



Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape

Wael Albayaydh and Ivan Flechais, *University of Oxford*

<https://www.usenix.org/conference/usenixsecurity24/presentation/albayaydh>

**This paper is included in the Proceedings of the
33rd USENIX Security Symposium.**

August 14-16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

**Open access to the Proceedings of the
33rd USENIX Security Symposium
is sponsored by USENIX.**

Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape

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

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

Abstract

The proliferation of smart devices fuels privacy concerns, particularly for bystanders—individuals impacted by smart devices beyond their control. Existing research primarily addresses these concerns in Western contexts, with limited focus on Muslim Arab Middle-Eastern (MAME) regions like Jordan. Additionally, there is a scarcity of proposed interventions or assessments for effectively addressing, communicating, negotiating, and remediating privacy issues in these contexts. This study aims to bridge this gap by investigating how a technology probe in the form of a privacy-focused mobile application can serve as an auxiliary tool to support the privacy protection of smart home bystanders in Jordan.

We initiated our research by collaboratively designing the app through four focus groups involving 24 stakeholders. Subsequently, we present and qualitatively evaluate the app's potential for privacy protection with a diverse group of 26 representative stakeholders. While the app is generally well-received, it encounters challenges rooted in broader contextual norms and practices. Our discussion delves into these challenges, offering recommendations to enhance bystander privacy protection in Jordanian smart homes.

1 Introduction

The growing adoption of smart home devices in Jordan¹ has fueled privacy concerns, particularly for bystanders who might remain unaware of data collected by these devices. Smart homes are increasingly adopting smart devices that collect and process personal data, including video, audio, and location information. While these devices enhance convenience and living standards, they simultaneously present substantial privacy risks to users and bystanders. According to Yao et al. [89], "*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,*

and passersby". From this definition, we can see that smart home bystanders are subject to data collection and may be unaware of the existing smart devices or their functions.

The research question addressed is: "*How can we support the privacy protection of domestic workers in smart homes in Jordan?*" This study specifically targets domestic workers in smart homes in Jordan, including babysitters, home nurses, and maids, given the contextual richness in which bystanders are exposed to smart device use by others. As we discuss in §2, privacy research has predominantly focused on Western contexts, with limited attention given to Middle Eastern Muslim Arab contexts like Jordan. These overlooked contexts highlight a gap in knowledge regarding privacy concerns of smart home users and bystanders which can leave them vulnerable to privacy threats and breaches. Additionally, some studies [5, 6] indicated that mobile applications could provide a novel means of supporting bystander privacy protection in smart homes. In this study, we address this gap by co-designing a technology probe mobile application to investigate its potential as an auxiliary tool for enhancing privacy protection for domestic workers in Jordanian smart homes. The terms "domestic workers," "workers," and "bystanders" are used interchangeably throughout the paper. Similarly, "mobile application", "app", and the "probe" are used interchangeably to denote the proposed application.

Employing a mixed-methods approach, this study explores privacy concerns, gathers user insights through co-designing an app, and assesses its potential in supporting privacy protection. The first phase involved focus groups with 24 participants, including households, workers, designers, and app developers. The second phase aimed to evaluate the app with 26 participants, including domestic workers, households, designers, regulators, and heads of recruiting agencies for domestic workers. Both phases were audio recorded, transcribed, and analyzed using Thematic Analysis [49] to systematically look for meaning and identify themes in the data.

The first phase findings, outlined in §4, unveil two key themes: "*Privacy Protection with the App*" and "*Considerations and Challenges*." Participants highlighted privacy con-

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

cerns within domestic settings and the importance of user awareness. They also revealed autocratic dynamics, tensions, and instances of contract slavery² in Jordanian smart homes. Collaborative solutions involving users, regulatory bodies, and companies were seen as crucial. The proposed app features aimed to address imbalanced dynamics and promote an equitable environment. The second theme discusses feasibility, adoption, legal, ethical, and developmental aspects associated with the app. These findings informed the development of the app (cf. §5), encompassing functional and non-functional screens, with elements prepared for future activation.

The evaluation study of the app, detailed in §5.2, reveals two main themes. The first, *"The App Supports Privacy Protection"*, highlights participants' appreciation for the app's role in improving communication between workers and households, empowering workers to make informed choices, and educating stakeholders about smart devices and privacy concerns. They also praised the app's technical aspects, including privacy notifications, user profiling, data segregation, and breach reporting. The second category, *"Barriers Confronting the App"*, discusses challenges such as households limiting worker internet and device access, reluctance to engage in privacy discussions due to power dynamics, workers' limited experience, and potential strategies to address these issues. Additionally, technical challenges like lack of design guidelines and potential privacy breaches were also discussed.

The paper concludes with discussions and recommendations for all stakeholders to inform the design, improve the efficiency, and promote adoption of such tools among smart home users to enhance privacy protection. This paper emphasizes that an app alone is not the sole solution, highlighting the need for interventions from all stakeholders.

2 Background and Related Work

2.1 Context Overview

Jordan, situated in the Middle East, is a predominantly Muslim Arab country characterized by Middle Eastern traditions and social norms, shaped by its moderate Islamic background [43]. Despite its cultural richness, Jordan remains an under-explored region in privacy research, particularly regarding smart home bystanders. By conducting this study in Jordan, we aim to delve into users' privacy apprehensions in this relatively overlooked context. This endeavor not only sheds light on the specific concerns within Jordan but also contributes significantly to the broader field of privacy research in this under-explored region. The insights garnered from this study will enrich the collective understanding of privacy issues and protective measures related to smart home devices, benefitting academic scholarship and practical applications both regionally and globally.

²Contract slavery refers to a form of exploitation akin to modern-day slavery, where workers are bound to work contracts under coercive conditions.

Over recent years, Jordan has witnessed a surge in the adoption of smartphones³ and smart devices¹, including cameras, smart speakers, and lights. Rooted in Arabic and Islamic elements, Jordanian culture reflects traditions, habits, and social values influenced by religion, family, and social class [34, 43, 71]. Prior studies [5–7, 44, 79] have revealed that female foreign domestic workers in Jordanian smart homes, primarily from countries like Ethiopia, Ghana, Bangladesh, and the Philippines, face challenges such as limited agency, data collection by smart devices, and privacy threats. These workers often refrain from discussing privacy preferences and defer to household decisions due to power imbalances favoring households in this context. While previous research [5, 6] suggests the use of mobile applications and innovative technology to enhance the privacy protection of smart home bystanders, we did not find any research exploring the utilization of mobile applications for bystander privacy protection in smart homes, either in Jordan or globally.

2.2 Similar Studies

In our prior studies [5–7], we have delved into privacy concerns and power dynamics of bystanders in Jordan, addressing challenges associated with smart home device design and proposing solutions. Complementing these insights, this study focuses on understanding how auxiliary tools like mobile apps can support protection. By utilizing a mobile app as a technology probe, we assess the effectiveness of such an auxiliary tool in protecting privacy.

While some of this study's findings resonate with some of our prior studies [5–7], and with findings of other studies in both Western and Non-Western contexts [8, 9, 16], further confirmatory research in diverse settings is necessary to complement and validate these insights, enriching the global collective knowledge of smart home privacy concerns. A review of studies in the MAME region, including Saudi Arabia, and Qatar [1, 8, 9], revealed common themes. Users often prioritize convenience over privacy concerns, with awareness emerging as a challenge in smart home environments. It was noted that privacy is context-dependent, gendered, communal, and extends beyond one's lifespan, rooted in religious and cultural norms, and influenced by Islamic faith.

