Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households

Wael Albayaydh and Ivan Flechais, *University of Oxford*

https://www.usenix.org/conference/usenixsecurity23/presentation/albayaydh

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households

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

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

Abstract

Smart technologies continue to raise concerns about privacy protection of both households and bystanders who may be targets of incidental or intentional monitoring. Domestic workers are an example of bystanders in smart homes who experience complex power dynamics and can be subjected to exploitative practices that are further facilitated through smart technology. Such power dynamics are rooted in complex social norms and customs, religious beliefs, and economics. While past research has focused on Western contexts to explore how smart technologies and power dynamics affect privacy of households and smart home bystanders, there is a limited understanding of the impact of such factors within non-Western contexts.

This paper presents the findings from 30 interviews with smart device users and bystanders (households, and domestic workers), policy makers, and human and civil rights activists to explore smart home power dynamics in the Muslim Arab Middle Eastern (MAME) context of Jordan. We uncover how asymmetric socio-economic power dynamics between households and domestic workers influence smart technology privacy concerns, practices, and rights perceptions. Drawing on the findings of this study, we present some recommendations for interventions to balance asymmetric power dynamics, to improve bystanders' agency and privacy protection, and to prevent technology exploitation.

1 Introduction

This paper investigates the impact of power dynamics on privacy in smart homes in the Muslim Arab Middle Eastern (MAME) context of Jordan. While existing research primarily focuses on Western perspectives and the perspectives of households and bystanders [14, 19, 24], there is limited understanding of power dynamics and privacy concerns in smart homes outside of Western contexts. Our study fills this gap by providing insights into the Jordanian context and exploring how power dynamics influence privacy concerns and practices of households and bystanders in smart homes. Following the definition provided by Yao et al. [98], *" bystanders are individuals who do not own or directly utilize the smart devices, but they may still be involved in the usage of smart home devices. This category includes other family members who have not purchased the devices, as well as guests, tenants, and passersby".*

We are seeking to answer the research question: **"How do socio-economic power dynamics affect the privacy of households and domestic workers in Jordanian smart homes?"**. We provide an overview of user and bystander privacy in smart homes and summarize the existing data protection regulations in Jordan in Section 2. Our research approach (Section 3), consists of 30 semi-structured interviews with various stakeholders in Jordan, including households, domestic workers, experts, policymakers, and activists.

We present our findings in two main categories: the first is *Smart Home Power Dynamics* (Section 5.1), which explores how power dynamics in smart homes are influenced by contextual factors such as norms, customs, religion, and economic status. We investigate the impact of these power dynamics on household-worker relationships, privacy concerns, and practices with smart devices. We also identify the vulnerability of women workers and foreign workers who are particularly affected by power dynamics and exploitation through smart technology. The second category, *Perspectives on Mitigating Smart Home Power Dynamics* (Section 5.2), delves into the current data protection landscape in Jordan, including the lack of explicit data protection laws and plans for new legislation. We then explore participants' perspectives on balancing power dynamics in Jordanian smart homes.

Overall, our research contributes to a better understanding of power dynamics and privacy concerns in smart homes, particularly in the Jordanian context. It offers insights (Section 6) that can inform the development of policies, contextual, and technical interventions to enhance privacy protection, mitigate power differentials, and prevent exploitation.

2 General Overview

2.1 Context Overview & Similar Studies

Jordan is a southwest Asian Arab country in the Middle East with a predominantly Muslim population, middle eastern customs and social norms, and a moderate Islamic background [53]. In recent years, it has seen an increasing adoption of smart devices (e.g., cameras, smart speakers, and smart lights)[1]. Jordanian culture is deeply rooted in Arabic and Islamic elements, with traditions, habits, and social values derived from religion, family, and social class [1, 38, 85]. Jordan is a patriarchal society where men hold power and resources, while women often face marginalization and social stigma for deviating from expected behavior [48, 72].

In Jordan, domestic workers (e.g. maids, nannies, and babysitters), are predominantly women and come from Far East and African countries (e.g., Ethiopia, Bangladesh, Sri Lanka, Philippines, Kenya, and Indonesia). These foreign domestic workers encounter many challenges, including limited agency and rights, long working hours, low wages, and restrictions on freedom of movement without their employer's permission [54, 92]. Unfortunately, there is a lack of effective oversight from both local authorities in Jordan and the consulates of the domestic workers' home countries regarding the status, rights, and difficulties faced by these workers.

Research specifically examining smart home power dynamics in Jordan or the wider MAME region is limited. Few studies indicate that socio-economic power dynamics in Jordanian smart homes tend to favor households, often disregarding the rights and preferences of domestic workers and leaving them vulnerable to exploitative practices facilitated by smart home technologies [6]. Moreover, few studies have explored privacy concerns and their impact on the acceptance and usage of smart home devices in Jordan [4, 5, 75]. Shehadeh et al. [89] found that users in Jordan have limited knowledge about smart homes, with cost and privacy concerns being significant factors influencing their decision to purchase and use devices. Aleisa et al. [7] reported that users often overlooked privacy concerns in favor of convenience, while Almutairi et al. [8] identified awareness as a privacy challenge in smart home settings in Saudi Arabia.

2.2 Privacy Concerns of Users and Bystanders With Smart Homes

Smart devices are becoming an integral part of the domestic environment, and it can be difficult to find out whether or how much data these smart devices are collecting about users. Prior studies have explored users' privacy concerns and expectations with smart home devices [2, 14, 52]. Other studies argue that this uncontrolled data collection [20, 96] can threaten not only user privacy, but also that of smart home bystanders who are generally not aware of the presence or purpose of smart devices. Bernd et al. [19] specifically investigate the impact of smart devices on nannies and propose some solutions to support privacy protection of this user group. Other research studies have explored bystander concerns with smart homes to study bystanders' ability to control data collection [86, 87, 87].

Kraemer et al. [65] discuss how socio-cultural dynamics impact the control and use of smart devices. Supporting this view, other researchers argue that user concerns about privacy of smart homes are dependent on contextual and situational factors [36, 39, 67]. Other studies explore how asymmetries in user knowledge and experience, in addition to the power dynamics between users, can generate privacy impacts in the smart home context [12, 30]. Finally, Yao et al. [97] point out that the context of smart homes, the inter-personal relations among users, and the asymmetric socio-power dynamics between users and bystanders can complicate privacy practices and protection, and show that smart home designs are biased toward protecting households.

2.3 Power Dynamics in the Smart Home

Smart homes collect a range of data such as audio-visual, location, behavioural, and environmental data. This can be stored locally or in the cloud, broadcast to other devices, and used more widely by service providers which can lead to privacy concerns. Smart devices have been shown to highlight asymmetries in knowledge, experience, and socio-economic power dynamics among users, and that these imbalances can produce different privacy vulnerabilities in the smart home context [18, 30]. Many researchers argue that privacy concerns are influenced by contextual and situational elements [6, 67]. Lau et al. [66] argue that asymmetric socio-economic power dynamics among users increase privacy tensions and limit users' agency in the home, and they argue that smart home devices should have guest modes. Bernd et al. [19] discuss that many workers leave smart home device deployment decisions to households. Geeng and Roesner [37] show that owners of smart devices generally do not consult with cohabitants prior to installation due to cohabitants' passivity, and asymmetric power dynamics among them. Albayaydh et al. [6] discuss privacy concerns of bystanders from a non-Western perspective and found that weak awareness, asymmetric power dynamics, contextual influences, and lack of regulations are the main factors influencing privacy concerns.

Research on privacy concerns in smart homes [51, 61, 84] reveals that bystanders often share their data despite having control over it due to a sense of inability to object. Cultural factors also influence bystanders' privacy protection [84]. Power dynamics and Contextual Integrity (CI) play a role in negotiating norms in specific contexts [17, 22]. Power imbalances among users reduce rights for powerless individuals [71, 73], and such vulnerabilities have been observed in employer-employee relationships, impacting worker performance and

[1] Growth of smart devices in Jordan, Jordan Digital Strategy

satisfaction [13, 68, 94].

Apthorpe et al. [10] discovered that smart devices impact power dynamics in smart homes related to household environment management. However, conflicts can arise as smart technology enables surveillance, leading to distrust and disagreements over device use. The control over devices within the home can indicate existing interpersonal and socio-cultural dynamics [37, 55]. Imbalances in device control can enable domestic abuse in extreme scenarios and make children targets or bystanders to data collection [35, 69]. To protect bystanders' privacy in smart homes, various proposals have been made, including detecting hidden cameras [70, 81] and signaling data collection or transmission [74, 83]. However, these technical approaches are limited due to user distrust in companies [62, 102]. Other ideas include improving awareness and fostering transparent discussions about device usage among households and bystanders in the home [6, 99].

2.4 Privacy Regulations in Jordan

Our review of Jordanian privacy rights, Jordan's Telecommunications Law – Article 71[2], Cyber-Crime law[3], Labour law[4], Penal-code[5], and related regulations has shown that Jordan does not have explicit privacy and data protection regulations at the time of writing this paper [33]. However, and in conformity with the Universal Declaration of Human Rights article-12 [34] which states that *"Everyone has the right to the protection of the law against privacy interference or attacks"*, Article 18 of the Jordanian constitution[6] [82] provides a broad outline of the right to privacy.

The Ministry of Digital Economy and Entrepreneurship[7] is working on a new data protection draft bill [77] which is inspired by the EU GDPR[8]. The Jordanian Telecom Regulatory Commission (TRC[9]) has issued the "Green Paper of Internet of Things"[10] and said it will support the development of regulations to protect privacy of personal data. At the time of writing, the expectation is that the new data protection law will be enacted in 2023. We do not expect it will address privacy rights in smart homes, but it is expected [90] that the new law will establish a legal framework of personal data protection, data processing and storage mandates. Also, it is expected that the law will not address privacy and data collection in the home, but will state that the ownership of data must be clearly identified, and that data should not be used without the owner's consent and awareness. We also found that Jordanian labour law[4] does not distinguish whether smart homes are domiciles or workplaces for workers.

