: *"for me, the privacy is not to send anything about us as a family outside the home without our knowledge or consent, or to post anything about us on the social media"*.

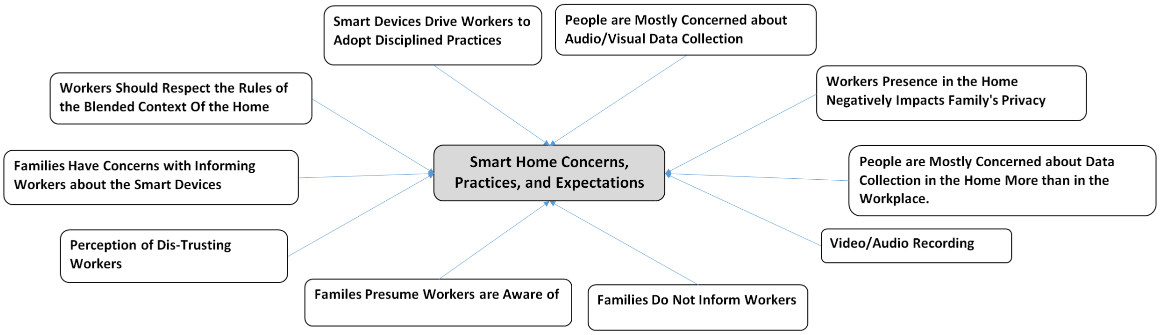
Impact of the Workers on family's Privacy. Both families and workers mentioned that family privacy is impacted by the existence of the domestic workers in the home. PE07 said: *"Of course. The presence of domestic workers in the home is squeezing our privacy and sometimes we do not feel comfortable about that situation"*.

Smart Devices Drive Workers to Adopt Disciplined Practices. Most of the participants said that workers' performance had been improved and that they had become more responsible and more productive as a result of being monitored and recorded all the time. PW12 said: *"I do my best to do everything perfectly, and to be honest without camera I may not do my job in that perfect way"*. Other workers said that they did not feel that their performance had been changed. PW06 said: *"Not really, the family trust is the most important factor for me"*.

Workers Should Respect the Rules of the Blended Context of the Home. When we asked participants about the difference between the home and the workplace for domestic workers, they said that their home is a blended context of a workplace for the workers and a home for the families, and workers have to respect the rules of the home. PE03 said: *"They are different, as for me I go and stay for a few hours in my workplace, and I have to respect the rules of my workplace. The same for the domestic worker, my home is her workplace, and she has to respect the rules of her workplace (my home) if it contradicts with her privacy rights"*.

Family members or Vendor staff manage the smart devices, and the collected data. When we asked participants about who controlled the smart devices and managed the collected data, families said one or more of the family members do. Workers said they do not know exactly who does that, but they think

Figure 5: Privacy Concerns


Smart Devices Drive Workers to Adopt Disciplined Practices
People are Mostly Concerned about Audio/Visual Data Collection
Workers Should Respect the Rules of the Blended Context Of the Home
Workers Presence in the Home Negatively Impacts Family's Privacy
Families Have Concerns with Informing Workers about the Smart Devices
Smart Home Concerns, Practices, and Expectations
People are Mostly Concerned about Data Collection in the Home More than in the Workplace.
Perception of Dis-Trusting Workers
Video/Audio Recording
Familes Presume Workers are Aware of
Families Do Not Inform Workers

that one of the family members does. PW06 said: *"The family do"*. Some participants said the device vendor's employees might do as well. PE01: *"According to amazon privacy rights, it is only us and amazon developers after we grant them our permission to do so."*

Families Presume Workers are Aware of the Devices Existence. When we asked participants about whether families inform workers about smart devices, some families said that they assume workers are aware of the smart devices. PE03 said: *"No, she has to know because everything is in the house"*.

Perception of Distrusting Workers. Some workers said that the lack of disclosure of the smart devices is a clear sign that families do not trust them. PW12 said: *"Because they do not trust us as a stranger in the house, as they do not know us, they want to be more careful about their families and homes"*.

Families Do Not Inform Workers About Devices. The analysis has shown that some families do not inform workers about the smart devices. PE03 said: *"We did not inform her."*

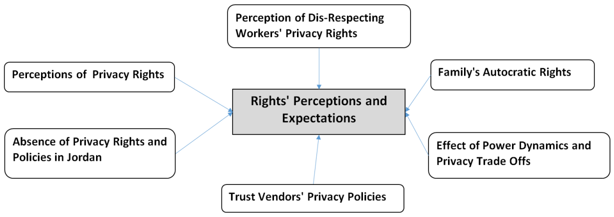
Families Have Concerns with Informing Workers about the Smart Devices. When we asked families about the reasons that prevent them from informing the workers about the smart devices, some of them said that they feel it is risky to inform them as they might quit job or create problems when they know about the devices. PE03 said: *"Yes, maybe she will break some of them or make a problem, she may misuse them."*.

*4.1.3 **Rights Perceptions and Expectations**.*

The following theme describes how privacy rights in Jordan are perceived by our participants. (See Fig-6):

Family's Autocracy. The analysis has shown that some families have an autocratic attitude concerning what should happen inside their homes, as these families think that their home is their own territory where they can do whatever they wish. Those families think that they do not have to inform workers about smart devices that are collecting data about them, nor do they need to request workers permissions to monitor and record them. PE05 said: *"It is my home, my territory, and the worker is coming to live with me or to visit me, she has to adapt to my rules. Her privacy should not affect my desire to feel secure in my home"*.

Figure 6: Rights Perceptions and Expectations


Perception of Dis-Respecting Workers' Privacy Rights
Perceptions of Privacy Rights
Family's Autocratic Rights
Rights' Perceptions and Expectations
Absence of Privacy Rights and Policies in Jordan
Effect of Power Dynamics and Privacy Trade Offs
Trust Vendors' Privacy Policies

Perception of Disrespecting Workers' Privacy Rights. Some workers said that the lack of disclosure of the smart devices is a clear sign that families do not respect their rights, but they have to accept that and to give up their privacy rights as they need to retain their jobs. PW02 said: *"In most cases and in general they do not respect the privacy of anyone inside their homes, as they believe people do not have any rights inside their home."*

Perceptions of Privacy Rights. We have identified several conflicting views relating to the perception of privacy rights for workers in smart homes. Some families thought that it is the family's right to monitor people inside their own home. PE05 said: *"No, I think it is always the right of the place owner to use any type of smart devices. If they are not ok with them, they can simply leave the place"*. Other families believed that families did not have the right to monitor workers without informing them and requesting their permission. PE01 said: *"It is not their right in my opinion"*. Workers, on the other hand, strongly believed that families should inform workers about the devices, and should request their permission. PW06 said: *"They should ask for the permission from the workers"*.

The analysis has also shown that some workers have adopted compensatory reactions to protect their privacy. One participant mentioned that she habitually placed her scarf on the cameras, and another worker mentioned that she would sit in some corners in the house to avoid the recording. PW01 said: *"Yeah my scarf. I put on the camera to prevent the recording"*, PW05 said: *"I managed* *to solve it by avoiding sitting close to them inside the home, same for the speakers"*. Additionally, some employers mentioned that cameras could be used to show what happened when there are any incidents, PE08 said: *"Legally they can be used to protect them, especially of there is a problem and someone needs to sue others in the court"*. We note that while this view was expressed by employers, it is very unclear whether and under what circumstances an employee could gain access to a recording on an employers' device.

Finally, our analysis shows that some families inform workers about smart devices and also allow them to use the devices, such as smart speakers, smart lights, and smart windows. PE05: *"Yes, she knows everything, and she uses the smart devices to help her with the daily works"*.

Absence of Privacy Rights and Policies in Jordan. We found that our participants did not think that Jordan has regulations or policies that address privacy rights in smart homes. PW05 said: *"No idea. I do not think they even exist"*. Most of families said that they did not consider privacy rights before buying and installing smart devices and they never had thought about that. PW11 said: *"No, I never thought about them"*. And when we asked participants whether work contracts have any articles about privacy rights, all of them said there is nothing about privacy rights in the work contracts. PE02 said: *"No. There is nothing about privacy in the contract"*.

Power Dynamics and User Agency. The analysis has shown the power dynamics between employers and workers are such that workers frequently give up their privacy rights in favor of other perceived benefits, such as safety, security, convenience, and to retain their jobs. PW09 said:*"Sometimes, I agree with families on not using the cams, and sometimes they do not accept. In the end I have to adapt as this is my job"*. This is consistent with what flechais and Kraemer [62] have discussed in their work on smart home families, where power dynamics and user agency [78] strongly influence awareness of how devices work, competence levels, and gaining permission to access the devices. Our finding also aligns with the work of Geen et al. [51], who found that power imbalances among smart home users reduce user agency.

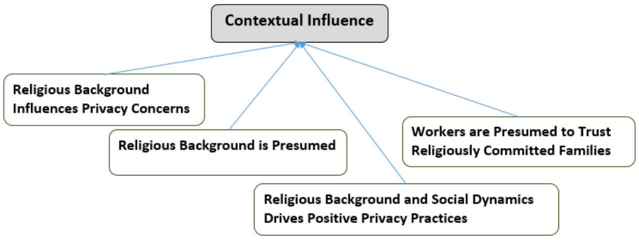
Trust Vendors' Privacy Policies. When we asked participants about whether they trusted the vendor privacy policies, they expressed a broad sense of trust. PE01 said: *"As per amazon, privacy is protected. But Alexa is turned on 24/7, and I have my doubts that Alexa can listen to us without our knowledge"*.

4.1.4 *Contextual Influence*.

Jordan's Moderate Religious background, social norms, and customs have influenced privacy concerns, practices and rights (see Fig-7):

Religious Background and Social Dynamics Drive Positive Privacy Practices. We found that the religious background, social norms, and customs of Jordan were raised as motivating some positive privacy practices such as urging families to treat workers well. PE05 said: *"Yes. I am religious person, I believe, I must inform her and respect her privacy"*.

Figure 7: Contextual Influence of Religious Background, Social Norms, and Customs


Contextual Influence
Religious Background Influences Privacy Concerns
Religious Background is Presumed
Workers are Presumed to Trust Religiously Committed Families
Religious Background and Social Dynamics Drives Positive Privacy Practices

We asked participants about the differences between visitors and domestic workers in their homes, and whether they would inform them about the installed smart devices. Some participants demonstrated a clear difference in the standing of workers and guests, saying that they would not inform workers, but they would inform visitors. This was because they felt that the social dynamics involved with having visitors would drive them to inform visitors about smart devices and also to respect visitors' privacy rights. PE04 said: *"The visitor may become upset if we do not tell him, but the worker is paid to do his job and he must accept that we are protecting our home"*

Religious Background, Social Norms, and Customs Influence Privacy Concerns, Practices, Expectations, and Rights. We found that some privacy concerns are influenced by the religious background of the person, like for example, some female workers mentioned that they do not accept to be monitored, or video recorded without their hijab (head covering). PW01 said: *"It does not feel good that they [the family] may see me when I change my clothes, or take off my hijab so I need to be careful."*.

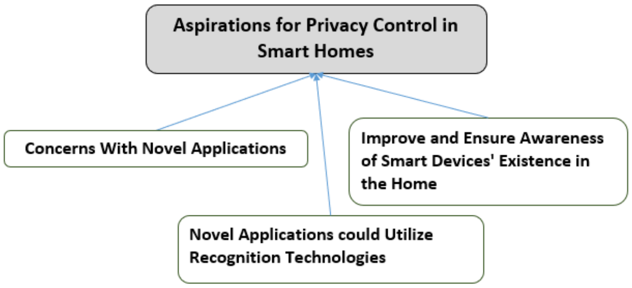
Religious Background is Presumed to Ensure Privacy Rights. We have found that many participants believe that Islam ensures privacy rights, that a committed Muslim person will adhere to Islam's statutes and will respect privacy of others, and that Islam also urges people to build good relationships with others and to trust each others. PW03 said: *"The family always tell me, they are religious people, and will not hurt you"*. PE07 said: *"We can not hide devices from her, it is forbidden in our religion"*.

4.1.5 *Aspirations for Privacy Control*.