2.3 Bystanders' Privacy Concerns

Smart home devices usually collect data about anyone in range of their sensors whether they are users or not (e.g., neighbours, household members, and domestic workers). Such data collection raises concerns about the privacy of bystanders as well as other members of the household. Prior research has focused primarily on household privacy concerns, preferences, and expectations [41, 90–92]. Other researchers in this space have focused on multi-user privacy concerns [32, 91, 93].

³Jordan: [Smart Phone Penetration Rate](#)

While there is a growing body of literature that explores smart home bystanders [5–7, 17], more needs to be done to elicit, understand, and contextualise different privacy preferences—whether they come from users or bystanders [11, 18, 32, 89].

There is no clear demarcation for how and where someone becomes a bystander to smart devices. People become bystanders in various social and business settings [63, 67]. Generally, bystanders may not be aware of smart devices or their functions [61, 65], and even if they are aware, they often lack adequate understanding of the privacy implications [2, 63]. Additionally, they may lack the social or economic power to negotiate and enforce their privacy preferences [2, 89].

Research has largely focused on bystanders in Western contexts [18, 60], outlining privacy protection strategies such as: a) notifying users about devices; b) permitting users to control data; and c) using privacy-protecting default settings. However, privacy concerns persist, especially since bystanders often remain unaware of smart devices or because control mechanisms are designed exclusively for device owners. Ahmad et al. [2] argue that smart devices should provide privacy assurances for everyone in range, while Markey et al. [63] emphasize that bystanders' limited awareness hinders effective privacy protection.

2.4 Power Dynamics

Smart home devices raise privacy concerns, accentuated by differences in knowledge, experience, and socio-economic disparities among users, and contextual factors further shape these concerns [5, 16, 70], and socio-economic power imbalances amplify privacy tensions and restrict users' agency [56]. Workers often defer device decisions to households, and owners neglect cohabitants due to passivity and power imbalances [17, 32]. Albayaydh et al. [7] highlight factors like limited awareness, asymmetric power dynamics, contextual influences, and regulatory gaps influencing bystanders' privacy concerns. Other studies indicate that bystanders often share their data, believing that they are not in a position to object [41, 53]. Power imbalances, especially in employer-employee relationships, can constrain less powerful users' rights [60, 62]. In smart homes, power dynamics, influenced by device control, mirror existing socio-economic relationships, potentially leading to privacy concerns [11, 32]. Proposals for protecting bystanders' privacy include detecting hidden cameras [58], signaling data collection [63], and fostering awareness through open discussions [5, 93].

2.5 Privacy Controls

Previous research emphasizes the importance of contextualizing privacy preferences within users' daily lives, considering social dynamics [31, 88]. Users express specific privacy preferences when notifications are presented clearly [33, 78], and the use of privacy labels detailing data types for devices has

been suggested [48]. Accountability measures and tools for informed decision-making are prioritized over direct control mechanisms [33, 78]. Seymour et al [74] developed a privacy assistant technology probe, featuring a network disaggregator, personal tutor, and firewall, empowering users in smart homes to understand and control privacy. Despite challenges, the study highlights the potential for users to navigate the smart home landscape with informed attitudes and strategies when supported by the right tools. Service providers aim to offer privacy controls, yet "dark patterns"—deceptive design techniques—often lead users to unintended choices [64, 85]. Some dark patterns violate data protection laws, and the EU-GDPR⁴ emphasizes specific, informed, and unambiguous consent [77, 84]. Usability challenges, including awareness, findability, comprehension, and trust, prompt users to default to permissive settings [28]. Efforts to enhance usability involve exploring novel interfaces, privacy assistants, and machine learning tools [40, 57]. Other studies argue for balancing users' privacy needs with business viability [6, 55].

While mobile applications show promise for privacy enhancement [6, 50], their adoption in Jordan is influenced by factors like education, app quality, age, gender, and income [4, 75]. A prior study highlights the strong impact of mobile applications in the Jordanian context [3], yet their potential in smart home contexts, particularly for bystanders, remains underexplored, emphasizing the need for research sensitive to diverse usage contexts.

2.6 Privacy Protection Regulations

As of this paper's writing, the Jordanian government has announced the forthcoming enforcement of its new data protection law⁵, slated for March 2024 [45]. However, the new law lacks explicit provisions addressing user data protection and privacy conflicts among smart home users, including bystanders. An exploration of the Jordanian legal landscape, encompassing laws such as the Telecommunications Law (Article 71)⁶, Cybercrime Law (Article 3)⁷, Labour Law⁸, and Penal Code⁹, reveals a lack of explicit privacy and data protection regulations for smart homes users. The new Jordanian data protection law⁵, inspired by the EU GDPR⁴, aims to establish comprehensive data protection measures and rights, though its applicability to privacy conflicts among smart home users remains unclear [5, 76]. Additionally, the Jordanian labor law's silence on workers' rights in smart homes raises questions about whether these spaces qualify as domiciles or workplaces for workers [10]. On a broader scale, neither the USA's data protection laws nor the EU GDPR explicitly

⁴GDPR-EU-General Data Protection Regulation

⁵Jordan: [Personal Data Protection Law](#)

⁶Jordan-[Telecommunications Law](#)

⁷Jordan-[Cyber Crime Law](#)

⁸Jordan-[Labour Law](#)

⁹Jordan-[Penal Code – Article 348](#)

address privacy concerns for smart home bystanders, with evolving USA regulations emphasizing user responsibility and the EU GDPR focusing on individual rights without explicit reference to bystander privacy [35, 38].

3 Methodology and Research Approach

This study aims to address the research question outlined in §1 through a two-phase investigation drawing on prior research insights [5, 7, 16]. It is essential to note that this study is intended as an exploration—not a comprehensive solution to the multifaceted challenges inherent in this privacy landscape. The study was conducted in two phases. The first phase focused on understanding users’ privacy concerns and gathering requirements for co-designing a technology probe in the form of a mobile app to help support privacy protection for domestic workers (bystanders) in Jordanian smart homes. The second phase aimed to assess how this probe could support privacy protection for bystanders in smart homes.

The first phase involved four focus groups comprising 24 participants from households, workers, designers, and app developers. In this phase, we focused on prevalent smart home devices such as cameras, speakers, lights, and door locks, addressing the growing privacy concerns associated with the proliferation of smart devices in Jordan digitalstrategy [6, 7]. Building on the outcomes of this first phase (cf. §4), we prototyped our technology probe as a mobile application on the Thunkable platform¹⁰. The app, detailed in §5, consists of various screens, including mock screens illustrating the envisioned design and active screens demonstrating the app’s functionality in supporting bystanders’ privacy protection [Click [Link-1](#)¹¹ for more details about the app’s screens].

The second phase of the study aimed to assess the potential of this technology probe to serve as an auxiliary tool for enhancing privacy protection. We engaged 26 participants, including smart device designers, households, domestic workers, regulators, and recruiters, through qualitative research and semi-structured interviews. Author#1 engaged with the participants to introduce them to the app’s functionalities, usage instructions, and its primary purpose of supporting privacy protection. Subsequently, participants were encouraged to interact with the app for three weeks before semi-structured interviews were conducted. This interaction allowed participants to understand how the app works, how to use it, what the features are, how they can utilize it in real-world scenarios, and how the app can be improved to support privacy protection. After this period, interviews were conducted to gather perspectives and insights on how such an intervention could effectively support privacy protection in real-world contexts. To mitigate potential harm or ethical concerns and ensure unbiased participation, we avoided recruiting workers and

households from the same homes. For all other participants, we did not exclude those who might be connected.