2.5 Regulation in USA and EU

Bystander privacy concerns with smart homes are not addressed explicitly in either the USA's data protection laws [44] (e.g., CCPA[11], CPRA[12]), or the EU-GDPR [15]. Gilman [40] argues that privacy laws in the USA place the duty of privacy protection on people and leaves businesses and government entities relatively free to collect, analyze, share, and trade personal data. In contrast, the EU's GDPR [50] protects a number of individual rights over personal data; however, GDPR applies to companies, and does not cover smart technology used by individuals in smart homes.

3 Methodology

This paper presents the outcomes of a qualitative study that addresses the research question outlined in Section **??**. Following established approaches in previous qualitative research [6, 18], we conducted a user study utilizing semi-structured interviews. The aim was to explore how smart devices affect, reinforce, and reflect power dynamics between households and their domestic workers in Jordan, as well as the potential role of regulation in mitigating any adverse implications of smart home devices on affected populations. To gain insights into these topics, we interviewed households and domestic workers, and participants involved in policy making: ICT regulators, labor law experts, and human and civil rights activists. Through these interviews, we sought to understand how smart devices could either reinforce or alleviate power dynamics within smart homes, as well as how regulation could address any adversarial effects of smart home devices on households and bystanders in Jordan.

In this paper, "Households" refers to families using smart devices and employing domestic workers, "Workers" refers to domestic workers (i.e., bystanders), "Regulators" denotes ICT policy makers in both public and private sectors in Jordan, "Labour Law Experts" refers to labor law policy makers in both public and private sectors in Jordan, and "Activists" represents human and civil rights activists in Jordan. We labelled our participants as follows: households [H01-H07], domestic workers [W01-W08], regulators [R01-R07], labor law experts [LE01-LE03], and activists [A01-A05].

3.1 Recruitment

We developed a screening questionnaire to identify potential candidates who met our criteria. These criteria included a minimum of 2 years of experience in their role, general

[2] Jordan-Telecommunications Law
[3] Jordan-Cyber Crime Law
[4] Jordan-Labour Law
[5] Jordan-Penal Code – Article 348
[6] Jordan-Constitution of Jordan, Article 18
[7] Jordan-Ministry of digital economy and entrepreneurship
[8] For more details, see: EU-General Data Protection Regulation
[9] TRC: Jordan Telecom Regulator Commission
[10] TRC-Jordan's Green Paper of Internet of Things
[11] CCPA: California Consumer Privacy Act
[12] CPRA: California Privacy Rights Act

knowledge about smart devices, and willingness to participate in interviews and audio recording.

To recruit households and domestic workers in Jordan, we advertised the study on social media groups, reached out to smart device sellers and domestic worker recruitment agencies, and used snowball sampling. We established connections with 12 candidate households and 12 candidate domestic workers. The competence of households and workers in using smart devices was assessed based on Dreyfus' model of skill acquisition [28], which categorizes competence levels as Novice, Competent, Proficient, Expert, and Master. To recruit regulators (i.e., ICT and labour) and human and civil rights activists, we contacted private and public sectors entities in Jordan (i.e., ICT companies, Mobile Operators, The Ministry of Digital Economy and Entrepreneurship[7], Jordan Telecom Regulator Commission[9], Intaj[13], and JOSA[14]). Recruiting regulators and activists posed challenges due to the sensitivities associated with data protection regulation [60]. Data protection can be considered a taboo topic in many private and public organizations [93]. To overcome these challenges, we employed snowball sampling [42], a method commonly used to recruit participants from hard-to-reach groups [11], allowing us to reach 11 ICT regulators, 6 labor law experts, and 9 activists. In total, we established connections with 50 candidates, including 12 households, 12 domestic workers, 11 ICT regulators, 6 labor law experts, and 9 activists.

We reached out to all 50 candidates by email and phone to request and arrange interviews. Of these, 38 expressed interest and completed our screening questionnaire. Consequently, we successfully recruited 30 participants, representing a diverse range of backgrounds: 7 household heads, 8 domestic workers, 7 ICT policy makers, 3 labor law experts, and 5 human and civil rights activists. Together, they collectively represent 15 households, 2 ICT companies, 3 government entities, 2 civil rights organizations, and 2 independent activists. (For participant demographics, see Appendix-1).

In order to avoid any potential harm or ethical concerns and to ensure the freedom of participation for domestic workers, we took measures to exclude participants who were connected to previous participants based on information provided by domestic workers about their employers. For other participants (policy makers and activists) we did not rule out people who might be connected.

3.2 Methodology and Interviews

To address the research question, we conducted semi-structured interviews with 30 participants from July 2022 to November 2022. The study script was structured using the funnel technique [23], which involved starting with general questions and gradually transitioning to more specific ones. This approach helps build rapport with the interviewees while eliciting detailed and relevant information. By initially asking broad questions and progressively delving into specifics, the interviewer ensures comprehensive coverage of relevant topics without overwhelming the interviewee with excessive details at the beginning.

Grounded Theory [91] was selected as the primary research methodology due to its suitability for investigating domains with limited prior exploration. Grounded Theory enables the development of substantive explanatory theories through structured approaches to data collection, analysis, coding, and inductive reasoning. It facilitates a comprehensive understanding of smart home power dynamics and data protection regulations, allowing for the derivation of context-specific recommendations. By examining research problems from various perspectives, Grounded Theory uncovers underlying perspectives, perceptions, and beliefs that drive behaviors, practices, and incidents [25].

We conducted all interviews remotely using Zoom and Facebook Messenger, which we audio-recorded with the participants' oral consent. A trained researcher conducted the interviews in English and Arabic – 23 interviews in English, and 7 interviews in Arabic. The recruitment advertisement clearly requested volunteers to assist with this study, and our participants were happy to volunteer without compensation.

3.2.1 Pilot Study

Three pilot interviews were carried out, each corresponding to one of the three semi-structured interview scripts: households, domestic workers, and policy makers (including regulators, labor law experts, and activists). These helped to ensure the clarity of the questions and detect any issues in the interview scripts beforehand. No significant alterations were made to the interview scripts after conducting the pilot interviews.

3.2.2 Interviews

The study included interviews with households, domestic workers, ICT policy makers, labour law experts, and activists about the use of smart home devices, their impact on privacy, privacy concerns, and data protection regulation in Jordan. The households were asked about the type and use of smart devices, their relation with domestic workers, and their understanding of data protection laws. Domestic workers were asked about their relation with households, their understanding of data protection rights, their use of smart devices, their privacy concerns and practices, and whether they can enforce their privacy preferences and why. ICT policy makers, labour law experts, and activists were asked about the impact of smart devices on privacy, data protection regulations in Jordan, and how to mitigate the adversarial implications of smart devices. To avoid response bias [26] we started with general questions about privacy concerns without mentioning power dynamics, marginalized user groups, and household autocracy.

[13] INTAJ: The Information and Communications Technology Association

[14] JOSA: Jordan Open Source Association

3.2.3 Data Analysis

Following Strauss and Corbin's Grounded Theory [41, 91], we transcribed and analyzed the 30 semi-structured interview scripts using NVivo 12 Pro. The main researcher translated the Arabic interviews, taking utmost care to represent the participants' insights during the translations without any kind of alterations or changes to the participants views and insights.

Author 1 (the primary researcher) and Author 2 (the principal investigator) independently conducted the initial coding of the interview scripts. Throughout the coding process, Author 2 engaged in discussions with Author 1, seeking clarifications, insights, and additional data. Author 1 also annotated the study scripts to provide further context and information. A total of 187 codes emerged from the initial coding. These codes were then applied to the remaining interviews through regular comparisons, and new codes were added where necessary. Subsequently, the two researchers grouped the codes into themes (axial coding) and categories (selective coding) based on the dimensions and properties of each theme. Data saturation (where new data no longer provides significant additional insights) was separately observed for all three participant groups [25, 45].

To verify the credibility of the codebook, Author 2 cross-checked the codes against the interview transcripts. We tested for inter-rater reliability and found that the average Cohen's kappa coefficient (κ) for all codes was 0.88, indicating strong agreement [76]. We also tested the findings for reliability and credibility using triangulation [57] by randomly selecting 7 participants (2 households, 2 workers, 1 regulator, 1 labour law expert, and 1 activist) and asked them to comment on the codes and themes. All participants agreed with the identified categories and themes, and their comments enabled us to identify some additional insights but did not generate new themes. In total, we identified 211 codes which we organised into the categories and themes presented in Section 5.

3.2.4 Research Position and Ethics

Our research focuses on power relationships and their impact on technology use. We consider our positionality [95] and its potential influence on participants and research outcomes. Our overarching research question explores the implications of power dynamics on technology use, particularly regarding ethical values such as freedom, fairness, and accountability. However, we took precautions to ensure that our views did not bias the research process. These precautions included framing our interview guide to avoid leading questions, positioning the study as an exploration of privacy and interpersonal implications of smart technology, and employing two coders to analyze and cross-check the data. We also prioritized preserving the anonymity and privacy of our respondents, while remaining vigilant for any evidence of illegal treatment (which we did not find). As our research is exploratory, we maintained a neutral standpoint and focused on reporting rather than intervening when evidence of potential unfair technology use arose. This research area poses challenges, and future studies may uncover additional instances of exploitation or unethical situations, necessitating standardized research strategies and protocols to identify, assess, and address such issues. We acknowledge the limitations of our study, including the potential influence of our own biases on the results. Despite these limitations, we have confidence in the validity of our findings. To ensure ethical considerations, our study received approval from the University of Oxford Central University Research Ethics Committee (CUREC) [Approval: CS_C1A_021_038]. Participants provided oral consent, and we assured them that their data would be handled with strict confidentiality. Interview scripts were encrypted and stored securely. Finally, participants had the right to withdraw from the study at any point without providing an explanation, and we assured them that their data would not be used if they chose to withdraw. No participants withdrew from the study.