We found that participants had a number of hopes and aspirations for more innovative privacy control features (see Fig-8):

To Improve and Ensure Awareness of Smart Devices in the Home. When we asked participants about whether they think novel technology could be used to improve the design of the smart devices to protect bystander's privacy in smart homes, most of them expressed a wish-list of privacy control features that could be adopted to protect people's privacy. PE02 said: *"Maybe we can use a secret word or something like that and maybe a mechanism to ask the device owner whether to record the new user or not, or through facial gestures, I mean through a certain mechanism"*.

Figure 8: Aspirations for Privacy Control in Smart Homes


Aspirations for Privacy Control in Smart Homes
Concerns With Novel Applications
Improve and Ensure Awareness of Smart Devices' Existence in the Home
Novel Applications could Utilize Recognition Technologies

Novel Applications Could Utilize Recognition Technologies. Some participants mentioned that recognition technologies could be used to improve the design of smart devices to help people enjoy the smart devices benefits, and to protect privacy at the same time by excluding identified individuals from data collection or use. PE01 said: *"I think by using voice recognition, and facial recognition"*.

Concerns With Novel Applications. Some participants mentioned that new privacy protections could jeopardize the safety, security, and privacy of people in the smart home. PE01 said: *"No, they may hide themselves from the devices, and conduct crimes, and they should not be given any ability to hide themselves from the devices. I think this may jeopardize the home security"*.

5 DISCUSSION AND RECOMMENDATIONS

5.1 Summary of findings

We have identified 5 themes about smart home bystander privacy concerns and expectations in Jordan. The findings showed weak awareness of smart technologies and privacy rights, basic understanding of privacy, cameras are the most concerning devices, lack of data protection and privacy regulations in Jordan, impact of asymmetric power dynamics and user agency, influence of social norms and religious background on privacy concerns, expectations, and rights, and it uncovered some user aspirations for privacy control in future smart home devices.

The findings and recommendations of this study resonate with the outcomes of prior research studies [26, 27, 32, 33, 79, 82], which have shown weak public awareness of smart technologies and the implications on people's privacy, the exigent demand for privacy research to address non-western contexts—specifically Muslim contexts, and the roles of policymakers and public awareness entities in improving the privacy protection of smart home bystanders.

Despite the fact that this study focuses on Jordan, we believe that the elicited outcomes and recommendations are applicable to some extent to other contexts in the MENA region (Middle East and North Africa) where these share similar social norms, customs, and religious background. Future research to address other MENA regions is needed to either confirm the outcomes of this study and/or present new findings and recommendations that are applicable in other MENA contexts, and also to explore whether these findings also apply to expatriate or other communities that live in foreign countries but share Jordanian social and religious customs and norms.

5.2 Recommendations for Public Awareness

To improve public awareness of smart technologies, privacy understanding, and privacy rights in Jordan, we recommend that government and public awareness organizations and related entities should collaborate to increase public awareness by: a) Conducting public awareness campaigns about smart technologies, b) Developing information booklet guides about using smart technologies in the home and its potential impact on people's privacy, c) Developing information materials and guidance for recruitment agencies, professional associations, and other concerned stakeholders on how to improve positive privacy practices, and e) To agree on a common public understanding of privacy in smart homes for different stakeholders, especially the smart home bystanders.

We believe that improving awareness of smart technologies among populations would help people mitigating privacy threats and improve privacy protection. It would also help in facilitating privacy-related discussions between employers and workers to resolve conflicts and mitigate impacts of families autocracy, and by explicitly raising awareness of privacy rights of domestic workers, may help address the asymmetric power dynamics between these different groups.

5.3 Recommendations for Policymakers

The lack of privacy regulations in Jordan is opening smart homes to asymmetric power dynamics between families and workers and also has a limiting effect on user agency given that there is a lack of clarity around what is acceptable and what is not. We recommend that policymakers and concerned entities need to consider bystander privacy concerns in future privacy policies and regulations in Jordan, and to consider and leverage social norms during the development of future regulations.

It is useful to highlight that the Jordanian government is adopting a draft bill in favor of issuing new data protection law inspired by the European GDPR [55]. It is expected the new Jordanian data protection regulations will be issued in the near future [18]. It is not clear on whether the new regulations will address user privacy rights in the smart home and similar spaces, however we do not expect the new regulations to do so. Another relevant law is the Jordanian Cybercrime law [3, 9], which has an ambiguous definition of "hate speech," defined as *"every writing and every speech or action intended to provoke sectarian or racial sedition, advocate violence or foster conflict between followers of different religions and various components of the nation."*. This can be interpreted to apply to online content regardless of whether it is intended to incite hatred or harm, or even represents a threat. Taken one step further, this could play a role in any privacy conflict between user groups in the smart homes, and it remains to be seen how this would be used by lawyers and prosecutors. Finally, the

Jordanian labour law [10] has no specific articles that discuss and address working in smart space and privacy rights of workers existing in such environments, and it is not clear whether smart homes are considered domestic or workplaces.

While the role of religion in setting policy goals is debated, it is important to note that the religion of Islam [54, 82] is being used to justify certain privacy attitudes and practices, and Islam places a strong emphasis on the importance of human rights in supporting the well-being and personal growth of every individual in civilized societies. Norwawi et al. [82] argued that the human rights recognized in modern constitutions, charters and international treaties are embedded in the religion of Islam, as respect for life, privacy, freedom, equality, property and religious belief are an essential features of Islam. Based on the above discussion, Muslim societies in general are expected to respect privacy rights.

5.4 Recommendations for Smart Device Designers

Our participants wanted more innovative privacy controls and features, such as adoption of visual and/or audio recognition technologies (i.e., facial gestures, and hand movements), different privacy modes, smart privacy settings, visual and/or audio alerts, and adoption of new features based on Artificial Intelligence technologies in order to reduce associated risks on privacy of different user groups, and to improve user agency in the smart home by making the smart devices discoverable, notifying users of what these devices are doing, and to request permissions wherever applicable.

Such aspirations are indicative of the need for more innovation and contextual awareness of the needs of bystanders for designers of smart devices, and the specific aspirations of workers and families of Jordanian smart homes are a useful inspiration for innovations that would be suitable to a wider middle eastern context.

6 LIMITATIONS

The interviews were conducted in English and Arabic. While some of the participants were non-native English or Arabic speakers, 18 participants were comfortable making the interviews in English or Arabic, however 2 participants did not find it easy to communicate in either language and we communicated as best we could. Given the difficulties in establishing a good communication, it is possible that we have missed some points about privacy concerns, power dynamics, user agency, and other issues from those two participants.

In addition to language barriers, our participants' did not have a strong awareness of smart devices, data handling, data security, and of privacy issues in smart homes, and as a result were not able to provide detailed answers to a number of more specific topics.

Finally, in common with other qualitative exploratory studies, our findings reflect the views of our 20 participants and are not generalisable to a wider population as a result. Exploring how applicable these findings are to the wider population of families and domestic workers is the subject of future work.

7 FUTURE WORK

This research is part of a research study of bystanders' privacy concerns with smart homes in Jordan. Future research will aim to verify our research findings, and to capitalize on them.

Areas of interest include: a) to study contextual dynamics (e.g., religious background, and social norms) and how to leverage them, and b) To study possible means of moderating autocratic tendencies within smart homes in light of the absence of privacy rights and policies in Jordan and similar contexts, c) To explore how designers can support mechanisms and practices which mitigate privacy risks for bystanders, and d) To investigate how policy makers can take into account workers in smart homes in future policy developments.

8 CONCLUSION

This research aims to study the impact of smart devices on the privacy of smart home bystanders (domestic workers) in a non-western context (Jordan) to identify potential privacy improvements for this user group. The study identified various privacy concerns, practices, and scenarios in which bystanders are subject to monitoring and data collection in smart homes. The study further pointed to asymmetries of knowledge, control, and power dynamics between different user groups. The importance of user agency in the smart home, both for workers and the families employing them, was highlighted against a background of unclear privacy policies, rights and regulations, and in addition to strong social and religious norms and customs.

We found that some workers perceived themselves to be targeted for data collection, while others perceived themselves as being just bystanders to smart devices. The research findings showed weak public awareness of smart homes and only a basic understating of privacy among our participants. Workers were mostly concerned about video and audio data collection, without paying attention to other types of data smart devices might be collecting about them. In contrast to this, families were much more concerned by the presence of workers in the smart homes and its impact on their family's privacy.

In light of the absence of explicit privacy rights in Jordan, we found that some families have an autocratic view about what is allowable in their home, and that they are free to do whatever they wish inside their home with or without permission. Interestingly, others believe that they have an ethical or religious obligation to inform workers about smart devices. Most workers prefer that families inform them about the existence, functions, locations, and the purposes of the installed smart devices. Some workers mentioned that the lack of disclosure of the smart devices is a clear sign of disrespect of workers' rights and of workers on the personal level. Many workers expressed that they do not feel able to assert their privacy preferences, or to protect their privacy with the installed smart devices, and they had to accept this to avoid conflicts with their employers and to maintain their job.

We found also that social and religious norms in Jordan influenced positive privacy practices and also influenced perceptions of privacy concerns and rights. We identified a level of mistrust from families towards workers, where families perceive workers as strangers in their homes, which is driving some families to use smart devices to monitor workers in order to ensure the security and safety of the home. Finally, our participants had a number of aspirations for innovative privacy controls which they believed would be better suited to their needs.

As a result of our findings, we made a number of recommendations to help inform and improve public awareness efforts; to point out areas for policymakers to address in future privacy rights, laws and policies; and to motivate smart device designers to consider non-western user aspirations for better privacy control features.

ACKNOWLEDGMENTS

The authors thank all the participants in this research study for their valuable comments and feedback and would like also to thank the staff in the department of computer science in the university of oxford for facilitating this research and for all the support they have provided.

REFERENCES

[1] [n. d.]. Big Data, Sport, and the Digital Divide: Theorizing How Athletes Might Respond to Big Data Monitoring - Andrew Baerg, 2017. https://journals.sagepub.com/doi/abs/10.1177/0193723516673409

[2] [n. d.]. Britannica (Viewed:21-March-2021). https://www.britannica.com/place/Jordan

[3] [n. d.]. Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010 (Viewed: 11-March-2021. ([n. d.]). https://www.cybercrimejournal.com/Faqir2013janijcc.pdf

[4] [n. d.]. Discovery of Grounded Theory: Strategies for Qualitative Research - Barney G Glaser, Anselm L Strauss - Google Books. https://books.google.jo/books?hl=en&lr=&id=GTMrDwAAQBAJ&oi=fnd&pg=PP1&dq=strauss+discovery+of+grounded+theory&ots=JtXbFCsrc_&sig=OIfOOscY08khAhUNPSnliQYlRJM&redir_esc=y#v=onepage&q=strauss%20discovery%20of%20grounded%20theory&f=false

[5] [n. d.]. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks *(Lecture Notes in Computer Science)*. Cham. https://link.springer.com/chapter/10.1007/978-3-319-58460-7_45

[6] [n. d.]. Grounded Theory in Practice - Anselm Strauss, Juliet M. Corbin - Google Books. https://books.google.jo/books?hl=en&lr=&id=TtRMolAapBYC&oi=fnd&pg=PP9&dq=Anselm+Strauss+and+Juliet+M.+Corbin.+Grounded+Theory+in+Practice.+SAGE+Publications,+Thousand+Oaks,+California,+1997.&ots=DBbi8voIZg&sig=MadlTZXNHMjw23EGi3gvVRqWV2U&redir_esc=y#v=onepage&q=Anselm%20Strauss%20and%20Juliet%20M.%20Corbin.%20Grounded%20Theory%20in%20Practice.%20SAGE%20Publications%2C%20Thousand%20Oaks%2C%20California%2C%201997.&f=false

[7] [n. d.]. Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life | SpringerLink. https://link.springer.com/article/10.1007%2Fs10790-010-9251-z

[8] [n. d.]. Home (Viewed:15-March-2021). https://microdata.epi.org/

[9] [n. d.]. Jordan (viewed: 11-March-2021). https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/jordan/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB&_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print