In this paper, we use specific terms to categorize participants: “*Designers*” for smart device designers, “*Household Users*” for smart home device users, “*Domestic Workers*” for bystanders in smart homes, “*App developers*” for mobile app developers, “*Recruiters*” for heads of recruiting agencies, and “*Regulators*” for labor law and data regulators. Throughout the transcripts, we employ an abbreviation system to identify participants. The system consists of a letter followed by two numbers, where the letter represents the participant type (i.e., [D] for designers, [H] for households, [W] for workers, [M] for app developers, [Rc] for recruiters, and [Rg] for regulators). The first number indicates the focus group number, and the second number represents the participant’s identifier within that specific focus group. For example, [D1_1] refers to designer one in focus group one, [H2_1] signifies household one in focus group two, [W3_1] denotes domestic worker one in focus group three, [Rc2] signifies recruiter two, and [Rg03] denotes regulator three.

3.1 Recruitment

We developed a screening questionnaire to identify potential candidates who met our criteria. These criteria include: a minimum of two years of experience for designers, app developers, regulators, and recruiters; all candidates are required to have basic knowledge of smart home devices and privacy; household heads should have an active role in decisions about smart devices and domestic workers; domestic workers should have internet and smartphone access within their employers’ homes; participants should be proficient in either English or Arabic for communication; and finally, participants must provide consent for interviews and agree to audio recording.

We utilized both purposive and theoretical sampling techniques [39, 59], allowing us to target specific participant groups with relevant characteristics for a diverse yet focused sample. This approach gathers varied data from participants offering valuable insights into the research topic. Theoretical sampling complements purposive sampling by adapting the strategy based on emerging themes, delving deeper into areas of interest and exploring unexpected findings. Sample size and number of participants were determined by reaching data saturation [26, 39], where new data no longer adds significant insights and no new codes are elicited from the data by the two coders. By reaching saturation, researchers ensure data richness and depth, bolstering the credibility and trustworthiness of study findings. Combining these methods facilitates a comprehensive exploration, yielding robust and valid outcomes.

In the first phase of the study, the objective was to gather design insights on privacy from direct users and bystanders to co-design the app. Additionally, we needed to include designers

¹⁰For more details, see: [Thunkable platform](#)

¹¹drive.google.com/file/d/1rrKu826xXa7XZdJeD6gG4plHBF91B09/view

of smart devices and mobile app developers to elicit insights into design challenges and opportunities for the app. Our recruitment strategy targeted domestic workers and households, along with smart device designers and mobile app developers to gather their insights about privacy and power dynamics, and to co-design the app. For the second study phase, which aims to evaluate the potential of this app, in addition to including participants from the first study phase, we included participants who are not direct users of the app but play a significant role in the privacy protection of smart home bystanders, and who might also have indirect interaction with the app. These newly added participants include labor law and data protection regulators in Jordan (regulators), and heads of recruiting agencies for domestic workers (recruiters).

To recruit households and domestic workers from Jordan, we advertised the study on social media groups (e.g., Facebook), engaged with smart device sellers, domestic worker recruitment agencies, and employed snowball sampling [36]. We connected with nine households and ten domestic workers. For smart device designers and mobile app developers, recruitment involved advertising on specialized LinkedIn groups and identifying potential candidates through online searches. We established connections with seven developers and nine designers. Recruiting designers proved challenging, as data protection is considered sensitive, strictly confidential [23, 47], and, to some extent, a taboo topic [83] in many organizations, making many candidates hesitant to participate, citing non-disclosure agreements (NDA) and business confidentiality obligations. To overcome this, participants were briefed on our ethical and security measures, emphasizing data encryption and compliance with GDPR. Additionally, snowball sampling [36] also proved useful in engaging with this hard-to-reach group [12, 80]. In the first phase, we contacted 35 candidates, including nine households, ten workers, nine designers, and seven app developers to schedule interviews. Out of the initial pool, 29 candidates expressed interest and completed a screening questionnaire. Ultimately, 24 participants from diverse backgrounds were successfully recruited, forming the basis for creating four focus groups, each with six members representing their respective categories.

In the second phase, we included recruiters and regulators in the app evaluation. We reached out to domestic worker recruitment agencies and public-private entities in Jordan, such as MODEE¹², ICT companies, and Mobile Operators. We established connections with 12 candidates—five regulators and seven recruiters. Ten candidates expressed interest and completed the screening questionnaire, resulting in the recruitment of four regulators and five recruiters. Invitations for the second phase were extended to 12 participants from focus groups, excluding app developers, prioritizing input from workers, households, designers, recruiters, and regulators. As the study progressed, the second-phase participant

pool expanded to ensure sufficient saturation [39], concluding the second phase with a total of 26 participants (17 from the first phase and nine new stakeholders). To measure users' proficiency with smart devices, we applied Dreyfus' model of skill acquisition [29], categorizing participants into Novice, Competent, Proficient, and Expert stages. For a sample of advertisement posts, see Figure-2, and for the demographic information for the 33 participants in both phases see Table-2.

3.2 Methodology

3.2.1 Focus Groups and Interviews

Focus groups, a valuable research tool for discussing perceptions and generating concepts [13, 30], typically involve six to twelve participants, promoting open dialogue and opinion development in a social context [20, 30]. Challenges in recruiting participants may arise [68]. Moderators, like author#1 in this study, guide discussions, encouraging diverse viewpoints while maintaining impartiality. Discussions are recorded, transcribed, and analyzed thematically [51]. From January to April 2023, four focus group sessions with six participants each were conducted, followed by 26 semi-structured interviews in June, July, and November 2023. Our methodology in both phases adhered to the funnel technique [25], transitioning from general to specific inquiries. This qualitative research approach fosters natural conversation, detailed information collection, and rapport establishment. The progression from open-ended to focused questions ensured comprehensive coverage without overwhelming participants. Remote sessions and interviews were conducted via Zoom, with audio recordings. Participants had opportunities to express thoughts, share insights, and seek clarifications. While a prepared question set was followed, adaptability was maintained by incorporating follow-ups and excluding redundancies.

In the focus group phase, participants shared perspectives on smart devices, patterns of use, and familiarity with data protection rights [14, 27]. We explored their views on data collection, trust in smart devices, and strategies for ensuring data protection. Our line of questioning included their insights on adopting a mobile app as an auxiliary tool to support privacy protection. In the second phase, participants provided views on the app focusing on its practicality, features, potential to support privacy, and potential to balance power dynamics. We improved the app based on participants' suggestions through an iterative feedback process. To mitigate response bias [14, 27], we started with general inquiries about privacy concerns and the app's concept, and avoided leading questions. Both the focus groups and interviews were conducted in English and Arabic by a proficient researcher. All focus groups were in English, while interviews were bilingual, with nine in Arabic. The information sheet and advertisements for the study explicitly invited volunteers, who willingly contributed their time without compensation.

¹²MODEE: Ministry of Digital Economy and Entrepreneurship

Before conducting the focus groups and interviews, we conducted a pilot focus group study with a convenience sample [15], involving four experienced researchers. This pilot study ensured the clarity and effectiveness of the guidance script and provided valuable feedback. No significant modifications were needed for the focus group or semi-structured interview scripts, with feedback primarily focusing on question phrasing and comprehensibility.

3.2.2 Co-Design Approach

Informed by insights from prior research on co-design promoting collaboration between designers and end-users [72], we used a participatory design process to develop a mobile app aimed at enhancing privacy in smart homes (cf. Fig-1). Given the widespread use of smartphones in Jordan¹³ and the ease of developing mobile apps [42], this approach proved practical. This decision was further supported by previous research [5, 7]. We developed a mobile app prototype based on initial insights and refined it iteratively with feedback from the second phase for a comprehensive evaluation.