4 Limitations

Similar to all qualitative research studies, this study has some limitations: 1) We conducted all interviews in English, except for 7 interviews that were conducted in Arabic with participants who were unable to communicate in English. Those interviews were translated carefully, but it is possible that some nuances were lost as a result of the language barriers. 2) Qualitative research depends on researchers' skills, and can be influenced by their personal biases [64]. To address this limitation, the primary researcher is a trained researcher on designing and conducting interviews to avoid influencing interviewees, and we outlined our positionality in Section 3.2.4. 3) Self-reporting bias is common in interview research studies [58]. To improve validity and to minimize self-reporting bias in this study, the researchers avoided leading questions and relied on open-ended questions. 4) This qualitative research study is limited by the size and diversity of recruited sample. 5) Due to sensitivity of the study topic, participants might have biased their answers due to different concerns they might have. To mitigate this, we explained to the participants about our security and privacy measures, focusing on how we will encrypt collected data and process it. 6) In common with other qualitative studies, our findings reflect the understanding of our 30 participants and are not generalisable to a wider population. Instead, the focus of such explorations is in gaining a greater understanding of the deeper issues and concerns, and how they relate to one another. Exploring how these findings are generalisable is the subject of future work.

5 Results and Findings

This section presents the findings of our study into smart home power dynamics in Jordan. We present and discuss the findings under two key categories: 1) Smart Home Power Dynamics (Section 5.1), and 2) Perspectives on Mitigating Smart Home Power Dynamics (Section 5.2). See Appendix-2 for a diagram of the identified categories and themes (Fig-1), and a general overview of the codebook (Table-4).

Findings show how smart home devices affect and reflect the power dynamics of household-worker relationships in smart homes in Jordan. In Section 5.1, we investigate the contextual and economic power dynamics in these smart homes, and we highlight how households exploit smart devices to monitor and control their domestic workers who can perceive this as a new kind of modern slavery [43], and how these exploitative technologies shape the privacy concerns and practices of households and their domestic workers. In Section 5.2, we discuss participants' perceptions of privacy rights and data protection in Jordan. Then we present their aspirations for mitigating and balancing the socio-economic smart home power dynamics in Jordan, and how smart technologies could be used to improve user and bystander agency, rather than being an extra tool to exploit them.

5.1 Smart Home Power Dynamics

This section presents smart home asymmetrical power dynamics between households (i.e., employers) and their domestic workers (i.e., employees), and how these power dynamics affect, and reflect household-worker relationships, and their privacy concerns, rights and practices. We further break down this category into the following themes:

5.1.1 Contextual Power Dynamics

Smart Home Social Power Map. Previous studies [47,59,78] discuss power-control theory and the relative power fathers have in patriarchal households, and how these inequalities are reduced in egalitarian households. Supporting these studies, our findings identified different levels of social power within households in Jordan; the highest *first social power level* is attributed to the family-head (usually the father). Our households argued that the family-head has the ultimate power in the home, and the final say in terms of home activities: particularly decisions related to smart devices and hiring domestic workers [H01]. However, they added that –in some cases – the head of the household could be the mother or the elder son [H01]. Moreover, our findings uncover that in many cases the family-head is neither the administrator of the smart devices, nor the direct recruiter of the domestic worker [H05].

The *second social power level* is attributed to household members who recruit the worker, and/or who administer smart devices [H03]. The *third social power level* is attributed to smart home visitors. This user group has limited power in the home, and receives more respect compared to other bystanders such as domestic workers. [H04] explained: *"in Jordan, we have to respect our visitors, we do not record them, we must inform them about our cameras"*. The *lower social power level* is attributed to domestic workers, who usually are unable to discuss working conditions or enforce privacy preferences. [W07] explained: *"they [households] do not discuss with us [workers] about devices and how they use them"*. However, we found that skilled or educated workers receive more respect than illiterate workers, [H02] explained: *"you cannot treat educated nurses like illiterate maids"*.

Household Privileges. Our findings suggest that households perceive themselves as having authority over data collection decisions within their smart homes. We observe that the privacy concerns and practices of users are influenced by contextual social norms and their past experiences with data collection through smart technologies. Domestic workers recognize that households, as the owners of the home, hold the privilege to determine the purpose of using smart devices (e.g., safety, security, entertainment), and the management of collected data [W01]. Both households and workers argue that households, as the employers of domestic workers, possess the right to establish work rules, conditions, and maintain records of workers' activities [H04, W05]. Workers also emphasize that households, as both employers and homeowners, possesses additional power in deciding about devices and data collection [W02]. Furthermore, workers argued that households can collect data about them as they are considered strangers within the home environment [W03]. However, workers acknowledge that privacy expectations in the home may differ from those in a non-domestic workplace, indicating their potential acceptance of video recording without audio [W06]. Activists argued for data protection regulations that address the overlapping privacy expectations between home and workplace settings, facilitating clearer demarcation between the two settings [A03].

Contextual Norms and Religious Background Influence Users' Relations and Privacy Considerations. This section presents how social norms and religious backgrounds influence users' relations, privacy concerns, practices, and considerations with smart devices in Jordan. Regulators argued that contextual norms and religion both influence user relationships and privacy practices. [R04] said: *"some households treat their workers well, and in good ways. As Muslims, [households] have to be good with their workers. They are employees not slaves"*. Moreover, regulators discussed that households assume Muslim workers are trustworthy [R02]; however, another regulator argued that households assume non-Muslim workers are more professional and disciplined [R03]. Regulators also mentioned that social norms and religious beliefs influence positive privacy practices [R02], and households argued that religiously committed households will inform workers about the devices they use [H06]. From their side, workers believe that Muslim households will treat them well, and will respect their privacy [W03]. Moreover, findings uncover that households showed *Autocratic Practices* in Jordan, as households believe that they are free to do whatever they see fit inside their home [H03]. Regulators affirmed that household autocracy is part of the Jordanian culture [R02]. Despite displaying autocratic practices against workers, activists noted that households do not deny workers' basic rights (i.e., shelter, salary, and food). Activists argued that this is a cultural issue, and limiting household power inside the home will require cultural transformation [A05].

Women Experience Reduced Power and Rights. Regulators and activists argued that women are a marginalized group in MAME region [A02,R01], and activists explained that because of this, foreign female workers experience reduced rights and freedom in the home [A02], and also have to compromise privacy rights *"to survive"* the contract period [A02]. One female foreign worker said that she was not allowed to express herself, to go out of the home on her own, or to talk to outsiders, and she was required to wear loose clothes, and hijab[15] [W06]. Activists argued that many people in MAME region consider women a symbol of honor[16], and some households consider female workers' honor part of their own honor. [W04] said: *"my employer does not allow his wife to sit with visiting men, and he asked me not to talk to men"*. Regulators also argued that women are protected through social norms, and religious beliefs in Jordan [R01].

5.1.2 Economic Power Dynamics

Differences in economic status between workers and households represents one of the key power dynamics between the two groups, which can result in undermining workers' ability to defend or discuss their rights with their employers.

Imbalanced Economic Power Dynamics. Activists argued that domestic workers come from low economic societies, thus they accept hard working conditions [A03], and noted that worker-household relations are shaped by these economic imbalances [A04]. Workers confirmed this [W02], and households argued that workers have to accept and respect the rules of the home [H06]. Adding more details, regulators highlighted that wealthy households tend to be more autocratic and stringent with their workers due to the economic disparity between the two groups [R07], *"I believe rich families put a big load on their maids, and they do not talk with them about anything other than the jobs they do"*. Supporting this, workers argued that it is more comfortable to work for average income households compared to higher income ones [W03]. Activists also thought that the financial gap between households and workers is huge, and results in households undervaluing workers' rights and freedom [A05].

Workers Compromise Privacy Rights. As discussed in Section 5.1.1, our findings uncover that workers compromise their privacy rights with smart devices and tend to normalize co-living with them [W07]. Another worker argued that she accepts devices as she wants to avoid conflicts, and to maintain good relations with the household: *"I find it easier to accept that and to avoid conflicts with [the household]"* [W05]. Moreover, workers highlighted *Difficulty in Finding Jobs*, and explained that they trade-off privacy rights and hard work conditions to maintain jobs [W05]. From their side, labour law experts discussed that jobs are becoming scarce, and not easy to find, which results in workers making trade-offs to maintain jobs [LE03], adding that workers tend to be less concerned about privacy when salaries are good [LE03]. A foreign domestic worker [W04] said: *"there are no jobs in my country, I will not lose my job because of cameras"*. Moreover, workers explained that the socio-economic power dynamics are not on their side, and they are unable to discuss or enforce any preferences on households [W05].

5.1.3 Smart Devices Impact Users Relations

This section presents how qualities of household-worker relations (trust, respect, and comfort) are reflected in, and affected by, the growing use of smart home devices in Jordan.

Privacy Concerns. Smart home devices are increasingly used to collect, store and share different types of data about populations in range. Whether these devices are used intentionally or incidentally, they impact the dynamics of household-worker relation from different angles. Worker [W03] said: *"they installed the cameras last year, and I feel that my relation with [the household] is not like before"*. Households expressed that smart devices are becoming an integral part of their daily life [H05], and argued that smart devices could be helpful in mitigating safety and security threats [H06]. Both households and workers highlighted that they are mostly concerned about audio-visual data collection [H01,W07]. Households, and workers mentioned that they are not fully aware of what different types of smart devices might be collecting about them, and where the collected data stored [H02,W02]. Some also expressed uncertainty about potential threats on privacy arising from non audio-visual smart devices: [W02] said *"I do not know how smart heating system, or smart lights could affect me. I am not saying they are not, but I really do not know how"*.