[10] [n. d.]. Jordan's New Labour Law Amendments Impact the Employment Relationship - Ogletree Deakins (viewed: 09-March-2021). https://ogletree.com/international-employment-update/articles/

[11] [n. d.]. Opinion | The Devastating Consequences of Being Poor in the Digital Age - The New York Times. https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html

[12] [n. d.]. (PDF) "What Can't Data Be Used For?": Privacy Expectations about Smart TVs in the U.S.. In *ResearchGate*. https://doi.org/10.14722/eurousec.2018.23016

[13] [n. d.]. PRIVACY | Definition of PRIVACY by Oxford Dictionary on Lexico.com also meaning of PRIVACY. https://www.lexico.com/definition/privacy

[14] [n. d.]. Privacy as Contextual Integrity Symposium - Technology, Values, and the Justice System 79 Washington Law Review 2004. https://heinonline.org/HOL/LandingPage?handle=hein.journals/washlr79&div=16&id=&page=

[15] [n. d.]. Privacy behaviors of lifeloggers using wearable cameras | Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. https://dl.acm.org/doi/abs/10.1145/2632048.2632079

[16] Sabine Trepte and Leonard Reinecke (Eds.). [n. d.]. *Privacy Online* (Berlin, Heidelberg, 2011). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21521-6

[17] [n. d.]. SMART HOME | Definition of SMART HOME by Oxford Dictionary on Lexico.com also meaning of SMART HOME. https://www.lexico.com/definition/smart_home

[18] [n. d.]. State of Privacy Jordan | Privacy International. https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

[19] [n. d.]. What is a Smart Home? https://smarthomeenergy.co.uk/what-smart-home/

[20] [n. d.]. Wink | Buy and View Smart Home Products(Viewed:21-March-2021). https://www.wink.com/products/

[21] 2018. http://www.robotshop.com/community/forum/community/forum/t/saint-louis-university-is-placing/-2-300-echo-dots-in-student-living/-spaces-https-www-theverge-com-2018/-8-15-17693174-saint-louis-/university-echo-dots-amazon-student/-living-spaces/61322

[22] 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. 36 (2018). http://www.mdpi.com/1424-8220/18/3/817

[23] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. 451–466. https://www.usenix.org/conference/soups2019/presentation/abdi

[24] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. [n. d.]. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. 4 ([n. d.]), 1–28. Issue CSCW2. https://doi.org/10.1145/3415187

[25] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. [n. d.]. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. 1 ([n. d.]), 1–20. Issue CSCW. https://doi.org/10.1145/3134652

[26] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. [n. d.]. 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* (Denver Colorado USA, 2017-05-02). ACM, 906–918. https://doi.org/10.1145/3025453.3025961

[27] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. 2017. Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments. *IEEE Internet Computing* (2017), 1–1. https://doi.org/10.1109/MIC.2017.265103316 Conference Name: IEEE Internet Computing.

[28] Ebtisam Alabdulqader, Norah Abokhodair, and Shaimaa Lazem. [n. d.]. Human-Computer Interaction Across the Arab World. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (Denver Colorado USA, 2017-05-06). ACM, 1356–1359. https://doi.org/10.1145/3027063.3049280

[29] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (July 2018), 59:1–59:23. https://doi.org/10.1145/3214262

[30] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. 2018. Ethical Design in the Internet of Things. *Science and Engineering Ethics* 24, 3 (June 2018), 905–925. https://doi.org/10.1007/s11948-016-9754-5

[31] A. Barth, A. Datta, J.C. Mitchell, and H. Nissenbaum. 2006. Privacy and contextual integrity: framework and applications. In *2006 IEEE Symposium on Security and Privacy (S P'06)*. 15 pp.–198. http://doi.org/10.1109/SP.2006.32 ISSN: 2375-1207.

[32] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. https://www.usenix.org/conference/foci20/presentation/bernd

[33] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. 2019. Smart Home Bystanders: Further Complexifying a Complex Context. (2019), 6. https://privaci.info/symposium2/papers_and_slides/Sub_Bernd_et_al_Bystanders_CI_2019.pdf

[34] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times* (June 2018). https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[35] Denys Brand, Florence D. DiGennaro Reed, Mariah D. Morley, Tyler G. Erath, and Matthew D. Novak. 2020. A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities. *Behavior Analysis in Practice* 13, 1 (March 2020), 11–21. https://doi.org/10.1007/s40617-018-00329-y

[36] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 2115–2124. https://doi.org/10.1145/1978942.1979249

[37] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place* 50 (March 2018), 112–118. https://doi.org/10.1016/j.healthplace.2018.01.006

[38] George Chalhoub and Ivan Flechais. [n. d.]. "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In *HCI for Cybersecurity, Privacy and Trust*, Abbas Moallem (Ed.). Vol. 12210. Springer International Publishing, 305–325. https://doi.org/10.1007/978-3-030-50309-3_21 Series Title: Lecture Notes in Computer Science.

[39] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[40] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3334480.3382850

[41] Chola Chhetri and Vivian Genaro Motti. 2019. Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. In *Information in Contemporary Society*. Springer, Cham, 91–101. https://doi.org/10.1007/978-3-030-15742-5_8

[42] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/2370216.2370226

[43] Andy Crabtree, Peter Tolmie, and Will Knight. [n. d.]. Repacking 'Privacy' for a Networked World. 26, 4 ([n. d.]), 453–488. https://doi.org/10.1007/s10606-017-9276-y

[44] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *Comput. Surveys* 52, 6 (Oct. 2019), 110:1–110:37. https://doi.org/10.1145/3359626

[45] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352

[46] David Eckhoff and Isabel Wagner. 2018. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys Tutorials* 20, 1 (2018), 489–516. http://doi.org/10.1109/COMST.2017.2748998 Conference Name: IEEE Communications Surveys Tutorials.

[47] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. 21–40. https://www.usenix.org/conference/soups2019/presentation/frik

[48] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2 (June 2019), 44:1–44:21. https://doi.org/10.1145/3328915

[49] Vaibhav Garg, L. Jean Camp, Lesa Lorenzen-Huber, Kalpana Shankar, and Kay Connelly. 2014. Privacy concerns in assisted living technologies. *annals of telecommunications - annales des télécommunications* 69, 1 (Feb. 2014), 75–88. https://doi.org/10.1007/s12243-013-0397-0

[50] Jun Ge. 2016. Observers' Privacy Concerns about Wearable Cameras. (March 2016). https://etda.libraries.psu.edu/catalog/28890

[51] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[52] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. [n. d.]. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. ([n. d.]), 4. https://spice.luddy.indiana.edu/files/2018/07/wssp2018-paper2.pdf

[53] Loni Hagen. 2017. Overcoming the Privacy Challenges of Wearable Devices: A Study on the Role of Digital Literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research (dg.o '17)*. Association for Computing Machinery, New York, NY, USA, 598–599. https://doi.org/10.1145/3085228.3085254

[54] Muhammad Aslam Hayat1. 2007. Privacy and Islam: From the Quran to data protection in Pakistan. *Information & Communications Technology Law* 16, 2 (June 2007), 137–148. https://doi.org/10.1080/13600830701532043 Publisher: Routledge.

[55] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 2019. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law* 28, 1 (Jan. 2019), 65–98. https://doi.org/10.1080/13600834.2019.1573501 Publisher: Routledge _eprint: https://doi.org/10.1080/13600834.2019.1573501.

[56] Fukiko IKEHATA. 2017. <Special Feature "Toward New Studies on Islamic Moderate Trends">Aspiring to be a Leader of Moderation: A Study on Jordan's Islamic Policy. https://doi.org/10.14989/225232

[57] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(es) with Smart Home: Experiences of a Living Lab field Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799

[58] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and privacy: it's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/2335356.2335369

[59] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't look at me that way! Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 362–372. https://doi.org/10.1145/2785830.2785842

[60] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (Jan. 2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[61] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2017. Exploring Design Directions for Wearable Privacy. https://publications.cispa.saarland/2808/

[62] Martin Krämer. [n. d.]. Disentangling Privacy in Smart Homes. ([n. d.]), 11. https://www.martin-kraemer.net/presentations/2018-10-cdt-showcase.pdf

[63] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 102:1–102:31. https://doi.org/10.1145/3274371

[64] Hosub Lee and Alfred Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. 407–412. http://doi.org/10.1109/WF-IoT.2016.7845392

[65] Linda Lee, JoongHwa Lee, Serge Egelman, and David Wagner. 2016. Information Disclosure Concerns in The Age of Wearable Computing. In *Proceedings 2016 Workshop on Usable Security*. Internet Society, San Diego, CA. https://doi.org/10.14722/usec.2016.23006

[66] Roxanne Leitão. 2018. Digital Technologies and their Role in Intimate Partner Violence. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3180305

[67] Michael Lipka. [n. d.]. *Muslims and Islam: Key findings in the U.S. and around the world*. https://www.pewresearch.org/fact-tank/2017/08/09/muslims-and-islam-key-findings-in-the-u-s-and-around-the-world/

[68] Deborah Lupton. 2014. Self-tracking cultures: towards a sociology of personal informatics. In *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: the Future of Design (OzCHI '14)*. Association for Computing Machinery, New York, NY, USA, 77–86. https://doi.org/10.1145/2686612.2686623

[69] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. 340–345. http://doi.org/10.1109/PerComW.2012.6197507

[70] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (April 2020), 436–458. https://doi.org/10.2478/popets-2020-0035

[71] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. [n. d.]. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (Essen Germany, 2020-11-22). ACM, 83–95. https://doi.org/10.1145/3428361.3428464

[72] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. &#x201d;I don&#x2019;t know how to protect myself&#x201d;: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3419249.3420164

[73] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543. https://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc4&id=563&div=&collection=

[74] Oriana McDonough. 2019. A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices. *Syracuse University Honors Program Capstone Projects* (May 2019). https://surface.syr.edu/honors_capstone/1085

[75] Sarah Mennicken, David Kim, and Elaine May Huang. 2016. Integrating the Smart Home into the Digital Calendar. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 5958–5969. https://doi.org/10.1145/2858036.2858168

[76] M. Mikusz, S. Houben, N. Davies, K. Moessner, and M. Langheinrich. 2018. Raising Awareness of IoT Sensor Deployments. (Jan. 2018), 9 (8 pp.)–9 (8 pp.). https://doi.org/10.1049/cp.2018.0009 Publisher: IET Digital Library.

[77] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. 2016. Understanding the Privacy Design Space for Personal Connected Objects. (July 2016). https://doi.org/10.14236/ewic/HCI2016.18 Publisher: BCS Learning & Development.

[78] James W. Moore. 2016. What Is the Sense of Agency and Why Does it Matter? *Frontiers in Psychology* 7 (Aug. 2016). https://doi.org/10.3389/fpsyg.2016.01272

[79] Maryam Mustafa, Shaimaa Lazem, Ebtisam Alabdulqader, Kentaro Toyama, Sharifa Sultana, Samia Ibtasam, Richard Anderson, and Syed Ishtiaque Ahmed. [n. d.]. IslamicHCI: Designing with and within Muslim Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu HI USA, 2020-04-25). ACM, 1–8. https://doi.org/10.1145/3334480.3375151

[80] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[81] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Oct. 2011), 32–48. https://doi.org/10.1162/DAED_a_00113

[82] Norita Md Norwawi, Roesnita Ismail, Fauziah Wahid, Nader M. Alkaenay, and Najwa Hayaati Mohd Alwi. 2014. Promoting Islamic Ethics on Privacy in Digital Social Network for User Data Protection and Trust. *Islamic Science* 197, 1979 (Dec. 2014), 1–23. https://doi.org/10.12816/0012632 Publisher: Islamic Science University of Malaysia.

[83] Leysia Palen and Paul Dourish. [n. d.]. Unpacking "Privacy" for a Networked World. ([n. d.]), 8.

[84] Scott R. Peppet. 2014. Regulating the Internet of Things: first Steps toward Managing Discrimination, Privacy, Security and Consent. *Texas Law Review* 93 (2014), 85. https://heinonline.org/HOL/Page?handle=hein.journals/tlr93&id=95&div=&collection=

[85] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. [n. d.]. NotiSense: An Urban Sensing Notification System To Improve Bystander Privacy. ([n. d.]), 5.