3.3 Data Analysis

Thematic analysis [22] was employed as the methodology for both phases, providing a structured approach to data collection, coding, and inductive reasoning in exploring under-researched areas. It enabled a thorough examination of privacy concerns, uncovering underlying perceptions, beliefs, and behaviors. Fig-1 illustrates research process and methodology.

In the focus group phase, systematic thematic analysis was applied to explore privacy concerns related to smart home devices. NVivo 12 Pro¹⁴ software aided in the coding of professionally transcribed audio recordings. The iterative open coding [82] and Braun and Clark's thematic analysis approach [22] were used, involving both authors. The collaborative initial codebook was cross-referenced against focus group transcripts, resulting in a final codebook. A total of 138 codes were identified and organized into categories and themes discussed in §4. Inter-rater reliability indicated perfect agreement (Cohen's kappa coefficient, $\kappa = 0.85$) [66]. In the second phase, a similar thematic analysis approach was applied to interview data, also using NVivo 12 Pro¹⁴. The iterative open coding and thematic analysis involved both authors, and the collaborative initial codebook was cross-validated against interview transcripts. Inter-rater reliability remained perfect (Cohen's kappa coefficient, $\kappa = 0.82$). The analysis identified 87 codes, organized into categories and themes in §5.2. Data saturation [26, 39] was observed separately for each study phase, occurring between the 3rd and 4th focus group in the first phase and between the 24th and 25th interviews in the evaluation phase. Reaching saturation

¹³Jordan: [Digital Report-2021](#)

¹⁴NVivo Pro 12: [Application to organize, analyze and visualize information](#)

was determined when no new themes or codes emerge, and additional data collection yields redundant information. This is confirmed through iterative analysis, where researchers find that the newly collected data consistently fits existing themes without adding significant new insights.

3.3.1 Research Position and Ethics

Our research in Jordanian smart homes explores the intersection of privacy protection, power dynamics, and technology use. The objective is to examine how a socio-technical intervention could enhance user awareness, mitigates power imbalances, empowers users, and offers auxiliary tools for privacy protection. We acknowledge our positionality [86] and its potential impact on participants and research outcomes. Our primary research question delves into the implications of power dynamics on technology use and privacy, emphasizing ethical values like fairness, freedom, and accountability. To mitigate bias, we designed our focus group and interview guides to avoid leading questions, framing the study as an exploration of privacy and interpersonal implications of smart technology. Two coders were employed to ensure data analysis reliability.

We prioritized participant anonymity and privacy, actively seeking evidence of any illegal treatment (which was not found). Maintaining a neutral standpoint, we focused on reporting rather than intervening when uncovering potential instances of unfair technology use. Challenges persist in this research area, and future studies may reveal more instances requiring standardized research strategies and protocols for identification, assessment, and resolution. Despite acknowledging study limitations and potential biases, we remain confident in the validity of our findings. Ethical considerations were paramount, with approval from the Central University Research Ethics Committee (CUREC) at the University of Oxford [Approval No: CS_C1A_23_012]. This approval was granted after we provided comprehensive details about the study and demonstrated how we would implement measures to ensure participant safety, security, and confidentiality. Participants provided oral consent, assured of the strict confidentiality of their data and their right to withdraw without explanation. Focus group and interview scripts were securely encrypted and stored. No participants withdraw from the study.

3.4 Limitations

Like all qualitative research studies, this study has limitations:

Language: While the focus group sessions were conducted in English, the choice of English or Arabic interviews was provided in the second phase. Arabic interviews were carefully translated to preserve original perspectives. Challenges were faced by some non-native English speakers due to language nuances. Nevertheless, minimal impact on analysis was found during validation of results.

Quality: Qualitative research quality depends on researchers' skills and potential biases. Novice researchers may encounter difficulties in conducting effective focus groups, interviews, posing probing questions, and exploring critical subjects, potentially leading to overlooking of relevant data [54]. The depth of data collection significantly relies on moderators' and interviewers' expertise, as well as question quality [19]. To address this, a skilled researcher moderated the four focus groups and conducted the 26 interviews, utilizing neutral and open questioning techniques to prevent influencing participants' responses.

Self-Reporting Bias: A common challenge in qualitative research [46] is participants forgetting details or providing inaccurate responses. Furthermore, participants may adjust their answers based on their perception of researchers' viewpoints, introducing bias [81]. To enhance validity and mitigate self-reporting bias, proactive measures were taken. This included using open-ended questions to elicit comprehensive responses and prompting further inquiries for additional information, ensuring a thorough understanding of participants' perspectives.

Focus Group dynamics: These dynamics may lead participants to experience some pressure to align with the majority's opinions, or one participant might dominate the conversation. To mitigate these challenges, the moderator guides the discussion to foster productivity, maintain balance, and ensure that every participant can express their viewpoints.

Recruitment: The study encountered challenges in participant recruitment due to confidentiality concerns, resulting in a limited and less diverse sample. Additionally, the sensitive nature of privacy topics may have led to biased or incomplete participant responses. To address this, security measures were outlined, emphasizing anonymization and GDPR compliance.

Generalizability: The qualitative nature of this study limits the generalizability of findings beyond the specific Jordanian context. By delving into privacy concerns and protection measures in Jordanian smart homes, the research sheds light on the intricate interplay of cultural, social, and regulatory factors. While offering valuable insights into participants' experiences and behaviors, the study's qualitative approach may not extend readily to other MAME countries like Saudi Arabia, Iraq, Syria, and Lebanon. Each country's unique cultural, social, and regulatory dynamics can influence privacy perceptions differently. Therefore, findings should be interpreted within the Jordanian context, with caution regarding their applicability elsewhere in the region. Future research can build on our findings to explore privacy concerns in smart homes across various MAME countries to better understand regional differences, thereby paving the way for further research in this under-explored region.

4 Findings of the Focus Groups Study

The findings from our focus groups detail insights for co-designing the app. Two main categories emerged: "*Privacy Protection with the App*" and "*Considerations and Challenges*". In the subsequent section, we provide details on the identified themes (cf. Table-3 for identified Themes).

4.1 Privacy Protection with the App

4.1.1 Privacy Concerns & Power Dynamics

This section presents participants' perspectives on privacy concerns and smart home power dynamics.

4.1.1.1 Privacy Concerns. Our findings highlight unanimous appreciation for the value of smart home devices among participants, acknowledging their benefits in enhancing productivity, simplifying tasks, and improving overall comfort. For instance, [H2_1] noted the convenience and efficiency of remotely controlling the temperature through a smart thermostat. Similarly, [D2_1] emphasized how these devices assist in managing household chores, focusing on time-saving and enhanced manageability. Despite these positive views, participants raised significant privacy concerns associated with smart devices, including issues like data collection, potential misuse, unauthorized access, low awareness [H1_1,W1_1], and challenges related to dark patterns [37] and complex privacy policies [H1_1,D3_1,W1_1,D2_1]. Notably, [H2_2] emphasized the importance of protecting personal data, while workers expressed concerns about privacy breaches through monitoring devices [W2_1], and also highlighted trust issues and constraints on worker agency [W2_2].

Insights from our study uncovered weak awareness and a lack of transparency regarding smart devices and data collection [H1_2,W3_1], limited understanding of data protection rights and regulations [W2_1,H1_1], and challenges related to user consent [W2_1,W2_2], as well as a call for collective responsibility for privacy protection [H3_2,W3_1]. However, participants often argued that the benefits of smart devices outweigh the associated risks [H1_1,H3_1].