Workers mentioned that they feel uncomfortable being the target of monitoring [W01], and adopt compensatory practices to protect their privacy such as avoiding devices, hiding their face, switching-off devices, or blocking cameras. [W05] said: *"I avoid being close to camera (...) [the family] puts a smart TV in my room, and I put a piece of gum on its camera"*. Workers also pointed out that they prefer working without devices [W08], and claimed that finding jobs without devices is increasingly difficult [W03]. One worker said that he tried to trade-off working with devices for a higher salary, but the family rejected [W03].

Strained Relationships. Our findings indicate that workers have perceptions of distrust, disrespect, and lack of trans-

[15] Hijab: Head covering worn in public by Muslim women.

[16] In MAME, female honor depends on chastity, fidelity, and modesty. Breaching these undermines family and tribal honor.

parency in smart homes [W06]. Workers perceive household use of smart devices inside the home as a sign of distrust [W04], which is influenced by the purpose and location of devices [W07]. Conversely, workers expressed their own distrust towards households due to uncertainty about how collected data is used, particularly when households conceal or refrain from informing them about devices [W01]. Both households and workers acknowledge that smart devices can serve as tools to demonstrate worker trustworthiness and foster trust within households. This can strengthen trust between workers and households, lead to a gradual decrease in monitoring, and blur the boundaries between home and workplace [H06,H07,W05]. On the other hand, households claim they use devices to monitor their homes, rather than intentionally monitoring workers [H02]. Furthermore, while workers feel uncomfortable with smart devices [W04], households argue that they cannot simply turn off the devices to make workers more comfortable [H04]. Workers clarify that they do not expect households to switch off the devices entirely, but rather seek agreement on when, where, and how households use the devices to create a comfortable work setting [W01].

Smart Home Devices Reinforce Asymmetrical Power Dynamics. Similar to what Bernd et. al. [18] discussed, we found that smart devices reinforce power dynamics between households and domestic workers as they provide households with tools to monitor and control workers. Workers argued that households can use collected data against them in many ways (e.g., terminate their contracts, exploit, or defame them) [W04]. However, regulators said that smart devices can be good for the security of both households and workers, and can provide evidence in case of any dispute [R04]. Workers also argued that smart devices could be good as they provide evidence of workers' good attitudes and performance [W04].

5.1.4 Foreign Workers Suffer Contract Slavery

Findings demonstrate the strict practices imposed on workers, with households considering the worker's living quarters as their workplace and disregarding their privacy rights within the home [H03]. Some workers recounted instances where households would use devices to record them without seeking their consent [W01]. Workers argued that these actions constituted intrusive monitoring and made them feel constantly surveilled and controlled [W05]. They cited examples of households using smart devices to monitor them extensively, leading to discomfort and violations of privacy [W05]. Furthermore, one worker expressed concerns that they could be observed during private moments such as changing clothes or removing their hijab[15] [W05]. Another worker described how the household remotely monitored her activities through smart devices [W04]. These practices are indicative of the limited rights of foreign domestic workers in Jordan, and could be seen as signs of contract slavery. Expanding on this, activists argued that foreign domestic workers in Jordan face marginalization, reduced agency, and a lack of privacy rights in their employers' homes [A04]. Some workers said they felt like slaves—particularly female workers [W06]. Labor law experts gave examples of wider mistreatment: some households confiscate workers' passports and Identity Cards, deny vacations, restrict phone and internet access, and confine them to the home for most of their contracts' periods [LE03]. Furthermore, activists highlighted the inability of foreign domestic workers to terminate their contracts without paying back the cost of recruitment to their employers [A02]. This practice sustains a cycle of contract slavery as workers cannot afford these costs [W06]. Consequently, activists explained that workers are forced to endure harsh working conditions and limited rights [A03]. Workers also reported that recruitment agencies in their home countries fail to clarify the financial obligations related to contract termination before their arrival in Jordan [W08].

5.2 Perspectives on Mitigating Smart Home Power Dynamics

In this section we discuss our findings relating to how participants thought the issues surrounding smart home power dynamics should be addressed.

5.2.1 Privacy Rights and Data Protection

Labour law experts argued that workers do not have explicit rights in the home, and are not in a position to discuss and enforce any kind of privacy preferences. They added that workers needed to respect natural household rights in the Jordanian context [LE01]. From their side, households argued that workers have some private places in the home (e.g., bedrooms, and toilets) [H03]. However, workers clearly thought that they do not have any rights in the home [W04].

Lack of Data Protection Regulation in Jordan. As presented in Section 2.4, we found that Jordan lacks explicit data protection laws that address data protection of households, and bystanders in smart homes. Regulators, labour law experts, and activists confirmed that Jordan lacks explicit data protection regulation and policies [A05,LE02,R04]. Moreover, regulators argued that existing laws are outdated [R02], and activists argued that *"privacy is overlooked in existing laws"* [A04]. Regulators mentioned that Jordan applies its cybercrime law[3], and the penal code-Article 348[5] [R04]. They added that privacy – as a general concept – is expressed in the Jordanian constitution[6] [R06]; however, regulators noted that how this relates to data protection is not explicitly addressed in the constitution [R03]. Regulators mentioned that Jordan is about to issue a new data protection law [R07], and argued that the new law is inspired by the EU GDPR[8], and will be tailored to fit Jordanian context [R03].

Economic-Contextual Influences on Privacy Rights. As discussed in Section 5.1.2, and Section 5.1.1, activists mentioned some economic, contextual and religious influences on privacy rights, and highlighted how contextual norms in Jordan ensure the inviolability of home [A01]. Regulators argued that religious background and cultural norms encourage households to inform bystanders (e.g., visitors, and domestic workers) about smart devices, and do not allow households to monitor their workers. [R05] said: *"In my social culture and in Islam it is not allowed"*. In contrast to this, other regulators said the existing culture tends towards an autocratic model, a patriarchal power structure, women being dis-empowered, and individuals in lower social and economic order being disadvantaged [R06].

5.2.2 Balancing Power Dynamics

This section presents our participants' strategies and aspirations to balance smart home asymmetric power dynamics, prevent exploitation, and improve privacy protection.

Awareness is Important For Protection. To mitigate the negative effects of smart home asymmetrical power dynamics, activists mentioned the importance of awareness of different types of smart devices, and of privacy concerns [A04]. They argued that improving awareness can mitigate imbalanced socio-economic power dynamics [A03]. Regulators argued that awareness is crucial to protection as it enables informed attitudes and perspectives, and also emphasized that regulations alone are not enough [R05]. Labour law experts argued that providing social security coverage and health insurance to workers, and educating them could empower them and help mitigate unequal power dynamics [LE02]. When we asked activists, labour law experts, and regulators about how to improve awareness of smart devices and privacy protection, they suggested a variety of channels: social media, mass communications advertisements, informing the education system, and running awareness campaigns [LE02]. Regulators added that both private and public sectors need to cooperate to improve public awareness [R04]. Additionally, activists, labour law experts, and regulators emphasized the importance of awareness guidelines to be available and accessible [A03,LE02,R04].

Consider Household-Workers Needs. Labour law experts argued that using smart devices to monitor domestic workers should be regulated as it is difficult to protect workers' privacy without proper regulations that consider and balance the needs of households and workers [LE02]. In contrast, regulators argued that no law could be adopted that undermined a household's freedom [R03]. Our participants overall felt that balancing the needs of both parties is fundamental to ensure the safety and security of the home, to protect workers' rights and privacy, and to encourage healthy relationships between them [R03,LE02,A02].

Regulation Modernization to Consider Smart Home Power Dynamics in Jordan. As discussed in Sections 5.2.1 & 5.2.1, Jordan currently lacks explicit regulations for data and privacy protection, despite the growing need due to the growing adoption of smart devices[18]. Regulators show optimism about the forthcoming law [R01], which is sharply in contrast with the concerns raised by activists regarding its effectiveness in addressing users' privacy concerns [A01].

Regulators acknowledged the global socio-economic context in shaping legislation in this field [R06], recognizing that Jordan's influence may not be significant enough to drive modifications in smart device designs by vendors [R04]. Activists and regulators emphasized the potential of international cooperation to exert influence on large technology companies, given that domestic regulations alone may not suffice in overcoming their power [A05,R04]. One avenue discussed was the introduction of legal liabilities to encourage manufacturers to enhance smart device design [R05], or the establishment of a global agreement that sets guidelines for manufacturers to improve their designs [R02]. Regulators also stressed the global nature of privacy protection as an overarching goal [R05], but also noted that various different parties hold different views on the direction and extent of privacy discussions and data laws in Jordan [R02]. Pushing back against the notion of privacy being negotiable, activists emphasized that data protection is a fundamental human right [A04]. Regulators clarified that the new law would be distinct from existing cybercrime legislation[3], while complementing the existing legal framework in Jordan [R04,R06]. Additionally, both activists and regulators argued that social norms and religious principles play a vital role in regulating data protection and maintaining a balance in smart home dynamics [A05].

Aspirations For Innovative Solutions. Activists argued that innovation and novel regulation should be accompanied by privacy protection for all users, and that new technologies should aim to minimize the ability of users to breach others' privacy [A03]. Labour law experts suggested using signs to notify people about existing smart devices, and to get consent from bystanders [LE02], and activists suggested agreeing on a global sign or a mark to alert people about existing smart devices [A01]. Moreover, activists said Artificial Intelligence (AI) and new technologies could help support privacy protection [A04]. Critiquing the existing approaches for consent, one of our household participants noted that devices request consent only from the device administrator, who consents on behalf of all other users (passive household members, and bystanders) [H05], which can result in exposing bystanders to devices' data collection activities without their awareness. Another activist suggested devising new ways for workers to complain and report privacy violations [A02], and another proposal was made for a hot-line for workers to report privacy violations [LE01].