[86] James Pierce, Richmond Y. Wong, and Nick Merrill. 2020. Sensor Illumination: Exploring Design Qualities and Ethical Implications of Smart Cameras and Image/Video Analytics. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–19. https://doi.org/10.1145/3313831.3376347

[87] Blaine A. Price, Avelie Stuart, Gul Calikli, Ciaran Mccormick, Vikram Mehta, Luke Hutton, Arosha K. Bandara, Mark Levine, and Bashar Nuseibeh. 2017. Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 2 (June 2017), 22:1–22:18. https://doi.org/10.1145/3090087

[88] Gilles Privat. 2000. A system-architecture viewpoint on smart networked devices. *Microelectronic Engineering* 54, 1 (Dec. 2000), 193–197. https://doi.org/10.1016/S0167-9317(00)80070-2

[89] Halley Profita, Reem Albaghli, Leah findlater, Paul Jaeger, and Shaun K. Kane. 2016. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 4884–4895. https://doi.org/10.1145/2858036.2858130

[90] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. "You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. 143–157. https://www.usenix.org/conference/soups2018/presentation/rashidi

[91] Tom A. Rodden, Joel E. fischer, Nadia Pantidi, Khaled Bachour, and Stuart Moran. 2013. At home with agents: exploring attitudes towards future smart energy infrastructures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1173–1182. https://doi.org/10.1145/2470654.2466152

[92] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. 2014. Augmented reality: hard problems of law and policy. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 1283–1288. https://doi.org/10.1145/2638728.2641709

[93] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. [n. d.]. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. ([n. d.]), 17.

[94] J. SathishKumar and Dhiren R. Patel. 2014. A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications* 90, 11 (March 2014), 20–26. https://doi.org/10.5120/15764-4454

[95] Manuel Silverio-Fernández, Suresh Renukappa, and Subashini Suresh. 2018. What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering* 6, 1 (May 2018), 3. https://doi.org/10.1186/s40327-018-0063-8

[96] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. 2016. You are Being Watched: Bystanders' Perspective on the Use of Camera Devices in Public Spaces. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 3197–3203. https://doi.org/10.1145/2851581.2892522

[97] Manya Sleeper, Sebastian Schnorf, Brian Kemler, and Sunny Consolvo. 2015. Attitudes toward vehicle-based sensing and recording. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. Association for Computing Machinery, New York, NY, USA, 1017–1028. https://doi.org/10.1145/2750858.2806064

[98] Daniel J Solove. [n. d.]. A Brief History of Information Privacy Law. ([n. d.]), 47. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

[99] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. 435–450. https://www.usenix.org/conference/soups2019/presentation/tabassum

[100] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. 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 (UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[101] John Vines, Stephen Lindsay, Gary W. Pritchard, Mabel Lie, David Greathead, Patrick Olivier, and Katie Brittain. 2013. Making family care work: dependence, privacy and remote home monitoring telecare systems. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing (UbiComp '13)*. Association for Computing Machinery, New York, NY, USA, 607–616. https://doi.org/10.1145/2493432.2493469

[102] Samuel Warren and Louis Brandeis. 1989. *The Right to Privacy*. Columbia University Press. https://www.degruyter.com/document/doi/10.7312/gold91730-002/html Pages: 1-21 Publication Title: Killing the Messenger Section: Killing the Messenger.

[103] Alan F. Westin. 1966. Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I–The Current Impact of Surveillance on Privacy. *Columbia Law Review* 66, 6 (1966), 1003–1050. https://doi.org/10.2307/1120997 Publisher: Columbia Law Review Association, Inc..

[104] Jenifer Sunrise Winter. 2015. Citizen Perspectives on the Customization/Privacy Paradox Related to Smart Meter Implementation:. *International Journal of Technoethics* 6, 1 (Jan. 2015), 45–59. https://doi.org/10.4018/ijt.2015010104

[105] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. Association for Computing Machinery, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890

[106] Brad Wuetherick. 2010. Review: "Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory 3e" (Corbin and Strauss). 36 (Dec. 2010). https://doi.org/10.21225/D5G01T

[107] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[108] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 59:1–59:24. https://doi.org/10.1145/3359161

[109] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 6777–6788. https://doi.org/10.1145/3025453.3025907

[110] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[111] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

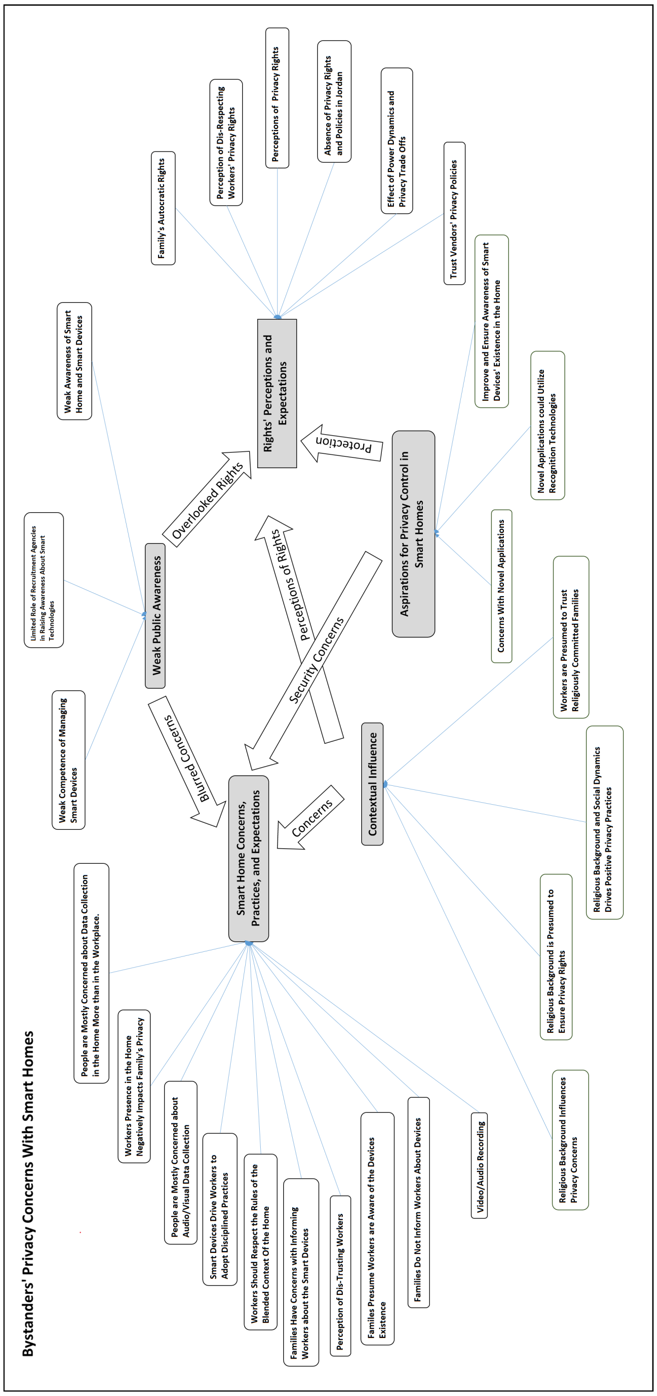
[112] Yu Zhai, Yan Liu, Minghao Yang, Feiyuan Long, and Johanna Virkki. 2014. A Survey Study of the Usefulness and Concerns about Smart Home Applications

from the Human Perspective. *Open Journal of Social Sciences* 02, 11 (2014), 119. https://doi.org/10.4236/jss.2014.211017 Number: 11 Publisher: Scientific Research Publishing.

[113] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 200:1–200:20. https://doi.org/10.1145/3274469

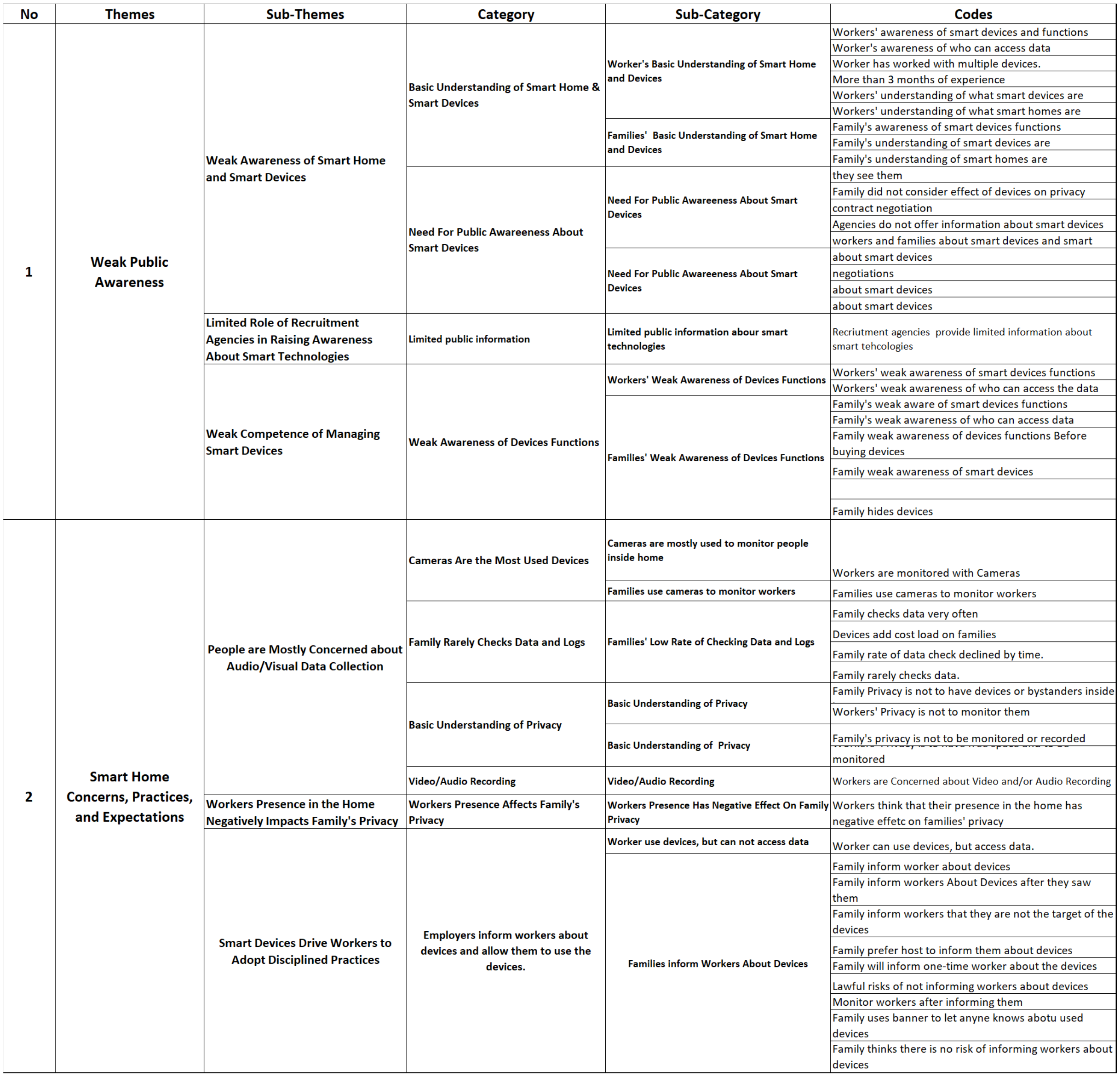
Appendix-A

Figure 9: Visual Representation of Themes and Codes


Bystanders' Privacy Concerns With Smart Homes
Family's Autocratic Rights
Perception of Dis-Respecting Workers' Privacy Rights
Perceptions of Privacy Rights
Absence of Privacy Rights and Policies in Jordan
Effect of Power Dynamics and Privacy Trade Offs
Trust Vendors' Privacy Policies
Improve and Ensure Awareness of Smart Devices' Existence in the Home
Novel Applications could Utilize Recognition Technologies
Concerns With Novel Applications
Rights' Perceptions and Expectations
Protection
Aspirations for Privacy Control in Smart Homes
Overlooked Rights
Weak Awareness of Smart Home and Smart Devices
Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies
Weak Public Awareness
Weak Competence of Managing Smart Devices
Perceptions of Rights
Security Concerns
Blurred Concerns
Concerns
Contextual Influence
Smart Home Concerns, Practices, and Expectations
Workers are Presumed to Trust Religiously Committed Families
Religious Background and Social Dynamics Drives Positive Privacy Practices
Religious Background is Presumed to Ensure Privacy Rights
Religious Background Influences Privacy Concerns
People are Mostly Concerned about Data Collection in the Home More than in the Workplace.
Workers Presence in the Home Negatively Impacts Family's Privacy
People are Mostly Concerned about Audio/Visual Data Collection
Smart Devices Drive Workers to Adopt Disciplined Practices
Workers Should Respect the Rules of the Blended Context Of the Home
Families Have Concerns with Informing Workers about the Smart Devices
Perception of Dis-Trusting Workers
Families Presume Workers are Aware of the Devices Existence
Families Do Not Inform Workers About Devices
Video/Audio Recording