4.1.1.2 Autocratic Dynamics and Marginalization Within Domestic Settings.

Findings reveal dynamics within Jordanian smart homes, exposing tensions between workers and households [H4_1,D2_1]. Participants express privacy concerns, highlighting the delicate balance between convenience and protecting user privacy [H1_1,W2_1,W4_1]. Some households discuss privacy concerns with workers [H3_1], while others avoid such discussions due to trust issues and imbalanced power dynamics [H4_2,W2_1,W3_1]. Both households and workers report a form of marginalization resembling contract slavery in Jordanian smart homes, particularly affecting female foreign workers

who worry about privacy breaches through smart devices [W2_1,W3_1,H3_1]. Instances of restrictive practices, such as confiscating workers' passports and IDs, limiting their movement, and restricting internet and smartphone access, are shared [W1_2]. Workers express a desire to discuss privacy needs but refrain due to potential job consequences [W1_1,W1_2]. Participants suggest that the prototype app could facilitate such discussions without jeopardizing jobs or relationships with households [D1_1,W2_1,M1_1]. Some households justify restricting workers' access, citing family security concerns [H4_2]. However, some workers report having access to smartphones, internet, and a weekly day off [W4_1]. A growing number of households permit workers access to the internet and smartphones, highlighting diverse practices in managing relationships with domestic workers in Jordanian smart homes [W1_1,H2_2,H3_1].

Participants emphasize understanding smart technology's implications on power relationships [D3_1,H2_1,M2_1], arguing for a holistic approach beyond individual actions [H3_2,W1_1]. Viewing the proposed app as an auxiliary tool [H3_2,W1_1,W3_1], they emphasize privacy protection as a collective responsibility, requiring collaboration from all stakeholders [D1_1,H3_1,W2_1], systematic changes, and ethical practices [D3_1,H2_2,W4_1], highlighting associated challenges and responsibilities [H2_1,D3_1,M4_1,W4_2].

4.1.2 Proposed Features and Protection Strategies

4.1.2.1 Proposed Features for the App. Participants proposed several features to support privacy protection:

Structured privacy discussions: Participants emphasized the need for structured privacy discussions, empowering workers to openly communicate their privacy preferences on topics like data collection, audio/video limitations, and data storage constraints. This dialogue is crucial for fostering effective communication with households, as outlined in §4.1.1.2. Participants [H3_1,W1_2,W2_2,W4_1] suggested using the app to guide these discussions, informing households about workers' privacy preferences, including data types, storage duration, sharing protocols, and other settings within the app's interface [D2_1,H3_1]. There were also discussions about involving recruitment agencies [H3_1,W1_2,W3_1] to oversee communication between households and workers, with updates facilitated by worker representatives [W2_2,W4_1]. However, concerns raised by households prompted designers [H2_2,D2_1] to stress the importance of developing careful regulatory measures.

Information sharing about smart devices and privacy risks: Participants [H4_1,W4_2,D1_1] suggested that the app could be utilized to provide information about smart devices, data collection processes, privacy threats, applicable data protection regulations, privacy protection best practices, and to promote respect for home safety. They felt this would raise user awareness and enable them to make informed decisions.

Discovering nearby devices and providing privacy threat alerts: Participants [D1_2,W3_1,W1_1] highlighted the importance of users knowing about existing devices and the types of collected data, and empowering informed actions. Designers emphasized the importance of notifications, and proposed that smart home devices should be designed to broadcast information about their type and the collected data. The app could then receive these information and notify users around the devices accordingly [D3_2].

Inquiries with a privacy advisor via dedicated hotline/chat agents: Workers [W2_1,W3_1] wanted an option to chat or discuss issues with a privacy advisor through a chat channel or hotline. This would assist them in obtaining information about smart devices, privacy threats, and guidance on how to respond in case of privacy breaches.

Channel to report privacy violations to government entities: Participants [H2_2,D3_1] argued that enabling users, especially workers, to report privacy breaches and autocratic practices to an official entity could improve their agency and enhance privacy protection. They suggested that such an official entity could be developed by the government in cooperation with concerned social organizations.

Supporting user profiling by collecting and sharing users' identification data with smart devices: Participants proposed the use of user profiling for smart devices, allowing data segregation and management based on household permissions and identifying types of user/bystander. Workers raised concerns about maintaining bystanders' anonymity [W2_1], [D2_1]. while designers supported multi-user consent mechanisms, proposing that smart devices can collect and share users' identification data (e.g., audio and video) with smart devices to facilitate user recognition and profiling [D2_1].

General requirements: Participants discussed general requirements for the app, such as language accessibility, ease of use, user-friendliness, intuitive design, and inclusivity, ensuring effective use by diverse users, including domestic workers [D2_1,M2_1,M2_1,M4_1,W3_1]. Furthermore, participants argued for separate User Account Management versions for households and workers [M1_1,D2_1,W3_1], available in relevant languages, in addition to highlighting the need for a comprehensive help and support function [D2_1,M2_1,M4_1].

4.1.2.2 Privacy Protection Strategies. Participants emphasized the need for increased awareness about smart devices, data collection, and privacy threats to mitigate power dynamics and protect workers' privacy [H2_1,D3_2]. Households stressed the importance of understanding surrounding devices, being cautious about sharing sensitive information, and staying well-informed about privacy features and risks [H2_1]. Worker perspectives highlighted the significance of user education in addressing privacy threats, arguing for devices with clear privacy controls and transparent information about data collection [W2_1,D3_1]. Additionally, workers emphasized the importance of open communication and

trust-building with households to address power dynamics [W4_2]. Mobile app developers emphasized shared ethical responsibilities [M1_1], while designers underscored prioritizing privacy, user autonomy, and multi-user consent [D1_2]. Both discussed using the app to access smart devices, contingent on household permission. Participants acknowledged the app's value as an auxiliary tool but recognized that it cannot fully protect workers' privacy alone [D1_1,W1_1]. Diverse views emerged: [D3_1] urged robust privacy measures, [D1_1] stressed manufacturers' informing and empowering responsibility, and [H3_2] believed in shared user-company responsibility.

4.2 Considerations and Challenges

This section presents participants' perspectives on the considerations and challenges associated with the app.

4.2.1 Concerns with the App

4.2.1.1 Feasibility and Adoption. Participants emphasized that the app's success relies on well-designed features [D2_1], users' correct use [D1_1], and permitting workers to use it [D4_1,W2_1,W3_1]. Households shared these sentiments, emphasizing concerns about the risks of allowing access to smart devices to users outside of the family [H1_1,H3_2,H4_1,H4_2,H2_1]. They also stressed the app's potential positive impact through user education [D2_1], fostering privacy respect among users [H1_2], ensuring home safety, privacy, and security [D2_1,D1_1], and facilitating privacy discussions between workers and households [W1_1,H1_1]. Thorough discussions regarding the app's utility in facilitating communication and privacy discussions with households were held, as elaborated in §4.1.1.2. While some participants acknowledged that workers can directly engage in privacy conversations with their employing households [H1_1,W2_1], others argued this did not happen in practice due to imbalanced power dynamics, autocratic household practices [H2_1], considerations related to empowerment and agency of workers [W1_2,D1_2,W2_2], and weak awareness among workers [W1_2,H2_1]. Participants also noted the sensitivity of discussing privacy preferences with households, as it could lead to suspicions of wrongdoing, illegal activities, unethical behavior, or even crimes, potentially resulting in the termination of worker contracts, especially for new workers lacking sufficient trust with families [W2_2,H3_1].