6 Discussion and Recommendations

Our findings show that power dynamics can affect and reflect household-worker relationships, and relate to contextual norms, customs, religious background, and economic status of individuals. Here, we propose interventions to rebalance power dynamics, to protect bystanders' privacy, and to improve their agency.

6.1 Summary of Findings

The findings were presented under two main categories. The first category is *Smart Home Power Dynamics* (Section 5.1), where we found that smart home power dynamics relate to the Jordanian contextual norms, customs, religious background of individuals, and their economic status, and how these affect and reflect dynamics of household-worker relationships. We found that domestic workers tend to compromise their privacy rights for received benefits and to avoid conflicts, and we found that foreign domestic workers can suffer contract slavery and are a marginalized group in Jordan. Additionally, we found that female workers experience reduced rights, yet they have some social standing. Moreover, we found that households, and workers are primarily concerned about audio-visual data collection and about the purpose of using devices (e.g., spying and/or controlling of workers). We also found that they are concerned about the potential data gathering activities of other smart devices (e.g., smart lights, smart door locks, smart heating), however, they are not well-informed about the specific categories of data that are being collected by these devices, nor are they aware of the possible consequences of these data gathering activities on their privacy.

The second category is *Perspectives on Mitigating Smart Home Power Dynamics* (Section 5.2), where we found that Jordan lacks explicit data protection laws, and we discuss participants' aspirations for mitigating and balancing asymmetrical smart home power dynamics. As a result, we discuss and we propose a set of recommendations for interventions to mitigate imbalanced power dynamics in Jordanian smart homes, protect privacy, empower domestic workers, and prevent technology exploitation.

6.2 Contextual Interventions

We highlight in Sections 5.1.1 and 5.1.2 the negative impacts of smart home power dynamics on workers' agency and privacy. Given that households are both employers and owners of the home and devices, they possess the greatest power to determine how, where, and when to use these devices. Drawing on the findings from Section 5.2.2, we explore contextual considerations and propose interventions for mitigating smart home power dynamics.

6.2.1 Consider Jordanian Context

Prior studies have shown contextual variations in privacy concepts across different cultures and contexts, indicating the limitations of applying Western research findings to non-Western contexts such as Jordan [3, 80]. These variations are evident in several aspects, including the centralization of decision-making and power, reduced women's rights, and the collective nature of MAME societies compared to the individualistic tendencies in Western societies [16, 79].

However, consistent with previous Western studies [19, 100], our study participants in Jordan emphasized various privacy concerns (e.g., invasive monitoring), while highlighting the impact of socio-economic power dynamics on relationship qualities (i.e., trust, respect, and comfort) between households and workers. It was noted that Jordanian households adopt autocratic practices that restrict workers' agency and limit their freedom of choice, leading workers to compromise their privacy rights for received benefits (i.e., jobs, salary, and shelter). Given these findings, it is imperative to address contextual privacy concerns in Jordan, considering the influence of social, religious, and cultural factors, to mitigate power imbalances and minimize the risk of privacy violations against vulnerable domestic workers. Therefore, we propose a set of recommendations for policy makers and social entities, and manufacturers for better consideration of this context.

Policy Makers to Consider Jordanian Context. As presented in Section 5.2.1, we found that Jordan lacks explicit data protection regulation. Similarly, existing data protection laws in certain countries (e.g., EU-GDPR[8], USA-CCPA[11], Brazil-LGPD[17]) primarily focus on regulating data protection with companies and service providers like Google, rather than explicitly addressing the data protection of smart home users. To address this, we propose for the upcoming regulation in Jordan to leverage the social norms and religious background of Jordanian society. Furthermore, we argue for a more international approach to data protection regulation, considering the increasing adoption[18] of smart technologies worldwide. Achieving this global consensus requires collaborative efforts between governments and international and regional entities such as ITU[19], GSMA[20], TMForum[21], Accessnow[22], and AADR[23].

In addition to these international efforts, another proposal is for new regulations in Jordan also to mandate privacy certifications for smart devices entering local markets. Given the dual nature of the smart home as both a workplace for domestic workers and a residence, it is also imperative for Jordan regulators and law-makers to address the specific needs of marginalized user groups, with a specific focus on women. To tackle this issue, we propose the establishment of a dedicated "privacy advice channel" through concerned authorities and societal entities in Jordan. This channel would provide a platform for workers and household members to seek guidance

[17] LGPD-Brazil Data Protection Law
[18] GSMA Report-Realising the potential of IoT in ME
[19] ITU-The United Nations specialized agency for ICT
[20] For more details, see: The GSMA is a global ICT industry organisation
[21] TMForum-The global industry association for ICT service providers
[22] Accessnow-Organization defends the digital rights of communities at risk.
[23] AADR-The Arab Alliance for Digital Rights.

on privacy matters, make recommendations on good practices, and offer opportunities to report autocratic practices and privacy violations. In addition, we argue for future regulations in Jordan to hold households accountable for their utilization of user data and to establish guidelines for obtaining informed consent, which is necessary for lawful data processing. To serve both user groups effectively, we emphasize the importance of innovative regulations that provide manufacturers with design guidelines that cater to users' needs and concerns. Finally, we note that collaboration among all stakeholders is crucial, including policy makers, manufacturers, and societal entities. Addressing these challenges requires not only regulatory measures, awareness campaigns, and technological advancements but also a fundamental cultural shift towards being more responsible with data.

Manufacturers to Consider Jordanian Context. Outside of the requirements imposed by regulation, it is also important for manufacturers to actively engage with socio-economic power dynamics and privacy concerns of the Jordanian context. Companies should engage more deeply with the principles of privacy by design (PbD) [88] and actively seek feedback from users in Jordan. Building on previous studies [32, 74], we recommend international manufacturers collaborate with local policy makers to establish design guidelines that align with the needs and expectations of users in Jordan, ensuring the inclusion of vulnerable user groups. This approach will help manufacturers strike a balance between business interests, user expectations and contextual privacy needs. Furthermore, companies can deepen their ability to develop context-friendly devices [101] by enhancing their designers' understanding of the contextual concerns in Jordan, and to meet the expectations of domestic workers while enhancing their agency. We argue that there are substantial business opportunities for manufacturers who can tailor their offerings to different markets, including Jordan and wider MAME areas, given the rapid growth of smart technologies[18].

6.2.2 Balance Household-Worker Needs.

Ensuring that households in Jordan will prioritize the privacy needs of domestic workers and create an environment that encourages open communication is a significant challenge. In achieving this, it is important for good practices to be developed for how households can be more respectful of workers' privacy in the context of smart homes. To promote privacy-respecting practices, targeted awareness campaigns should be conducted for households. These campaigns should educate households about privacy risks associated with smart devices and emphasize the importance of understanding and respecting workers' privacy preferences. This will need to be tempered with guidance to navigate the delicate balance between workers' privacy and the safety and security needs of the home, together with accessing support from government authorities and society organizations. Building on previous studies [37, 99], we suggest the leveraging of Jordan's unique social and religious norms – including the customs and obligations relating to good hospitality or Muslim traditions of morality (e.g., kindness, honesty, justice) – to shape how household should engage in proactive communication with workers regarding privacy. By promoting awareness and education, these campaigns should aim to foster an environment of mutual respect and trust, leading to healthier and more equitable relationships within smart homes.

6.2.3 Domestic Workers' Recruitment Agencies to Inform Workers.

The agencies that facilitate the recruitment of domestic workers should also be encouraged to inform and educate workers about privacy risks with smart homes. This can be achieved through tailored booklets and guidelines for workers from different linguistic backgrounds (e.g., Philippines, Indonesia, Ethiopia, and Bangladesh).Recruitment agencies should also provide comprehensive information about Jordanian culture, social norms, religious background, work conditions, and workers' privacy rights. Collaboration between recruitment agencies, local policymakers, and concerned organizations is recommended to develop simple guidelines that achieve a fair balance between privacy of workers and the needs of households. Agencies should also obtain workers' consent through job contracts, provide tailored information to households, and facilitate negotiations between workers and households to mitigate power imbalances and promote healthy relations.

6.3 Technical Considerations & Interventions

Drawing upon the recommendations outlined in Section 6.2.1 and the findings presented in Section 5.2.2, this section discusses some technical considerations and interventions aimed at rebalancing power dynamics.

6.3.1 Innovative Technologies & Multi-User Consent

We propose leveraging the outcomes of innovative technologies, such as Artificial Intelligence (AI) and Machine Learning (ML), to develop algorithms and statistical models that enable smart devices to learn from data collected in the context of application. This would enable the identification of bystanders, decision-making, and actions to support privacy protection and enhance user agency. AI-enabled smart devices can learn to improve privacy over time, understand contextual power dynamics and usage patterns, combine data protection with users' recognition technologies (e.g., user identification and profiling), and hide or delete bystanders' data. Furthermore, we argue for the empowerment of workers through the provision of control over collected data. However, achieving this relies on either obtaining consent from the family or implementing novel regulations in Jordan to enforce it.

As pointed out in other studies [9,56], our findings (Section 5.2.2) highlight concerns arising from single-user consent affecting passive users, which can result in unaware people subjected to data collection. We argue that more research should aim to develop and contextualise multi-user consent mechanisms to fit Jordanian expectations and values. In addition, devices should be designed to prioritize data management across privacy settings, recognizing the challenges highlighted in previous studies [27, 49] such as granularity, complexity, user awareness, interoperability, managing changes in privacy settings, and transparency. One promising approach for this is to adopt and tailor Information Flow Control techniques to monitor the use of bystander data and enforce regulations [21, 31].