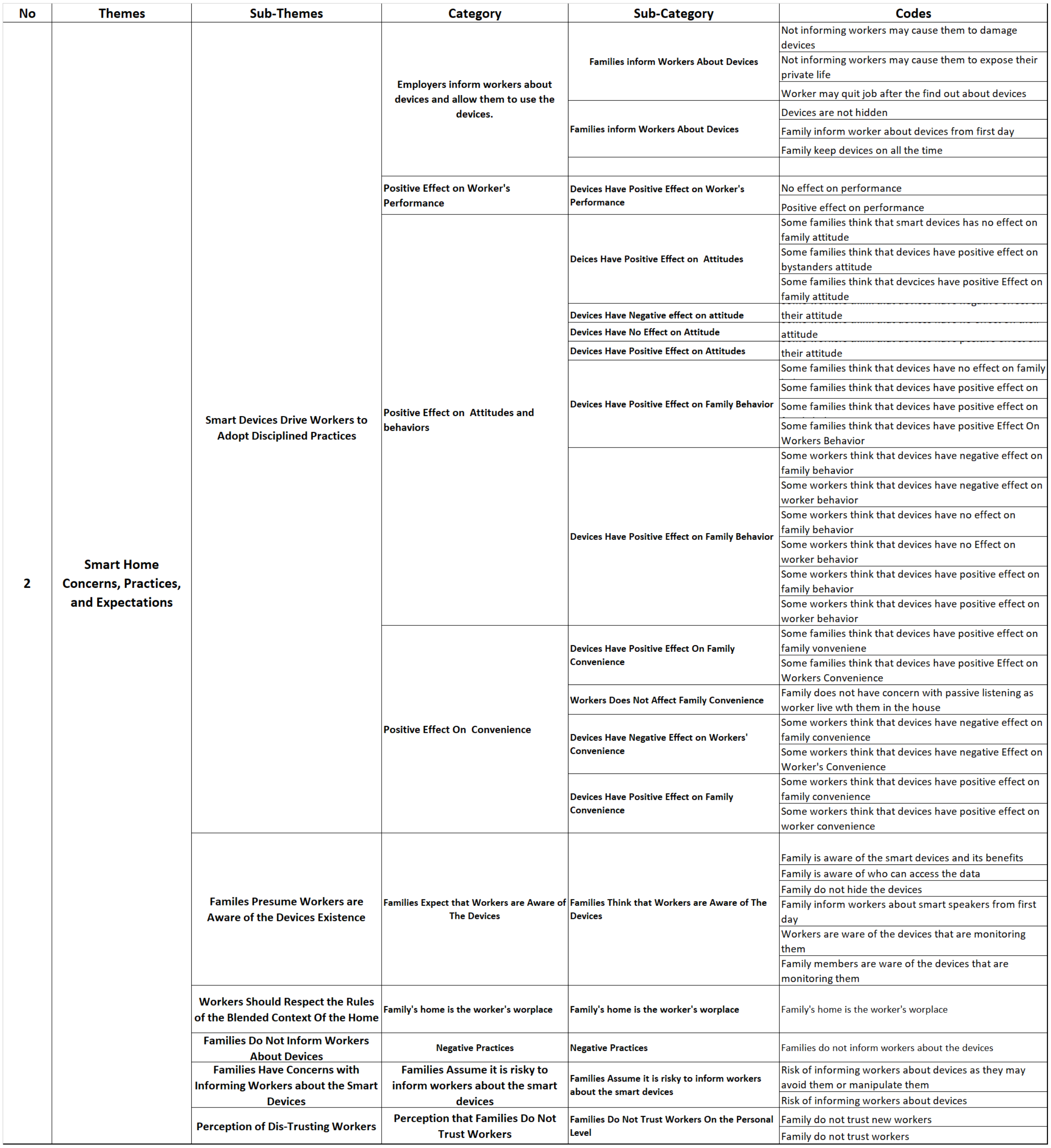
Appendix- B

Figure 10: Code book of Themes and Codes-1



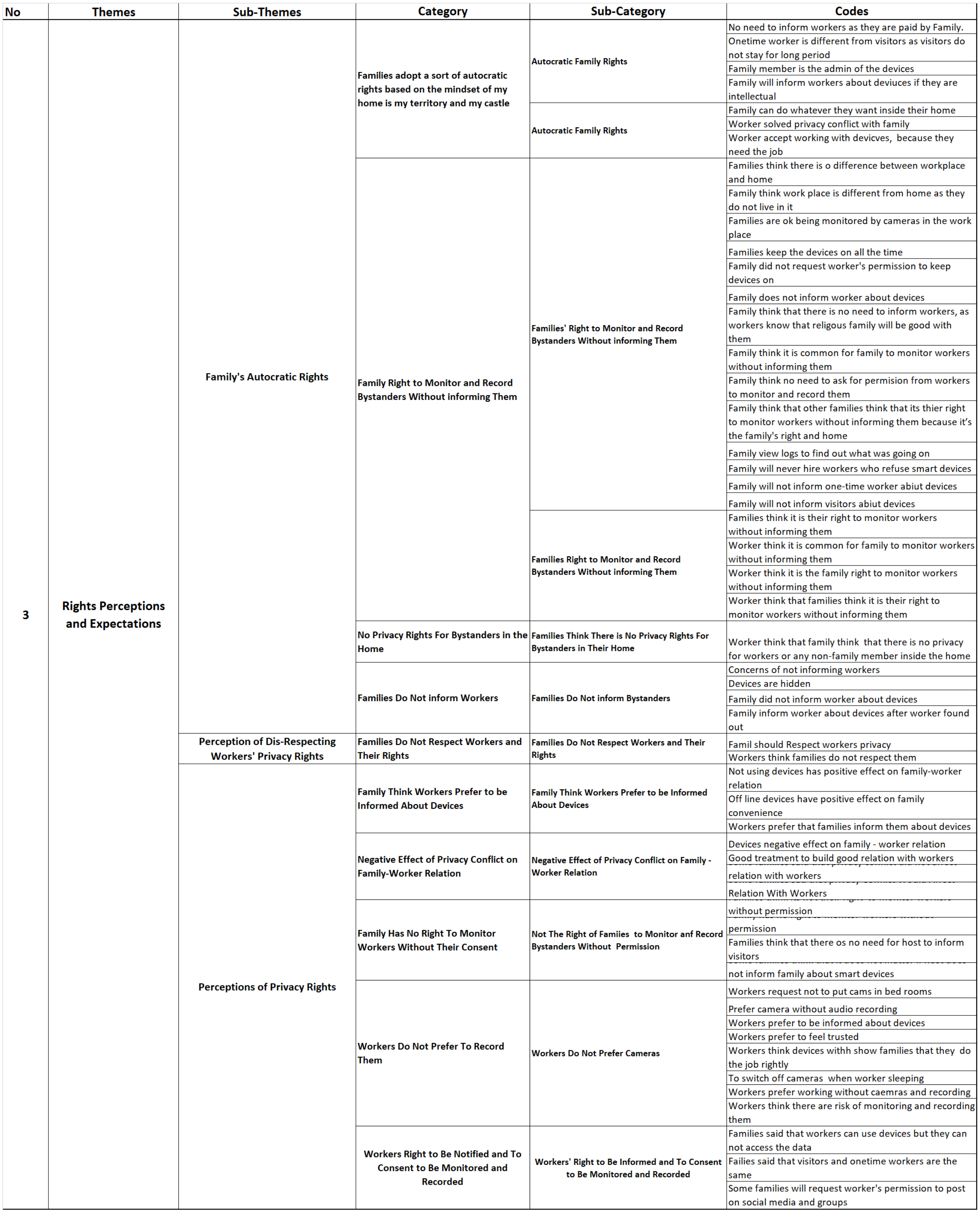
No	Themes	Sub-Themes	Category	Sub-Category	Codes
1	Weak Public Awareness	Weak Awareness of Smart Home and Smart Devices	Basic Understanding of Smart Home & Smart Devices	Worker's Basic Understanding of Smart Home and Devices	Workers' awareness of smart devices and functions
					Worker's awareness of who can access data
					Worker has worked with multiple devices.
					More than 3 months of experience
					Workers' understanding of what smart devices are
					Workers' understanding of what smart homes are
				Families' Basic Understanding of Smart Home and Devices	Family's awareness of smart devices functions
					Family's understanding of smart devices are
					Family's understanding of smart homes are
			Need For Public Awareeness About Smart Devices	Need For Public Awareeness About Smart Devices	they see them
					Family did not consider effect of devices on privacy
					contract negotiation
					Agencies do not offer information about smart devices
					workers and families about smart devices and smart
				Need For Public Awareeness About Smart Devices	about smart devices
					negotiations
					about smart devices
					about smart devices
		Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies	Limited public information	Limited public information abour smart technologies	Recriutment agencies provide limited information about smart tehcologies
		Weak Competence of Managing Smart Devices	Weak Awareness of Devices Functions	Workers' Weak Awareness of Devices Functions	Workers' weak awareness of smart devices functions
					Workers' weak awareness of who can access the data
				Families' Weak Awareness of Devices Functions	Family's weak aware of smart devices functions
					Family's weak awareness of who can access data
					Family weak awareness of devices functions Before buying devices
					Family weak awareness of smart devices
					Family hides devices
2	Smart Home Concerns, Practices, and Expectations	People are Mostly Concerned about Audio/Visual Data Collection	Cameras Are the Most Used Devices	Cameras are mostly used to monitor people inside home	Workers are monitored with Cameras
				Families use cameras to monitor workers	Families use cameras to monitor workers
			Family Rarely Checks Data and Logs	Families' Low Rate of Checking Data and Logs	Family checks data very often
					Devices add cost load on families
					Family rate of data check declined by time.
					Family rarely checks data.
			Basic Understanding of Privacy	Basic Understanding of Privacy	Family Privacy is not to have devices or bystanders inside
					Workers' Privacy is not to monitor them
				Basic Understanding of Privacy	Family's privacy is not to be monitored or recorded
					monitored
			Video/Audio Recording	Video/Audio Recording	Workers are Concerned about Video and/or Audio Recording
		Workers Presence in the Home Negatively Impacts Family's Privacy	Workers Presence Affects Family's Privacy	Workers Presence Has Negative Effect On Family Privacy	Workers think that their presence in the home has negative effetc on families' privacy
		Smart Devices Drive Workers to Adopt Disciplined Practices	Employers inform workers about devices and allow them to use the devices.	Worker use devices, but can not access data	Worker can use devices, but access data.
				Families inform Workers About Devices	Family inform worker about devices
					Family inform workers About Devices after they saw them
					Family inform workers that they are not the target of the devices
					Family prefer host to inform them about devices
					Family will inform one-time worker about the devices
					Lawful risks of not informing workers about devices
					Monitor workers after informing them
					Family uses banner to let anyne knows abotu used devices
					Family thinks there is no risk of informing workers about devices