To avoid consequences of direct communication with households, participants suggested that recruitment agencies start a general dialogue about using the app with households to protect users' privacy [D2_1,W2_1]. This could lead to broader discussions on privacy preferences [W2_2,W3_1,H3_1,H3_2,D4_1] and detailed discussions about workers' privacy needs. Encouraging households to adopt the app would allow workers to use it during specific

periods. Participants favored mobile apps over websites for their user-friendliness and convenience [H2_1,D1_1,W2_1], believing that app adoption could improve trust and respect [D2_1], leading to better relations with households and enhanced worker performance [W1_1,H1_2]. Highlighting these benefits in discussions with households could promote app adoption [H1_2,W3_1,D4_1,M2_1]. However, households emphasized their right to evaluate workers and take disciplinary actions, including termination, for negative actions [H1_1,H3_2].

4.2.1.2 Legal and Ethical Considerations. Participants discussed the legal aspects of developing a privacy-focused mobile app for smart homes in Jordan. Designers and households emphasized compliance with data protection laws and regulations, prioritizing users' privacy rights [D3_1,H3_1]. Workers emphasized the importance of informed consent, seeking clarity on data collection purpose, access, and transparency [W1_1]. All parties agreed on the necessity of explicit consent and user-controlled data sharing options [H2_1,M4_1]. Developers emphasized defining liability and transparent data collection practices through clear privacy policies and third-party integration disclosures [M1_1].

4.2.2 Development of the App

This section presents participants' perspectives on the technical requirements and the associated challenges for the app to be able to provide the proposed features in §4.1.2.1. Participants highlighted seamless integration with various smart devices [D4_1], and emphasized requirements like audio-video recording [M4_1], location sharing [W2_2], chat agent [H2_2,M2_1], and messaging [H3_2,M4_1]. Designers emphasized an intuitive UI¹⁵\UX¹⁶ design catering to diverse users [D3_2], with continuous technical support and updates deemed crucial [M2_1].

Participants discussed technical challenges in developing the proposed app. Key concerns included:

Device Compatibility and Integration: Developers emphasized the importance of ensuring compatibility with various smart devices, mentioning protocols like Zigbee¹⁷, Z-Wave¹⁸, and Wi-Fi¹⁹. Support for popular platforms like Amazon Alexa and Google Assistant was also highlighted [M3_1,D3_2].

Scalability and Performance: Developers addressed the challenge of increasing number of devices and optimizing performance. They suggested using protocols like MQTT²⁰ and RESTful APIs²¹ for effective communication [M3_1].

¹⁵UI: [User Interface Design](#)

¹⁶UX: [User Experience Design](#)

¹⁷For more details, see: [Zigbee](#)

¹⁸For more details, see: [Z-Wave](#)

¹⁹For more details, see: [802.11x: Wi-Fi standards](#)

²⁰For more details, see: [MQTT: The Standard for IoT Messaging](#)

²¹For more details, see: [RESTful APIs: What is a REST API?](#)

Usability: Households emphasized the importance of clear privacy instructions and well-designed features, while designers argued that clear design guidelines are essential, and the lack of such guidelines poses a challenge in designing compelling smart devices [H3_2,D1_1].

5 Developing and Evaluating the App

Drawing on focus group outcomes, we identified essential requirements for app development. This section presents these requirements and the developed prototype app.

5.1 The App Features and Use

We collaboratively developed a prototype mobile app²² (the probe) in an iterative process to meet identified requirements (cf. Table-1). While not fully implementing all proposed features, the app serves as a demonstration of an auxiliary tool to support privacy protection. Key functions include structured privacy discussions, smart device information sharing, privacy threat alerts, and inquiries with a privacy advisor. The app empowers workers to transparently communicate privacy preferences, covering data collection, audio/video restrictions, and data storage limits. Educational content on smart devices and privacy risks, advisory hotlines, and a reporting channel for breaches are provided. The app scans for nearby devices, notifies of potential threats, and supports user profiling by collecting and sharing users' identification data with smart devices. For more details on the app's proposed features, please refer to §4.1.2.1.

The app includes operational and mock screens with demo functions for privacy notifications, reporting privacy breaches, and live chat with a privacy advisor. A chat simulation using OpenAI's²³ API simulates real-time chat services. Reporting privacy violations or seeking information from a proposed official entity is nonfunctional and requires establishing such a service within the government, and the scanning function requires household permission. In summary, the app's features offer insights into its potential as an auxiliary tool for privacy protection. Click [Link-1](#)¹¹ to show samples of the prototype app's screens, and click [Link-2](#)²⁴ to download a diagram that illustrates how users can utilize the app.

5.2 Evaluation of The Mobile Application

This section outlines the outcomes of the app (the probe) evaluation phase. Through iterative enhancements based on participant feedback, the app was refined until no further suggestions were received. Results, categorized into "*The App Supports Privacy Protection*" and "*Barriers Confronting the*

App". In the subsequent sections, we provide details of the identified themes and categories (cf. Table-4).

5.2.1 The App Supports Privacy Protection

5.2.1.1 The App Facilitates Privacy Discussion. Many participants recognized the app's effectiveness in facilitating structured privacy discussions between workers and households that adopt the app and allow workers use [H3_1,W1_2]. They believed that the app establishes a framework for privacy discussions, as it offers a user-friendly interface for workers to share their privacy preferences [D4_1,W4_2,Rc1], and enable households to gain insight into these preferences, fostering collaborative privacy discussions [H1_1,Rc03], and enhancing understanding and trust between workers and households [D4_1]. They added that the app enables workers to make informed decisions by informing them about smart devices, privacy threats, and rights [H2_2,W1_1,Rc02,D3_1]. However, some participants argued that households retain the ultimate decision in their homes [H3_1,Rc04,W2_1,Rg01].

5.2.1.2 The App Educates Stakeholders. Many participants acknowledged the app's role in educating stakeholders about smart devices and privacy threats, emphasizing the need for regular updates [H2_1,W2_1,W4_1,Rc05,Rg03]. Improvements were suggested which included providing detailed explanations of device functionalities, privacy-preserving practices, and risks to empower informed decision-making [W1_2,W4_1,Rc03]. The app was valued for raising awareness about privacy rights in Jordan and offering information on legal rights [Rg02,Rg04,W1_1,H4_1]. Understanding these rights was seen as crucial for fostering respectful and privacy-conscious environments [H2_1,W4_2,Rc01]. The provision of privacy best practices and practical tips for workers and households was highly appreciated, and participants thought this could significantly enhance privacy protection [H2_1,W2_1,W4_2,Rc04,W4_2]. Among workers, the feature for reporting privacy breaches was particularly endorsed [W3_1], and humorously referred to as 'The Privacy Police' by households [H4_2]. Workers, recruiters, and households all acknowledged the potential for expanding the collective knowledge of privacy threats and protection practices [H4_1,Rc03,W4_2].

5.2.1.3 App's Technical Features. Many participants were satisfied with the technical features in the app. These include: scanning and discovering smart devices, establishing connections with devices to view and manage collected data, and notifying workers about existing smart devices and potential privacy threats, all subject to households' permission [W4_2,Rc05,Rg01]. They believed that this helps to support more informed privacy decisions [H4_2,Rc04]. Some participants argued that the app could support smart devices for user profiling and data segregation by collecting user identification

²²Android- [Copy of the privacy app](#)

²³OpenAI-[API for chat services](#)

²⁴drive.google.com/file/d/1gI4w9lpX9UxFyh2mBzEu7NWDSZj4okBJ/view

data and sharing it with the devices, subject to household's permission. Many participants valued user profiling for data segregation [W4_2,Rc01], although concerns arose regarding family members' data mixing [H3_1,Rg01], as workers often stay with family members, and the data collected for workers may also include information about other family members, making it challenging to separate data [H2_1].