6.3.2 Semiotics of Privacy

To facilitate effective user-device communication, we propose leveraging Semiotics[24] to enhance protection of users' privacy. This involves using consistent signs and symbols suitable for Jordanian users and comprehensible for foreign domestic workers. Considering the complexities of accommodating diverse languages, education levels, religious and cultural norms, as well as the potential of AI, ML, and natural language processing, Semiotics can help to advance this domain. For example, smart devices can employ diverse communication channels (e.g., audio, visual) to convey their presence or data collection capabilities to people nearby. Furthermore, we suggest that smart devices could notify the devices or mobile apps of bystanders. This could be achieved through discovery protocols like UPnP[25], SSDP[26], or BLE[27], however, it is crucial to consider the security implications of revealing such information.

6.3.3 Data Minimization and Perturbation Techniques

To enhance privacy protection, we propose the use of data minimization techniques [46] to ensure data is collected only for specific purposes. By reducing the amount of data collected, the risks associated with misuse, exploitation, and exposure of sensitive information can be mitigated. However, it is crucial to ensure that this reduction in data collection does not adversely affect the performance or functionality of smart systems. Combining data minimization with giving bystanders control over the collection and use of their personal data (see Section 6.3.1) empowers workers to make informed decisions and mitigates exploitation. This approach also facilitates a balance between the amount of data collected and the extent to which bystanders are authorized to access and control it [46].

Prior research has shown the effectiveness of data perturbation techniques and differential privacy in protecting datasets [29,30]. We propose to apply perturbation techniques to bystander data by intentionally adding noise or modifying the data to protect users' privacy and prevent exploitation. For instance, smart devices can collect various types of data from the home, such as temperature, humidity, light levels, or audio-visual data, which can be used to infer the presence and activities of users, including bystanders. However, we argue that perturbation of bystander's data makes it harder to accurately infer information about them. Balancing perturbation of data with household security and safety requirements is challenging, and perturbation techniques may not be effective against all types of internal and external privacy breaches. Therefore, we may need to combine them with other privacy protection techniques to ensure robust privacy protection [29, 30]. Finally, our overarching recommendation remains that designing innovative smart technologies should follow established principles of responsible innovation (RI) [63].

7 Conclusion

Our study explores smart home power dynamics between households and their domestic workers in Jordan, and makes a number of recommendations to help balance smart home power dynamics, to prevent households from using smart technologies to exploit powerless domestic workers, to improve domestic workers' agency, and to protect their privacy.

The study identifies power differentials and household privileges, and how socio-economic power dynamics affect and reflect users' relations qualities (i.e., trust, respect, and comfort) in the home. The study reveals that foreign and women domestic workers can suffer contract slavery, and are marginalized group in Jordan. The study notes perceptions of privacy rights and data protection, and presented aspirations for interventions to address concerns. The study highlights the lack of explicit data protection regulations in Jordan, and discusses that this has left powerless workers unprotected and subject to imbalanced socio-economic power dynamics in favour of autocratic households who believe they can use smart technologies to monitor and record workers without permission.

Finally, the study proposes and discusses interventions from a variety of contextual, technical, and legal perspectives in Section 6 which taken together, are aimed at redressing the balance of power in smart homes, and to help prevent using smart technologies against powerless domestic workers and similar user groups in the MAME context of Jordan.

Future work will aim to verify our research findings, and to capitalize on them. Areas of interest include: a) studying contextual dynamics and how to balance and leverage them, b) protecting users from external privacy breaches, c) exploring how designers can mitigate privacy risks for powerless users, and d) investigating how policy makers can take into account bystander concerns.

[24] Semiotics-The study of signs, symbols, and their meaning

[25] UPnP- Universal Plug and Play

[26] SSDP- Simple Service Discovery Protocol

[27] BLE- Bluetooth Low Energy

References

[1] Why Do Jordanian Women Stay in an Abusive Relationship: Implications for Health and Social Well-Being - Gharaibeh - 2009 - Journal of Nursing Scholarship - Wiley Online Library.

[2] ABDI, N., RAMOKAPANE, K. M., AND SUCH, J. M. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants.

[3] AHMED, S. I., HAQUE, M. R., CHEN, J., AND DELL, N. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction 1*, CSCW (Dec. 2017), 1–20.

[4] AL-ALAMI, H., HADI, A., AND AL-BAHADILI, H. Vulnerability scanning of IoT devices in Jordan using Shodan. pp. 1–6.

[5] AL-HUSAMIYAH, A., AND AL-BASHAYREH, M. A comprehensive acceptance model for smart home services. *International Journal of Data and Network Science 6*, 1 (2022), 45–58.

[6] ALBAYAYDH, W. S., AND FLECHAIS, I. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In *CHI Conference on Human Factors in Computing Systems* (New Orleans LA USA, Apr. 2022), ACM, pp. 1–24.

[7] ALEISA, N., RENAUD, K., AND BONGIOVANNI, I. The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Computers & Security 96* (Sept. 2020), 101897.

[8] ALMUTAIRI, O., AND ALMARHABI, K. Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia. *International Journal of Advanced Computer Science and Applications 12*, 4 (2021).

[9] AMAZON, HELP & CUSTOMER SERVICE., A. T. O. U. Alexa Terms of Use - Amazon Customer Service, Dec. 2021.

[10] APTHORPE, N., EMAMI-NAEINI, P., MATHUR, A., CHETTY, M., AND FEAMSTER, N. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. *ACM Transactions on Internet of Things* (June 2022), 3539737.

[11] ATKINSON, R., AND FLINT, J. Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies.

[12] BALDINI, G., BOTTERMAN, M., NEISSE, R., AND TALLACCHINI, M. Ethical Design in the Internet of Things. *Science and Engineering Ethics 24*, 3 (June 2018), 905–925.

[13] BALL, K. Workplace surveillance: an overview. Kirstie Ball (2010) Workplace surveillance: an overview, Labor History. *Labor History 51*, 1 (Feb. 2010), 87–106.

[14] BARBOSA, N. M., ZHANG, Z., AND WANG, Y. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption.

[15] BASTOS, D., GIUBILO, F., SHACKLETON, M., AND EL-MOUSA, F. *GDPR Privacy Implications for the Internet of Things*. Dec. 2018.

[16] BENAIDA, M., AND ARIF, M. *Differences Between Arab World Culture and British Culture Based on Hofstede Dimensions and Their Impact on Web Design*. Apr. 2013.

[17] BENTHALL, S., AND HAYNES, B. D. Contexts are Political: Field Theory and Privacy. Association for Computing Machinery. ACM. 3.

[18] BERND, J., ABU-SALMA, R., CHOY, J., AND FRIK, A. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. 21.

[19] BERND, J., ABU-SALMA, R., AND FRIK, A. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance,. 14.

[20] BRUSH, A. B., LEE, B., MAHAJAN, R., AGARWAL, S., SAROIU, S., AND DIXON, C. Home automation in the wild: challenges and opportunities. ACM, pp. 2115–2124.

[21] BUGEJA, J., JACOBSSON, A., AND DAVIDSSON, P. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)* (Aug. 2016), pp. 172–175.

[22] BURKE, P. J., Ed. *Contemporary social psychological theories . Center for Internet and Society, Stanford Law School Andreas Katsanevas, Department of Communication, Stanford University*. Stanford Social Sciences, Stanford, Calif, 2006.

[23] CANNELL, C. F., MILLER, P. V., AND OKSENBERG, L. Research on Interviewing Techniques. *Sociological Methodology 12* (1981), 389–437. Publisher: [American Sociological Association, Wiley, Sage Publications, Inc.].

[24] CHOE, E. K., CONSOLVO, S., JUNG, J., HARRISON, B., PATEL, S. N., AND KIENTZ, J. A. Investigating receptiveness to sensing and inference in the home using sensor proxies. ACM Press, p. 61.

[25] CORBIN, J., AND STRAUSS, A. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Nov. 2014. Google-Books-ID: hZ6kBQAAQBAJ.

[26] DELL, N., VAIDYANATHAN, V., MEDHI, I., CUTRELL, E., AND THIES, W. "Yours is better!": participant response bias in HCI. ACM, pp. 1321–1330.

[27] DHUNGANA, D., ENGELBRECHT, G., PARREIRA, J. X., SCHUSTER, A., AND VALERIO, D. Aspern smart ICT: Data analytics and privacy challenges in a smart city. pp. 447–452.

[28] DREYFUS, S. E. A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition. Tech. rep., Feb. 1980. Section: Technical Reports.

[29] DWORK, C., NAOR, M., REINGOLD, O., ROTHBLUM, G. N., AND VADHAN, S. On the complexity of differentially private data release: efficient algorithms and hardness results. ACM, pp. 381–390.

[30] ECKHOFF, D., AND WAGNER, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. 489–516. Conference Name: IEEE Communications Surveys & Tutorials.

[31] ENCK, W., GILBERT, P., HAN, S., TENDULKAR, V., CHUN, B.-G., COX, L. P., JUNG, J., MCDANIEL, P., AND SHETH, A. N. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *ACM Transactions on Computer Systems 32*, 2 (June 2014), 1–29.

[32] ENS, B., GROSSMAN, T., ANDERSON, F., MATEJKA, J., AND FITZMAURICE, G. Candid Interaction: Revealing Hidden Mobile and Wearable Computing Activities. ACM, pp. 467–476.

[33] FAQIR, R. S. A. Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010. 10.

[34] FOUNDATION, U. N. About the Universal Declaration of Human Rights, Curated Article., Dec. 2017.