Figure 11: Code book of Themes and Codes-2



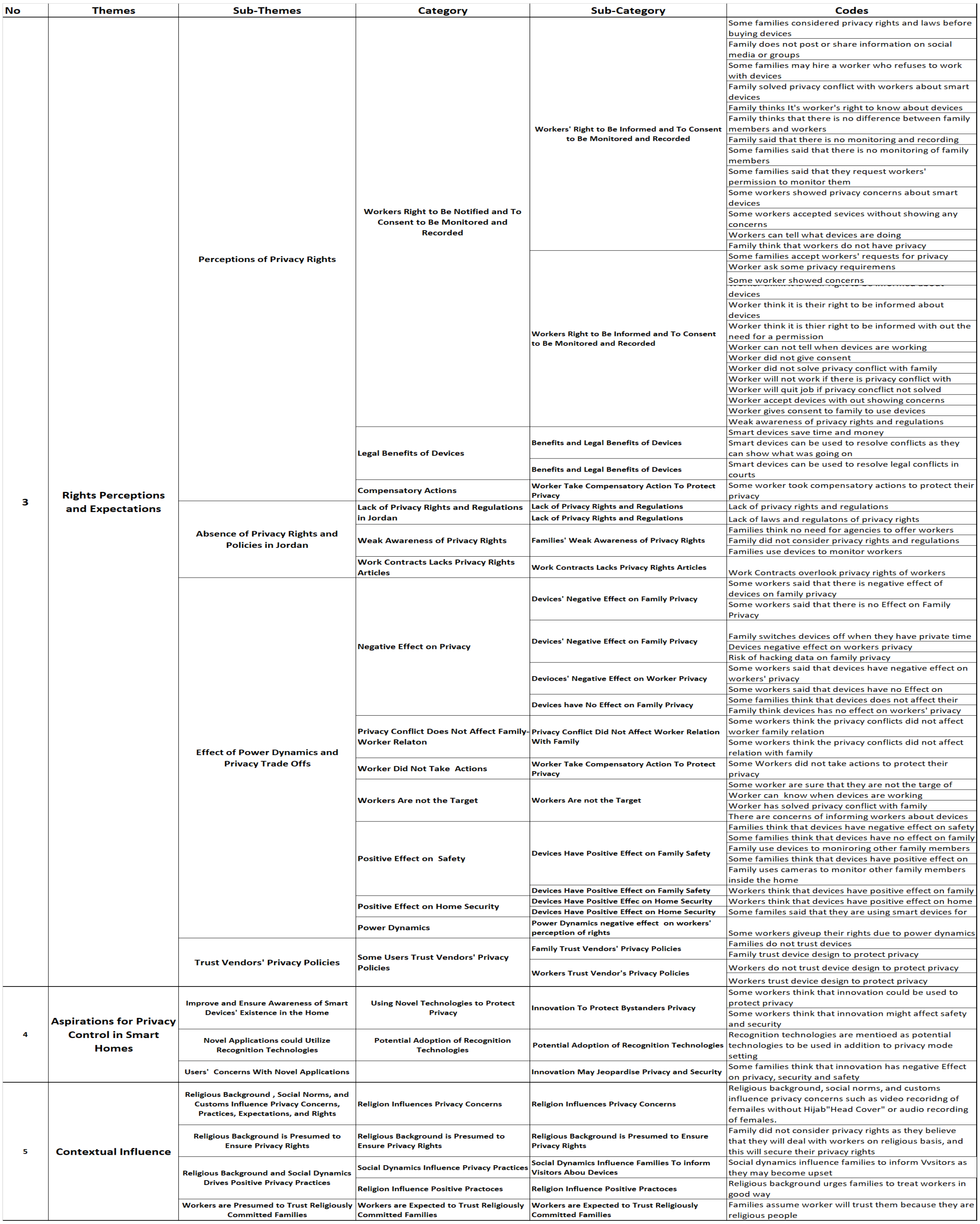
No	Themes	Sub-Themes	Category	Sub-Category	Codes
2	Smart Home Concerns, Practices, and Expectations	Smart Devices Drive Workers to Adopt Disciplined Practices	Employers inform workers about devices and allow them to use the devices.	Families inform Workers About Devices	Not informing workers may cause them to damage devices
					Not informing workers may cause them to expose their private life
					Worker may quit job after the find out about devices
				Families inform Workers About Devices	Devices are not hidden
					Family inform worker about devices from first day
					Family keep devices on all the time
			Positive Effect on Worker's Performance	Devices Have Positive Effect on Worker's Performance	No effect on performance
					Positive effect on performance
			Positive Effect on Attitudes and behaviors	Deices Have Positive Effect on Attitudes	Some families think that smart devices has no effect on family attitude
					Some families think that devices have positive effect on bystanders attitude
					Some families think that devcices have positive Effect on family attitude
				Devices Have Negative effect on attitude	their attitude
				Devices Have No Effect on Attitude	attitude
				Devices Have Positive Effect on Attitudes	their attitude
				Devices Have Positive Effect on Family Behavior	Some families think that devices have no effect on family
					Some families think that devices have positive effect on
					Some families think that devices have positive effect on
					Some families think that devices have positive Effect On Workers Behavior
				Devices Have Positive Effect on Family Behavior	Some workers think that devices have negative effect on family behavior
					Some workers think that devices have negative effect on worker behavior
					Some workers think that devices have no effect on family behavior
					Some workers think that devices have no Effect on worker behavior
					Some workers think that devices have positive effect on family behavior
					Some workers think that devices have positive effect on worker behavior
			Positive Effect On Convenience	Devices Have Positive Effect On Family Convenience	Some families think that devices have positive effect on family vonveniene
					Some families think that devices have positive Effect on Workers Convenience
				Workers Does Not Affect Family Convenience	Family does not have concern with passive listening as worker live wth them in the house
				Devices Have Negative Effect on Workers' Convenience	Some workers think that devices have negative effect on family convenience
					Some workers think that devices have negative Effect on Worker's Convenience
				Devices Have Positive Effect on Family Convenience	Some workers think that devices have positive effect on family convenience
					Some workers think that devices have positive effect on worker convenience
		Familes Presume Workers are Aware of the Devices Existence	Families Expect that Workers are Aware of The Devices	Families Think that Workers are Aware of The Devices	Family is aware of the smart devices and its benefits
					Family is aware of who can access the data
					Family do not hide the devices
					Family inform workers about smart speakers from first day
					Workers are ware of the devices that are monitoring them
					Family members are ware of the devices that are monitoring them
		Workers Should Respect the Rules of the Blended Context Of the Home	Family's home is the worker's worplace	Family's home is the worker's worplace	Family's home is the worker's worplace
		Families Do Not Inform Workers About Devices	Negative Practices	Negative Practices	Families do not inform workers about the devices
		Families Have Concerns with Informing Workers about the Smart Devices	Families Assume it is risky to inform workers about the smart devices	Families Assume it is risky to inform workers about the smart devices	Risk of informing workers about devices as they may avoid them or manipulate them
					Risk of informing workers about devices
		Perception of Dis-Trusting Workers	Perception that Families Do Not Trust Workers	Families Do Not Trust Workers On the Personal Level	Family do not trust new workers
					Family do not trust workers

Figure 12: Code book of Themes and Codes



No	Themes	Sub-Themes	Category	Sub-Category	Codes
3	Rights Perceptions and Expectations	Family's Autocratic Rights	Families adopt a sort of autocratic rights based on the mindset of my home is my territory and my castle	Autocratic Family Rights	No need to inform workers as they are paid by Family.
					Onetime worker is different from visitors as visitors do not stay for long period
					Family member is the admin of the devices
					Family will inform workers about deviuces if they are intellectual
				Autocratic Family Rights	Family can do whatever they want inside their home
					Worker solved privacy conflict with family
					Worker accept working with devicves, because they need the job
			Family Right to Monitor and Record Bystanders Without informing Them	Families' Right to Monitor and Record Bystanders Without informing Them	Families think there is o difference between workplace and home
					Family think work place is different from home as they do not live in it
					Families are ok being monitored by cameras in the work place
					Families keep the devices on all the time
					Family did not request worker's permission to keep devices on
					Family does not inform worker about devices
					Family think that there is no need to inform workers, as workers know that religous family will be good with them
					Family think it is common for family to monitor workers without informing them
					Family think no need to ask for permision from workers to monitor and record them
					Family think that other families think that its thier right to monitor workers without informing them because it's the family's right and home
					Family view logs to find out what was going on
					Family will never hire workers who refuse smart devices
					Family will not inform one-time worker abiut devices
					Family will not inform visitors abiut devices
				Families Right to Monitor and Record Bystanders Without informing Them	Families think it is their right to monitor workers without informing them
					Worker think it is common for family to monitor workers without informing them
					Worker think it is the family right to monitor workers without informing them
					Worker think that families think it is their right to monitor workers without informing them
			No Privacy Rights For Bystanders in the Home	Families Think There is No Privacy Rights For Bystanders in Their Home	Worker think that family think that there is no privacy for workers or any non-family member inside the home
			Families Do Not inform Workers	Families Do Not inform Bystanders	Concerns of not informing workers
					Devices are hidden
					Family did not inform worker about devices
					Family inform worker about devices after worker found out
		Perception of Dis-Respecting Workers' Privacy Rights	Families Do Not Respect Workers and Their Rights	Families Do Not Respect Workers and Their Rights	Famil should Respect workers privacy
					Workers think families do not respect them
		Perceptions of Privacy Rights	Family Think Workers Prefer to be Informed About Devices	Family Think Workers Prefer to be Informed About Devices	Not using devices has positive effect on family-worker relation
					Off line devices have positive effect on family convenience
					Workers prefer that families inform them about devices
			Negative Effect of Privacy Conflict on Family-Worker Relation	Negative Effect of Privacy Conflict on Family - Worker Relation	Devices negative effect on family - worker relation
					Good treatment to build good relation with workers
					relation with workers
					Relation With Workers
			Family Has No Right To Monitor Workers Without Their Consent	Not The Right of Famiies to Monitor anf Record Bystanders Without Permission	without permission
					permission
					Families think that there os no need for host to inform visitors
					not inform family about smart devices
			Workers Do Not Prefer To Record Them	Workers Do Not Prefer Cameras	Workers request not to put cams in bed rooms
					Prefer camera without audio recording
					Workers prefer to be informed about devices
					Workers prefer to feel trusted
					Workers think devices withh show families that they do the job rightly
					To switch off cameras when worker sleeping
					Workers prefer working without caemras and recording
					Workers think there are risk of monitoring and recording them
			Workers Right to Be Notified and To Consent to Be Monitored and Recorded	Workers' Right to Be Informed and To Consent to Be Monitored and Recorded	Families said that workers can use devices but they can not access the data
					Failies said that visitors and onetime workers are the same
					Some families will request worker's permission to post on social media and groups