5.2.2 Barriers to the App

5.2.2.1 Households' Restrictions. Households' limitations on worker access to the internet and smartphones are potential obstacles to app usage. Our study highlights several factors contributing to households' hesitance in adopting the app and engaging in privacy discussions with workers [H4_2,Rc05,W1_2]. The first centers around household autonomy, as households assert their final authority in making home-related decisions [H1_1,H2_1,H4_1]. Power imbalances within household-worker relationships also hinder privacy discussions, resulting in app usage restrictions, and workers' concerns about job security [H4_1,W2_2,Rc01]. Furthermore, households tend to avoid open privacy discussions with workers due to trust issues [H2_2,Rc05] and limited awareness of privacy risks [H4_1]. Trust concerns are evident as some households fear data misuse or privacy breaches by workers [H2_1,W1_2,Rc02]. Participants emphasize the need to address household barriers to app adoption through awareness campaigns, highlighting the app's benefits for worker performance, relationships with households, and overall home security [Rg02,D3_1]. Additionally, our findings emphasize the importance of open dialogue and trust-building to foster a respectful environment that prioritizes workers' privacy and home safety [Rc04,Rg03,D4_1,H2_1].

5.2.2.2 Strategies for Promoting App Adoption. Participants discussed several strategies to enable app utilization: *Promote App Adoption Among Households:* Participants stressed the need to promote household use of the app for creating a privacy-conscious environment [Rc05,D3_1]. Suggestions included awareness campaigns through social media, booklets, and community groups to educate households about the app's role in improving the overall home environment and the qualities of relationships (i.e., trust, respect) with workers. The aim is to encourage open privacy discussions that lead to building trust and healthy relationships, promoting the app's value, and potentially increasing app adoption [H3_1].

Encourage Recruitment Agencies to Incorporate the Use of the App into the Work Contract: Most participants recognized the significant role of recruitment agencies in shaping relationships and employment contracts between workers and households [H3_1,W2_1,D3_1,Rc03,Rg04]. It was deemed crucial to include app adoption clauses in work contracts to protect workers' privacy rights [W2_1,W3_1,H4_2]. While recruiters endorsed this idea [Rc03,Rc05], concerns were

raised about potential challenges due to the lack of explicit regulation, highlighting imbalanced power dynamics favoring households [Rc01]. Recruiters emphasized that workers may defer to household decisions in case of disagreement [Rc02]. Participants stressed the importance of educating recruitment agencies about the app's functionalities and benefits [Rc03], facilitating effective communication of its value to workers and households for broader adoption in smart homes [H2_2].

Encourage Workers to Only Accept Jobs that Permit them to Use the App: Some participants noted that encouraging workers to prioritize jobs that allow them to access the internet and use smartphones and similar apps can significantly enhance their privacy protection [W1_1,W3_1,H3_1]. Recruitment agencies, social entities, and relevant organizations can conduct workshops and awareness campaigns to inform workers about such apps' capabilities and how they can support privacy protection [W2_2,D1_1]. Recruiters endorsed the proposal but expressed concerns due to economic power dynamics that do not favor workers [Rc03].

5.2.2.3 Workers' Limited Experience and Agency. The study found that workers may face challenges with using the app due to limited technical skills and experience [W4_2,Rc04,Rg02], including challenges in navigating features and setting privacy preferences effectively [W1_2,Rc04]. Solutions proposed included training programs [W2_1] and ongoing technical support [H2_2,Rc01], as well as multilingual support and clear instructions to overcome language and literacy barriers [W4_2,Rc02]. Concerns about potential retaliation and the need for a privacy-focused culture were also highlighted [W2_2,Rc01,Rc02,Rg04].

5.2.2.4 Technical Challenges. The study identified several technical challenges. One challenge is the absence of standardized privacy protection design guidelines, as designers noted variations in data collection practices and privacy settings among different smart devices [D4_1]. This diversity hinders the ability of apps to offer consistent and comprehensive privacy protection [D3_1]. To overcome this, designers argued for industry collaboration to establish privacy standards integrated into such apps [D4_1]. Another challenge is the lack of attention given to bystander privacy in current smart devices [D3_1]. Designers proposed extending the app's capabilities to manage bystanders' privacy preferences or implementing mechanisms for smart devices to identify and protect bystanders automatically [D2_1]. Addressing these technical challenges requires collaborative efforts among designers, policymakers, and end-users [D1_1].

6 Discussion and Recommendations

Our literature review highlights the significance of considering a mobile app in addressing bystanders' privacy protection

in Jordanian smart homes. The prevalence and affordability of smartphones²⁵ in Jordan make mobile apps a practical intervention. Although the primary focus of this paper is to present and evaluate an auxiliary tool (app) that supports privacy protection rather than proposing a comprehensive solution, it argues for collaborative efforts among all stakeholders. Emphasizing a collective approach over a standalone app is crucial in tackling such a complex problem. This section discusses the study's findings and concludes with recommendations for all stakeholders.

6.1 Summary of the Findings

This study provides valuable insights into the privacy of smart home bystanders, the aspirations for protection, and the potential, feasibility and viability of a bystander privacy app. In the focus groups, our aim was to co-design an app as a technology probe to explore potential privacy protection options for domestic workers in smart homes. The results (cf. §4) reveal two main themes. Firstly, under "*Privacy Protection with the App*", participants discuss multifaceted privacy concerns in domestic settings, proposing app features to address challenges and foster an informed and equitable environment within the smart home. Secondly, in "*Considerations and Challenges*," concerns regarding the app's feasibility, adoption, legal and ethical aspects, and development intricacies are explored. These findings complement previous studies [5, 6, 16], focusing on privacy concerns, regulatory considerations, and power dynamics.

The evaluation study (cf. §5.2) unveils two main themes. In the first theme, "*The App Supports Privacy Protection*," participants commend the app's potential for enhancing communication, empowering workers, and educating stakeholders on smart devices and privacy. Technical aspects, including privacy notifications, and user profiling, are highly appreciated. The second theme, "*Barriers Confronting the App*," addresses challenges such as households restricting worker access and avoiding privacy discussions, workers' limited experience, and technical issues. As discussed in §5, the development of the app was guided by requirements identified in the focus group study. The app encompasses both functional and mock screens, with certain features designed for future activation. Further discussions are provided in the subsequent sections.

6.1.1 App Adoption and Ethical Consideration

In line with prior studies [5, 6], findings reveal variations in households' practices, with some allowing workers internet and smartphone access while others restrict it to family members. Such restrictions can impede app usage for workers in more stringent households. We argue that effective deployment of the app relies on discussions with these households, encouraging them to permit workers' app use. Recruitment

agencies can play a significant role in initiating and moderating discussions between households and workers, especially during the hiring process, and intervening when necessary to facilitate persuading households and reaching a consensus. We endorse this suggestion; however, relevant regulation will be necessary.

Discussions with households should emphasize the app's potential to enhance worker-family relationships, build trust, foster respect for privacy and home safety, and ultimately improve worker performance. While the emphasis is on adopting a persuasive approach rather than coercive measures, other strategies to facilitate app adoption include implementing regulations or incorporating app utilization into work contracts, contingent on households agreeing to such conditions.

6.1.2 The App as a Communication Tool

Findings reveal that spontaneous and unstructured communication between workers and households is often impractical due to existing imbalanced power dynamics (cf. §4.2.1.1). For instance, in conformity with prior studies [5, 7], workers refrain from initiating discussions about privacy with households, fearing job loss and potential consequences. Similarly, households avoid engaging in privacy conversations with workers due to power dynamics and mistrust. Additionally, the findings reveal that workers lack an adequate level of awareness about smart technologies and associated privacy risks [5, 7]. This weak awareness hinders the workers' ability to discuss their privacy needs effectively with households even when they are happy to engage in privacy discussions. As a result, we argue that the app emerges as a promising solution to help mediate and structure an effective privacy discussion between workers and households. By providing a clear and neutral platform, the app can facilitate informed and respectful conversations, helping both parties understand and address privacy concerns. It can also offer educational resources to enhance workers' awareness of smart technologies and privacy risks, empowering them to communicate their needs more effectively. The structured approach of the app can help balance power dynamics, build trust, and ensure that privacy concerns are adequately addressed, improving overall communication and privacy protection in smart homes.