[35] FREED, D., PALMER, J., MINCHALA, D., LEVY, K., RISTENPART, T., AND DELL, N. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. ACM, pp. 1–13.

[36] GARG, V., CAMP, L. J., LORENZEN-HUBER, L., SHANKAR, K., AND CONNELLY, K. Privacy concerns in assisted living technologies. *annals of telecommunications - annales des télécommunications 69*, 1-2 (Feb. 2014), 75–88.

[37] GEENG, C., AND ROESNER, F. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow Scotland Uk, May 2019), ACM, pp. 1–13.

[38] GHARAYBEH, K. General Socio-Demographic Characteristics of the Jordanian Society: A Study in Social Geography. 10.

[39] GHIGLIERI, M., VOLKAMER, M., AND RENAUD, K. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. T. Tryfonas, Ed., Lecture Notes in Computer Science, Springer International Publishing, pp. 656–674.

[40] Gilman, M. E. Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice. University of Baltimore. 78.

[41] Glaser, B. G., and Strauss, A. L. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, 1967. Google-Books-ID: oUxEAQAAIAAJ.

[42] Goodman, L. A. Snowball Sampling. *The Annals of Mathematical Statistics 32*, 1 (1961), 148–170. Publisher: Institute of Mathematical Statistics.

[43] Gorbacheva, A., and Pestunov, A. On freedom and slavery when using a smart device. *AI & SOCIETY* (Dec. 2022), s00146–022–01606–9.

[44] Group, G. L. International Comparative Legal Guides, 2022. Archive Location: United Kingdom Publisher: Global Legal Group.

[45] Guest, G., Bunce, A., and Johnson, L. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods 18*, 1 (Feb. 2006), 59–82. Publisher: SAGE Publications Inc.

[46] Gurses, S., Troncoso, C., and Diaz, C. Engineering Privacy by Design. K.U. Leuven/IBBT, ESAT/SCD-COSIC.

[47] Hagan, J., Simpson, J., and Gillis, A. R. Class in the Household: A Power-Control Theory of Gender and Delinquency. *American Journal of Sociology* (Jan. 1987). Publisher: University of Chicago Press.

[48] Haj-Yahia, M. M. Can people's patriarchal ideology predict their beliefs about wife abuse? The case of Jordanian men. 545–567. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jcop.20068.

[49] Hoepman, J.-H. Privacy Design Strategies. vol. 428. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 446–459.

[50] Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. The European Union general data protection regulation: what it is and what it means. 65–98.

[51] Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., and Kapadia, A. Privacy behaviors of lifeloggers using wearable cameras. ACM, pp. 571–582.

[52] Huang, Y., Obada-Obieh, B., and Beznosov, K. K. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. ACM, pp. 1–13.

[53] IKEHATA, F. <Special Feature "Toward New Studies on Islamic Moderate Trends">Aspiring to be a Leader of Moderation: A Study on Jordan's Islamic Policy, Mar. 2017.

[54] ILO. Jordan: Regulatory framework governing migrant workers.. Private sector workers vs domestic workers., 2022.

[55] J Kraemer, M., Flechais, I., and Webb, H. Exploring Communal Technology Use in the Home. ACM, pp. 1–8.

[56] Jang, W., Chhabra, A., and Prasad, A. Enabling Multi-user Controls in Smart Home Devices. ACM, pp. 49–54.

[57] Jonsen, K., and Jehn, K. A. Using triangulation to validate themes in qualitative studies. 123–150.

[58] Jupp, V. *The SAGE Dictionary of Social Research Methods*. SAGE Publications, Ltd, 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom, 2006.

[59] Kathleen, L. M., and Eunsil, C. Gender, social class, and women's employment | Elsevier Enhanced Reader., 2017.

[60] Keane, E. The GDPR and Employee's Privacy: Much Ado but Nothing New. *King's Law Journal 29*, 3 (Sept. 2018), 354–363.

[61] Koelle, M., Kranz, M., and Möller, A. Don't look at me that way!: Understanding User Attitudes Towards Data Glasses Usage. ACM, pp. 362–372.

[62] Koelle, M., Wolf, K., and Boll, S. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. ACM, pp. 177–187.

[63] Koops, B.-J., Oosterlaken, I., Romijn, H., Swierstra, T., and van den Hoven, J., Eds. *Responsible Innovation 2*. Springer International Publishing, Cham, 2015.

[64] Koskei, B. K., and Simiyu, C. Role of Interviews, Observation, Pitfalls and Ethical Issues in Qualitative Research Methods. *Journal of Educational Policy and Entrepreneurial Research* (Oct. 2015).

[65] Krämer, M. Disentangling Privacy in Smart Homes. Privacy. Computer Science Department, University of Oxford.

[66] Lau, J., Zimmerman, B., and Schaub, F. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (Nov. 2018), 1–31.

[67] Lee, L., Lee, J., Egelman, S., and Wagner, D. Information Disclosure Concerns in The Age of Wearable Computing. Internet Society.

[68] Lee, S., and Kleiner, B. H. Electronic surveillance in the workplace. *Management Research News 26*, 2/3/4 (Mar. 2003), 72–81. Publisher: MCB UP Ltd.

[69] Leitão, R. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. ACM, pp. 527–539.

[70] Liu, T., Liu, Z., Huang, J., Tan, R., and Tan, Z. Detecting Wireless Spy Cameras Via Stimulating and Probing. ACM, pp. 243–255.

[71] Lupton, D. Self-tracking cultures: towards a sociology of personal informatics. ACM, pp. 77–86.

[72] Mahadeen, E. *Women and the Media in Jordan: Gender, Power, Resistance*. Gender, Sexualities and Culture in Asia. Springer Singapore, Singapore, 2022.

[73] Manovich, L. Trending: The Promises and the Challenges of Big Social Data. In *Debates in the Digital Humanities*, M. K. Gold, Ed. University of Minnesota Press, Jan. 2012, pp. 460–475.

[74] Marky, K., Prange, S., Krell, F., Mühlhäuser, M., and Alt, F. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. ACM, pp. 83–95.

[75] Mashal, I., Shuhaiber, A., and Daoud, M. Factors influencing the acceptance of smart homes in Jordan. Publisher: Inderscience Publishers (IEL).

[76] McHugh, M. L. Interrater reliability: the kappa statistic. *Biochemia Medica* (2012), 276–282.

[77] Modee, J. New Data Protection Bill, Draft. Ministry of Digital Economy And Entrepreneurship, Jordan., 2021.

[78] Moghadam, V. M. Patriarchy in Transition: Women and the Changing Family in the Middle East. *Journal of Comparative Family Studies* (Mar. 2019). Publisher: University of Toronto Press.

[79] Ourfali, E. Comparison between Western and Middle Eastern Cultures: Research on Why American Expatriates Struggle in the Middle East.

[80] Palen, L., and Dourish, P. Unpacking "Privacy" for a Networked World. Ft. Lauderdale, Florida, USA. Privacy and Trust. *NEW HORIZONS*, 5 (Apr. 2003), 8.

[81] Patel, S. N., Summet, J. W., and Truong, K. N. BlindSpot: Creating Capture-Resistant Spaces. In *Protecting Privacy in Video Surveillance*, A. Senior, Ed. Springer London, London, 2009, pp. 185–201.

[82] PI, H. r. o. p. i. J. State of Privacy Jordan | Privacy International. A study of privacy and surveillance issues in Jordan, 2019.

[83] PORTNOFF, R. S., LEE, L. N., EGELMAN, S., MISHRA, P., LEUNG, D., AND WAGNER, D. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. ACM, pp. 1649–1658.

[84] PRICE, B. A., STUART, A., CALIKLI, G., MCCORMICK, C., MEHTA, V., HUTTON, L., BANDARA, A. K., LEVINE, M., AND NUSEIBEH, B. Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers. 1–18.

[85] PRIVAT, G. A system-architecture viewpoint on smart networked devices. *Microelectronic Engineering 54*, 1-2 (Dec. 2000), 193–197.

[86] PROFITA, H., ALBAGHLI, R., FINDLATER, L., JAEGER, P., AND KANE, S. K. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. ACM.

[87] RASHIDI, Y., AHMED, T., PATEL, F., FATH, E., KAPADIA, A., NIPPERT-ENG, C., AND SU, N. M. "You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography.

[88] SCHAAR, P. Privacy by Design. *Identity in the Information Society 3*, 2 (Aug. 2010), 267–274.

[89] SHEHADEH, A., AND SARHAN, S. JORDANIAN PEOPLE PERSPECTIVE ABOUT SMART HOMES.

[90] SMEX, S. Will the New Jordanian Law Protect Personal Data?, Feb. 2022. Section: News.

[91] STRAUSS, A., AND CORBIN, J. M. *Grounded Theory in Practice*. SAGE, Mar. 1997. Google-Books-ID: TtRMolAapBYC.

[92] TAMKEEN. Tamkeen for Legal Aid and Human Rights is an independent Jordanian non-governmental civil society organization, 2019.

[93] VEIL, W. The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law.

[94] WATKINS ALLEN, M., COOPMAN, S. J., HART, J. L., AND WALKER, K. L. Workplace Surveillance and Managing Privacy Boundaries. 172–200.

[95] WILSON, C., JANES, G., AND WILLIAMS, J. Identity, positionality and reflexivity: relevance and application to research paramedics. *British Paramedic Journal 7*, 2 (Sept. 2022), 43–49.

[96] WORTHY, P., MATTHEWS, B., AND VILLER, S. Trust Me: Doubts and Concerns Living with the Internet of Things. ACM, pp. 427–434.

[97] YAO, Y., BASDEO, J. R., KAUSHIK, S., AND WANG, Y. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. ACM, pp. 1–12.