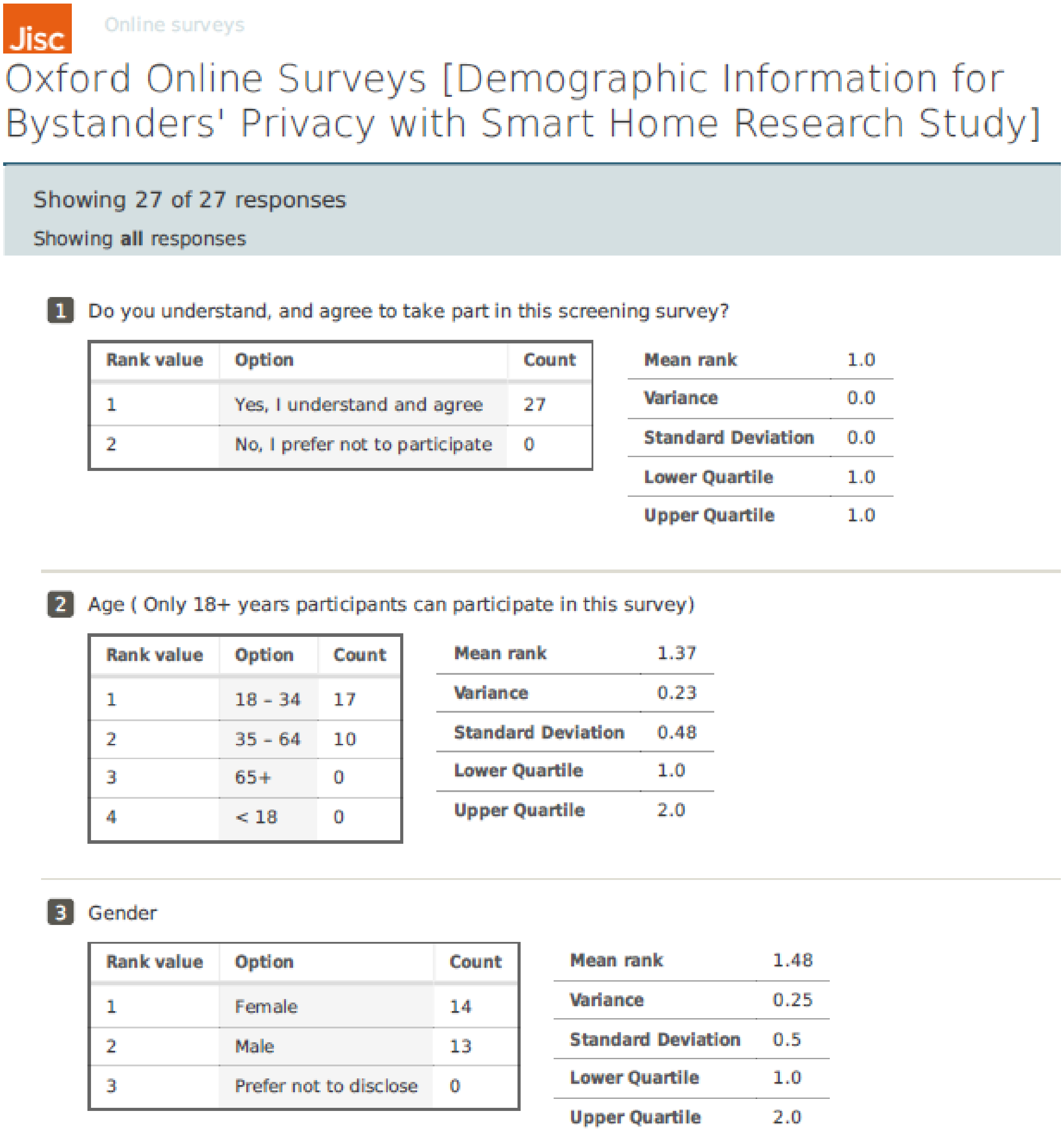
Figure 13: Code book of Themes and Codes



No	Themes	Sub-Themes	Category	Sub-Category	Codes
3	Rights Perceptions and Expectations	Perceptions of Privacy Rights	Workers Right to Be Notified and To Consent to Be Monitored and Recorded	Workers' Right to Be Informed and To Consent to Be Monitored and Recorded	Some families considered privacy rights and laws before buying devices
					Family does not post or share information on social media or groups
					Some families may hire a worker who refuses to work with devices
					Family solved privacy conflict with workers about smart devices
					Family thinks It's worker's right to know about devices
					Family thinks that there is no difference between family members and workers
					Family said that there is no monitoring and recording
					Some families said that there is no monitoring of family members
					Some families said that they request workers' permission to monitor them
					Some workers showed privacy concerns about smart devices
					Some workers accepted sevices without showing any concerns
					Workers can tell what devices are doing
					Family think that workers do not have privacy
				Workers Right to Be Informed and To Consent to Be Monitored and Recorded	Some families accept workers' requests for privacy
					Worker ask some privacy requiremens
					Some worker showed concerns
					devices
					Worker think it is their right to be informed about devices
					Worker think it is thier right to be informed with out the need for a permission
					Worker can not tell when devices are working
					Worker did not give consent
					Worker did not solve privacy conflict with family
					Worker will not work if there is privacy conflict with
					Worker will quit job if privacy concflict not solved
					Worker accept devices with out showing concerns
					Worker gives consent to family to use devices
					Weak awareness of privacy rights and regulations
			Legal Benefits of Devices	Benefits and Legal Benefits of Devices	Smart devices save time and money
					Smart devices can be used to resolve conflicts as they can show what was going on
				Benefits and Legal Benefits of Devices	Smart devices can be used to resolve legal conflicts in courts
			Compensatory Actions	Worker Take Compensatory Action To Protect Privacy	Some worker took compensatory actions to protect their privacy
		Absence of Privacy Rights and Policies in Jordan	Lack of Privacy Rights and Regulations in Jordan	Lack of Privacy Rights and Regulations	Lack of privacy rights and regulations
				Lack of Privacy Rights and Regulations	Lack of laws and regulatons of privacy rights
			Weak Awareness of Privacy Rights	Families' Weak Awareness of Privacy Rights	Families think no need for agencies to offer workers
					Family did not consider privacy rights and regulations
					Families use devices to monitor workers
			Work Contracts Lacks Privacy Rights Articles	Work Contracts Lacks Privacy Rights Articles	Work Contracts overlook privacy rights of workers
		Effect of Power Dynamics and Privacy Trade Offs	Negative Effect on Privacy	Devices' Negative Effect on Family Privacy	Some workers said that there is negative effect of devices on family privacy
					Some workers said that there is no Effect on Family Privacy
				Devices' Negative Effect on Family Privacy	Family switches devices off when they have private time
					Devices negative effect on workers privacy
					Risk of hacking data on family privacy
				Devioces' Negative Effect on Worker Privacy	Some workers said that devices have negative effect on workers' privacy
					Some workers said that devices have no Effect on
				Devices have No Effect on Family Privacy	Some families think that devices does not affect their
					Family think devices has no effect on workers' privacy
			Privacy Conflict Does Not Affect Family-Worker Relaton	Privacy Conflict Did Not Affect Worker Relation With Family	Some workers think the privacy conflicts did not affect worker family relation
					Some workers think the privacy conflicts did not affect relation with family
			Worker Did Not Take Actions	Worker Take Compensatory Action To Protect Privacy	Some Workers did not take actions to protect their privacy
			Workers Are not the Target	Workers Are not the Target	Some worker are sure that they are not the targe of
					Worker can know when devices are working
					Worker has solved privacy conflict with family
					There are concerns of informing workers about devices
			Positive Effect on Safety	Devices Have Positive Effect on Family Safety	Families think that devices have negative effect on safety
					Some families think that devices have no effect on family
					Family use devices to moniroring other family members
					Some families think that devices have positive effect on
					Family uses cameras to monitor other family members inside the home
				Devices Have Positive Effect on Family Safety	Workers think that devices have positive effect on family
			Positive Effect on Home Security	Devices Have Positive Effec on Home Security	Workers think that devices have positive effect on home
				Devices Have Positive Effect on Home Security	Some familes said that they are using smart devices for
			Power Dynamics	Power Dynamics negative effect on workers' perception of rights	Some workers giveup their rights due to power dynamics
		Trust Vendors' Privacy Policies	Some Users Trust Vendors' Privacy Policies	Family Trust Vendors' Privacy Policies	Families do not trust devices
					Family trust device design to protect privacy
				Workers Trust Vendor's Privacy Policies	Workers do not trust device design to protect privacy
					Workers trust device design to protect privacy
4	Aspirations for Privacy Control in Smart Homes	Improve and Ensure Awareness of Smart Devices' Existence in the Home	Using Novel Technologies to Protect Privacy	Innovation To Protect Bystanders Privacy	Some workers think that innovation could be used to protect privacy
					Some workers think that innovation might affect safety and security
		Novel Applications could Utilize Recognition Technologies	Potential Adoption of Recognition Technologies	Potential Adoption of Recognition Technologies	Recognition technologies are mentioed as potential technologies to be used in addition to privacy mode setting
		Users' Concerns With Novel Applications		Innovation May Jeopardise Privacy and Security	Some families think that innovation has negative Effect on privacy, security and safety
5	Contextual Influence	Religious Background , Social Norms, and Customs Influence Privacy Concerns, Practices, Expectations, and Rights	Religion Influences Privacy Concerns	Religion Influences Privacy Concerns	Religious background, social norms, and customs influence privacy concerns such as video recoridng of femailes without Hijab"Head Cover" or audio recording of females.
		Religious Background is Presumed to Ensure Privacy Rights	Religious Background is Presumed to Ensure Privacy Rights	Religious Background is Presumed to Ensure Privacy Rights	Family did not consider privacy rights as they believe that they will deal with workers on religious basis, and this will secure their privacy rights
		Religious Background and Social Dynamics Drives Positive Privacy Practices	Social Dynamics Influence Privacy Practices	Social Dynamics Influence Families To inform Visitors Abou Devices	Social dynamics influence families to inform Vvsitors as they may become upset
			Religion Influence Positive Practoces	Religion Influence Positive Practoces	Religious background urges families to treat workers in good way
		Workers are Presumed to Trust Religiously Committed Families	Workers are Expected to Trust Religiously Committed Families	Workers are Expected to Trust Religiously Committed Families	Families assume worker will trust them because they are religious people

Appendix- C

Figure 14: Survey Details-1



Jisc Online surveys

Oxford Online Surveys [Demographic Information for Bystanders' Privacy with Smart Home Research Study]

Showing 27 of 27 responses

Showing **all** responses

1 Do you understand, and agree to take part in this screening survey?

Rank value	Option	Count
1	Yes, I understand and agree	27
2	No, I prefer not to participate	0

Mean rank	1.0
Variance	0.0
Standard Deviation	0.0
Lower Quartile	1.0
Upper Quartile	1.0

2 Age (Only 18+ years participants can participate in this survey)

Rank value	Option	Count
1	18 - 34	17
2	35 - 64	10
3	65+	0
4	< 18	0

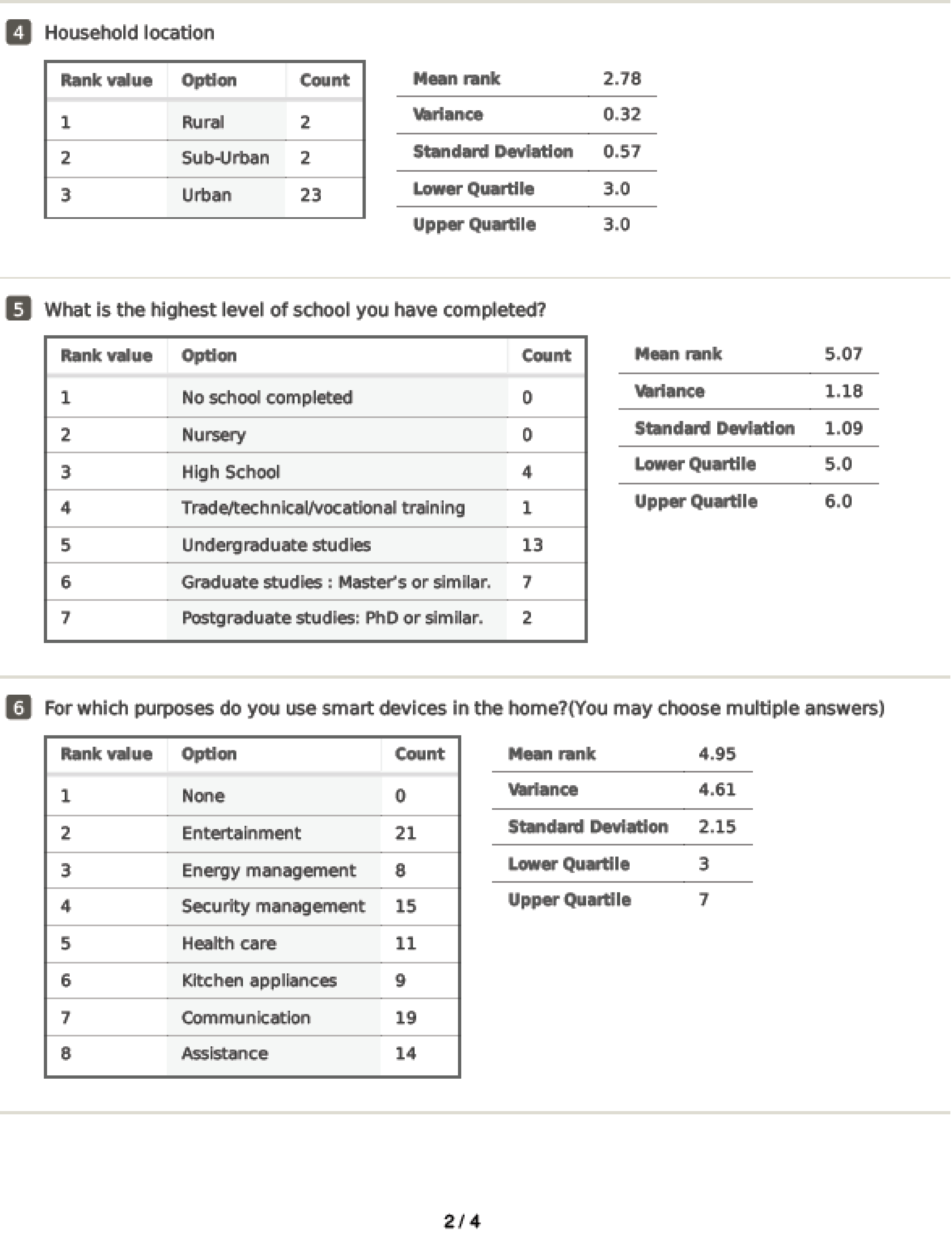
Mean rank	1.37
Variance	0.23
Standard Deviation	0.48
Lower Quartile	1.0
Upper Quartile	2.0