[98] YAO, Y., BASDEO, J. R., MCDONOUGH, O. R., AND WANG, Y. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction 3*, CSCW (May 2019), 1–24.

[99] ZENG11, E., AND ROESNER, F. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. 19.

[100] ZENG21, E., MARE, S., AND ROESNER, F. End User Security & Privacy Concerns with Smart Homes. 17.

[101] ZHANG, D., GU, T., AND WANG, X. Enabling Context-aware Smart Home with Semantic Web Technologies.

[102] ZHENG, S., APTHORPE, N., CHETTY, M., AND FEAMSTER, N. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (Nov. 2018), 1–20.

Appendix 1 Demographic Information

Table 1: Demographic Information of Domestic Workers

P#	Gender	Age Group	Education	Nationality	Job Type	Competence with Smart Devices	Existing Smart Devices in Home
W01	Female	30-39	Diploma	Philippines	Home Nurse, Full-Time, Lives with Household	Proficient	Smart Camera, Smart Speaker
W02	Male	40-49	BSc	Jordanian	Home Nurse, Part-Time, Not Living with Household	Novice	Smart Camera, Smart TV, Smart Light
W03	Male	20-29	BSc	Jordanian	Home Nurse, Part-Time, Not Living with Household	Proficient	Smart Camera, Smart Door Lock
W04	Female	20-29	High school	Philippines	Baby Sitter, Full-Time, Lives with Household	Novice	Baby Camera, Smart Heating System
W05	Female	30-39	Diploma	Jordanian	Baby Sitter, Part-Time, Not Living with Household	Novice	Baby Camera, Smart Light
W06	Female	20-29	High school	indonesian	Maid, Full-Time, Lives with Household	Novice	Smart Camera, Smart Security System, Smart Light
W07	Female	20-29	High school	Philippines	Maid, Full-Time, Lives with Household	Novice	Smart Camera, Smart Speaker
W08	Female	30-39	High school	Bangladish	Maid, Full-Time, Lives with Household	Novice	Baby Camera , Smart Refrigerator

Table 2: Demographic Information of Households

P#	Gender	Age Group, Head of Family (HoF)	Education Job	Used Smart Devices	Competence with Smart Devices	Domestic Worker Job Type	Worker Nationality, and Gender
H01	Female	40-49 (HoF)	B.Sc. Pharmacist	Amazon Echo Dot, Roku Smart Camera, Samsung Smart TV	Expert	Maid, Full-Time, Lives with Household	Bangladesh, Female
H02	Female	40-49 (HoF)	B.Sc. No Job	Google Home, REOLINK Smart Camera	Proficient	Baby Sitter, Part-Time, Not Living with Household	Jordanian, Female
H03	Male	30-39 (HoF)	B.Sc. System Support Manager	Samrt Camera, LIFEX Smart Light	Expert	Baby Sitter, Part-Time, Not Living with Household	Jordanian, Female
H04	Male	30-39 (HoF)	M.Sc. Finance Manager	Hikvision Camera, Sifely Smart Door Lock	Expert	Maid, Full-Time, Lives with Household	Philippines, Female
H05	Female	20-29 (HoF)	M.Sc. Mechanical Engineer	Merkury Smart Camera	Expert	Nurse, Part-Time, Not Living with Household	Jordanian, Male
H06	Female	40-49 (HoF)	B.Sc. Teacher	REOLINK Smart Camera, LG Smart TV	Proficient	Maid, Full-Time, Lives with Household	Indonesian, Female
H07	Female	30-39 (HoF)	M.Sc. CEO & Business Owner	Amazon Echo Dot, Hikvision Camera	Expert	Maid, Full-Time, Lives with Household	Bangladesh, Female

Table 3: Demographic Information of Policy Makers & Activists

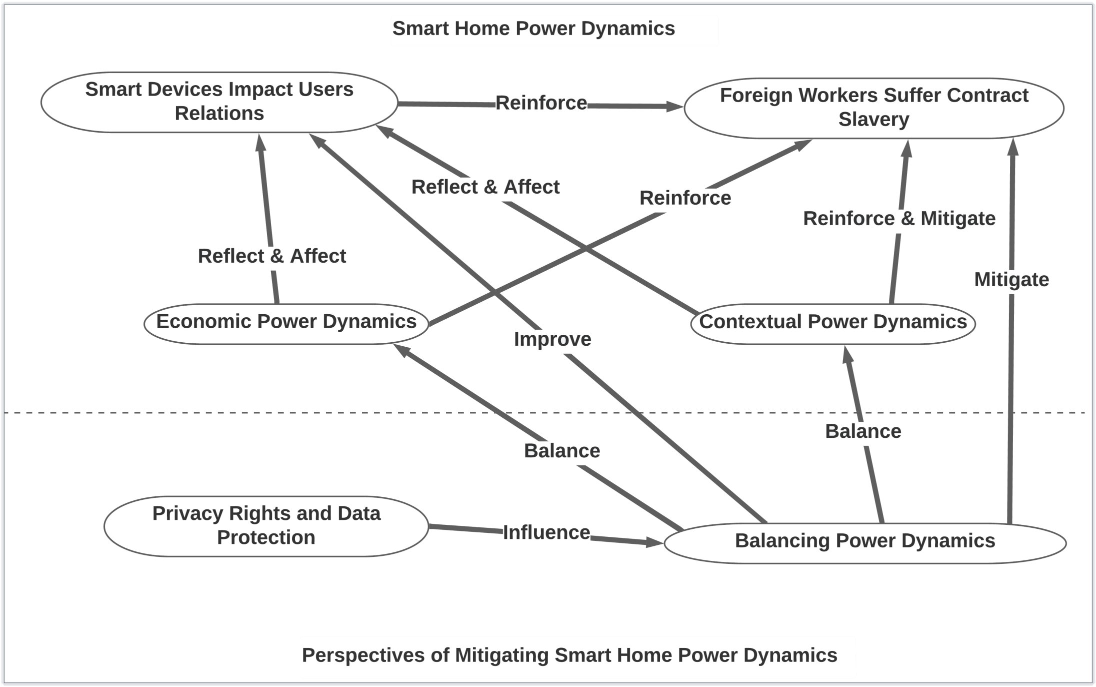
P#	Gender	Age Group	Education	Domain/Field	Organization/Sector	Experience	Entity
R01	Male	46-50	M.Sc.	Regulatory Expert	Private - ICT Sector	12 years	Mobile Operator
R02	Female	31-35	M.Sc.	ICT Regulatory Manager	Private - ICT Sector	8 years	Mobile Operator
R03	Female	25-30	M.Sc.	Regulatory Affairs Team Leader	Private - ICT Sector	6 years	Internet Service Provider
R04	Male	31-35	B.Sc.	ICT Policymaker	MODEE[7]	6 years	Government - Ministry
R05	Male	41-45	B.Sc.	Minister - MODEE	MODEE	12 years	Government - Ministry
R06	Male	46-50	B.Sc.	ICT Regulation Manager	MODEE	14 years	Government - Ministry
R07	Female	31-35	M.Sc.	ICT Regulation Advisor	Telecom Regulatory Commission	6 years	Government - TRC
A01	Female	46-50	B.Sc.	Human & Civil Rights activist	Jordan Open Source Association	8 years	Society NGO Organization
A02	Female	31-35	M.Sc.	Human & Civil Rights activist	Jordan Open Source Association	5 years	Society NGO Organization
A03	Female	36-40	B.Sc.	Human & Civil Rights activist	Amman Center for Human Rights	7 years	Society NGO Organization
A04	Male	25-30	B.Sc.	Human & Civil Rights activist	Independent Activist	4 years	Lawyer
A05	Male	36-40	M.Sc.	Human & Civil Rights activist	Independent Activist	8 years	Lawyer
LE01	Male	46-50	M.Sc.	Labour Law Expert	Ministry of Labour	10 years	Government - Ministry
LE02	Female	31-35	M.Sc.	Labour Law Expert	Ministry of Labour	12 years	Government - Ministry
LE03	Male	46-50	B.Sc.	Labour Law Expert	Lawyer	15 years	Government - Ministry

Appendix 2 - Codebook

Table 4: Summary of Categories and Themes

Categories	Themes	Sub-Themes
Smart Home Power Dynamics	**Contextual Power Dynamics**	Smart Home Social Power Map
		Household Privileges
		Contextual Norms and Religious Background Influence Users' Relations and Privacy Considerations
		Women Experience Reduced Power and Rights
	Economic Power Dynamics	Imbalanced Economic Power Dynamics
		Workers Compromise Privacy Rights
	Smart Devices Impact Users Relations	Privacy Concerns
		Strained Relationship
		Smart Home Devices Reinforce Asymmetrical Power Dynamics
	Foreign Workers Suffer Contract Slavery	Domestic Foreign Workers Are Marginalized Group
		Stringent Practices Towards Domestic Foreign Workers
Perspectives on Mitigating Smart Home Power Dynamics	**Privacy Rights and Data Protection**	Lack of Data Protection Regulation in Jordan
		Economic-Contextual Influences on Privacy Rights
	Balancing Power Dynamics	Awareness is Important For Protection
		Consider Household-Workers Needs
		Regulation Modernization to Consider Smart Home Power Dynamics in Jordan
		Aspirations For Innovative Solutions

Figure 1: Visual Representation of Categories and Themes


Smart Home Power Dynamics
Smart Devices Impact Users Relations
Reinforce
Foreign Workers Suffer Contract Slavery
Reflect & Affect
Reinforce
Reinforce & Mitigate
Reflect & Affect
Mitigate
Economic Power Dynamics
Improve
Contextual Power Dynamics
Balance
Balance
Privacy Rights and Data Protection
Influence
Balancing Power Dynamics
Perspectives of Mitigating Smart Home Power Dynamics