3 Gender

Rank value	Option	Count
1	Female	14
2	Male	13
3	Prefer not to disclose	0

Mean rank	1.48
Variance	0.25
Standard Deviation	0.5
Lower Quartile	1.0
Upper Quartile	2.0

Figure 15: Survey Details-2



4 Household location

Rank value	Option	Count
1	Rural	2
2	Sub-Urban	2
3	Urban	23

Mean rank	2.78
Variance	0.32
Standard Deviation	0.57
Lower Quartile	3.0
Upper Quartile	3.0

5 What is the highest level of school you have completed?

Rank value	Option	Count
1	No school completed	0
2	Nursery	0
3	High School	4
4	Trade/technical/vocational training	1
5	Undergraduate studies	13
6	Graduate studies : Master's or similar.	7
7	Postgraduate studies: PhD or similar.	2

Mean rank	5.07
Variance	1.18
Standard Deviation	1.09
Lower Quartile	5.0
Upper Quartile	6.0

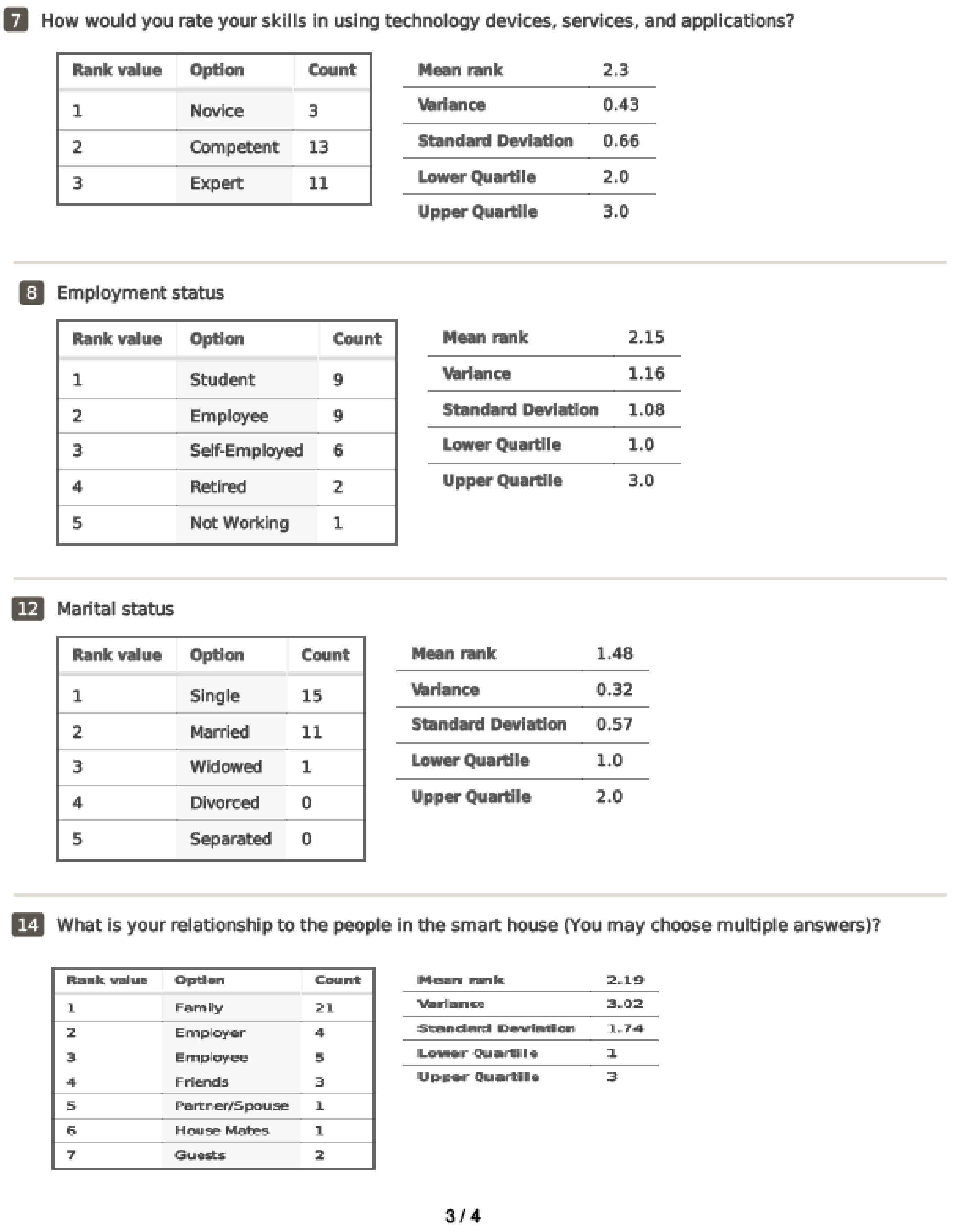
6 For which purposes do you use smart devices in the home?(You may choose multiple answers)

Rank value	Option	Count
1	None	0
2	Entertainment	21
3	Energy management	8
4	Security management	15
5	Health care	11
6	Kitchen appliances	9
7	Communication	19
8	Assistance	14

Mean rank	4.95
Variance	4.61
Standard Deviation	2.15
Lower Quartile	3
Upper Quartile	7

2 / 4

Figure 16: Survey Details-3



7 How would you rate your skills in using technology devices, services, and applications?

Rank value	Option	Count
1	Novice	3
2	Competent	13
3	Expert	11

Mean rank	2.3
Variance	0.43
Standard Deviation	0.66
Lower Quartile	2.0
Upper Quartile	3.0

8 Employment status

Rank value	Option	Count
1	Student	9
2	Employee	9
3	Self-Employed	6
4	Retired	2
5	Not Working	1

Mean rank	2.15
Variance	1.16
Standard Deviation	1.08
Lower Quartile	1.0
Upper Quartile	3.0

12 Marital status

Rank value	Option	Count
1	Single	15
2	Married	11
3	Widowed	1
4	Divorced	0
5	Separated	0

Mean rank	1.48
Variance	0.32
Standard Deviation	0.57
Lower Quartile	1.0
Upper Quartile	2.0

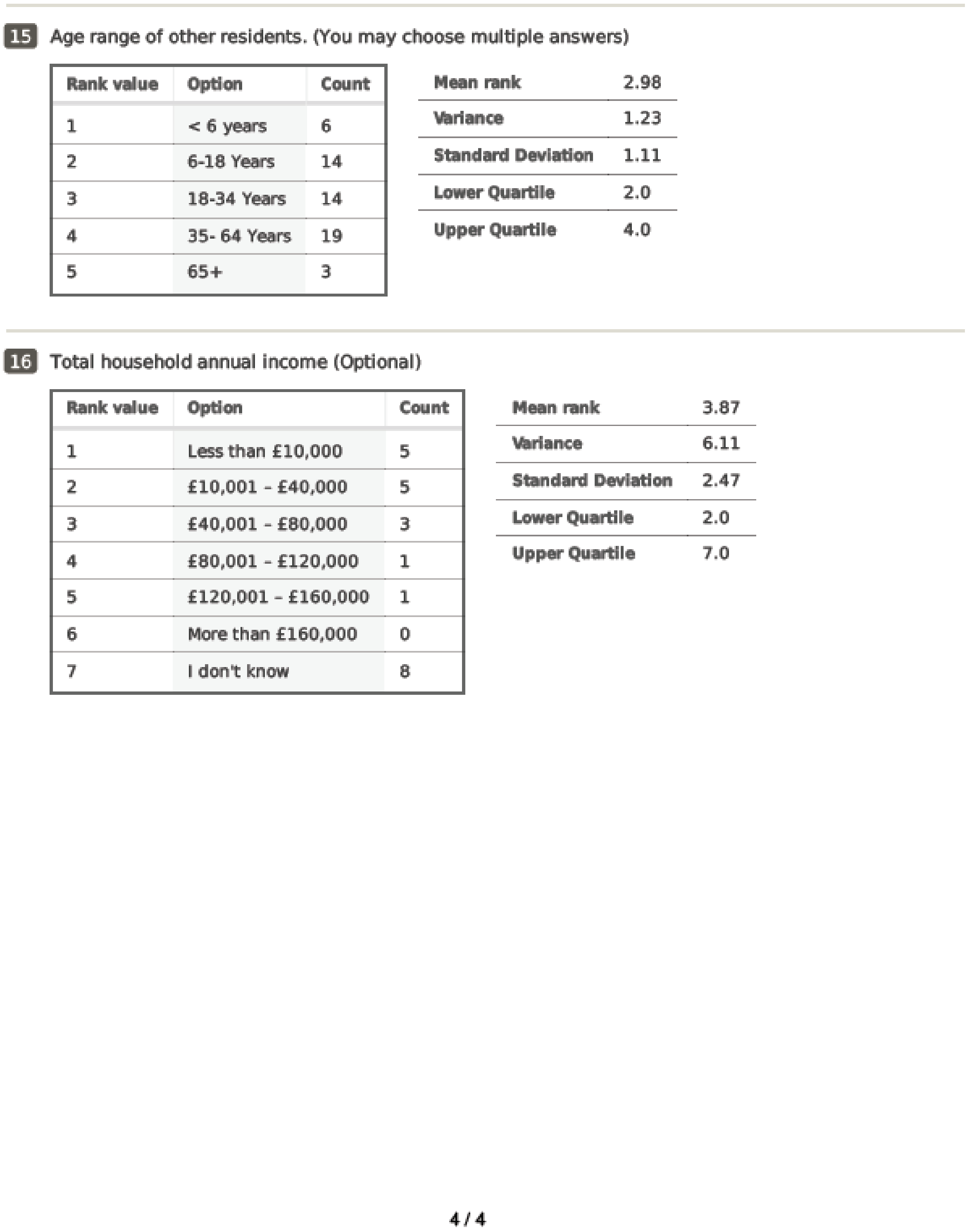
14 What is your relationship to the people in the smart house (You may choose multiple answers)?

Rank value	Option	Count
1	Family	21
2	Employer	4
3	Employee	5
4	Friends	3
5	Partner/Spouse	1
6	House Mates	1
7	Guests	2

Mean rank	2.19
Variance	3.02
Standard Deviation	1.74
Lower Quartile	1
Upper Quartile	3

3 / 4

Figure 17: Survey Details-4



15 Age range of other residents. (You may choose multiple answers)

Rank value	Option	Count
1	< 6 years	6
2	6-18 Years	14
3	18-34 Years	14
4	35- 64 Years	19
5	65+	3

Mean rank	2.98
Variance	1.23
Standard Deviation	1.11
Lower Quartile	2.0
Upper Quartile	4.0

16 Total household annual income (Optional)

Rank value	Option	Count
1	Less than £10,000	5
2	£10,001 - £40,000	5
3	£40,001 - £80,000	3
4	£80,001 - £120,000	1
5	£120,001 - £160,000	1
6	More than £160,000	0
7	I don't know	8

Mean rank	3.87
Variance	6.11
Standard Deviation	2.47
Lower Quartile	2.0
Upper Quartile	7.0

4 / 4