6.1.3 The App as an Educational Tool

We argue for utilizing the app as an educational tool to enhance the learning experiences of households and workers. This approach aligns with previous studies [21, 24] supporting the use of mobile apps for education. The app could be equipped with relevant resources to offer insights into smart devices, their potential impact on users' privacy, recommended privacy practices, and an overview of laws and regulations in Jordan governing personal privacy within home contexts, promoting a safe and respectful environment.

²⁵Jordan: [Smartphone Prices](#)

Additionally, we emphasize the importance of fostering enquiries and discussions on privacy-related topics to raise awareness among households and workers. To achieve this, we propose establishing a service facilitating privacy-related queries, open discussions, and support from privacy advisors for households, workers, and recruitment agencies. This service could be managed by a governmental or socially private unit governed by specific regulations. Workers should also be empowered to report privacy violations to relevant authorities. Furthermore, we argue for creating a multilingual comprehensive FAQ²⁶ repository, containing user inquiries and answers, accessible to all for learning and comparison purposes. This repository would aim to assist foreign workers in understanding privacy concerns within the Jordanian context and help households better understand the privacy concerns of workers with diverse backgrounds.

6.1.4 The App to Alleviate & Balance Power Dynamics

Aligned with prior studies [5–7, 16, 74], our research underscores that workers often face restricted autonomy and agency due to power imbalances, leading them to compromise their privacy (e.g., maintain job security). Participants also raised concerns about multi-user consent and accessibility, emphasizing the critical importance of privacy protection, transparent data practices, trust-building, balancing power dynamics, and empowering users to control their data. The app’s adoption could help as part of a broader initiative to reshape household-worker relationships and address these imbalances.

We argue that persuading households to adopt the app and enabling workers to use its features can empower them by fostering open discussions, imparting knowledge about devices and privacy threats, and providing guidance for privacy protection. Considering the app as an auxiliary tool, complemented by social, technical, and legal interventions, has the potential to address privacy concerns, balance power dynamics, and encourage a secure environment.

6.1.5 Technical Challenges and Concerns with the App

This paper, while addressing adoption barriers and ethical concerns (see §6.1.1), revealed several challenges with the proposed intervention. These include technical challenges such as the absence of standardized privacy protection design guidelines, resulting in inconsistent practices and privacy settings across smart devices, thus impeding the app’s ability to ensure privacy. Moreover, current devices overlook bystanders’ privacy, prompting the need for collaboration to establish integrated standards. Suggestions include improving the app’s capability to manage bystanders’ privacy or utilizing automatic protection mechanisms. Furthermore, some workers face challenges due to limited technical skills, with

²⁶FAQ: Frequently Asked Questions.

proposed solutions including training programs, ongoing support, and fostering a privacy-focused culture. Collaboration among designers, policymakers, and users is crucial to overcome these challenges and ensure positive impacts at home.

6.2 Recommendations

6.2.1 To Recruitment Agencies

Findings underscore the influential role of recruitment agencies in shaping household-worker relationships. In addition to initiating and moderating app adoption discussions with households, as discussed in §6.1.1, we argue for recruiters to leverage their influence to incorporate a greater consideration of worker privacy into employment contracts. We emphasize the importance of employing persuasive techniques to encourage households to willingly adopt the app [52], rather than mandating app usage forcefully through contracts. Additionally, recruiters should take the initiative to educate workers about privacy risks associated with smart devices, utilizing educational materials in languages spoken by the workers (e.g., Philippines²⁷, Indonesia²⁸, Ethiopia²⁹, Ghana³⁰, and Bangladesh³¹).

Moreover, we urge recruiters to provide comprehensive insights into Jordanian culture, societal norms, religious background, working conditions, and workers’ privacy rights. To ensure transparency, recruiters are encouraged to secure workers’ consent through employment contracts, promote a respectful environment for users’ privacy, and facilitate open discussions to address power dynamics and foster relationships built on trust.

6.2.2 To Users

Complementing prior research [5, 6, 16], we recommend that both workers and households familiarize themselves with smart devices and the associated privacy threats. We urge them to understand the app’s functionalities and features and provide feedback for continual app improvement. Households are encouraged to adopt a trust-building approach with their workers, respecting privacy needs and prioritizing home security. By leveraging the app, they can enhance awareness of smart devices and privacy concerns, structure discussions with workers, understand their needs, and prioritize home safety and family privacy, fostering trust. Workers are advised to use the app responsibly, giving priority to household safety and security.

²⁷Languages spoken in Philippines include: Tagalog, Cebuano, Ilocano

²⁸Indonesian is the official and national language of Indonesia

²⁹Spoken languages in Ethiopia include Oromo, Amharic, Somali

³⁰Spoken languages in Ghana include English, Akan, Ghanaian Pidgin

³¹Bengali is the language spoken by workers from Bangladesh

6.2.3 To Companies and Designers

We argue for developing smart devices that integrate with privacy-enhancing tools, such as our app, to leverage collected data (e.g., audio and visual) for user profiling and data segregation within smart home devices. We suggest designing smart devices that actively broadcast information regarding their functionalities, data collection practices, and potential privacy risks. This information can be processed by these tools (e.g., the app), which then notify nearby users about relevant privacy concerns. This feature must be designed carefully to avoid disclosing too much information about household devices, which could undermine the household's privacy and security. Our app scans for nearby smart devices using two communication channels: WiFi (802.11x)¹⁹ and BLE³². For future versions of the app and similar tools, we recommend employing protocols such as Z-Wave¹⁸, Zigbee¹⁷, MQTT²⁰, and UPnP³³ for enhanced scanning functions and connectivity. Utilizing these protocols requires smart home devices to be compatible and equipped with such protocols. These protocols facilitate the app's ability to detect and communicate with various smart home devices, ensuring seamless integration and enhanced privacy protection.

Furthermore, we urge designers to integrate innovative technologies, such as AI tools, and adopt differential privacy and data partitioning techniques [73, 94]. Multi-user consent [5, 6, 69] should be accommodated, and Semiotics³⁴ should be considered as a vital tool to ensure the development and adoption of culturally sensitive signals in smart devices. We argue that the insights from our technology probe can help inform the creation of a language to facilitate privacy discussions between domestic workers and household. Furthermore, the integration of Privacy by Design (PbD) principles [87] is essential, emphasizing the incorporation of privacy considerations at every stage of the design process. PbD should leverage contextual influences and norms, encompassing social, religious, and geopolitical factors. More work should be undertaken to identify common privacy-preserving permissions, both in the app and in smart devices, to mitigate conflicts and ensure widespread household acceptance. We strongly encourage the exploration of ethical business models that prioritize user data protection, emphasizing the adoption of responsible innovation (RI) principles, with adherence to established frameworks, such as the AREA framework³⁵.

6.2.4 To Policy Makers and Social Entities

In §2.6, we highlighted the lack of explicit data protection regulations in Jordan to address privacy conflicts among smart home users. To promote data protection and strike a balance

between the needs of workers and households, we urge Jordanian policymakers to consider the adoption of similar apps within regulatory frameworks. We also argue for broader regulatory interventions to navigate the complex privacy landscape. This includes the establishment of privacy advisory chat services, addressing reported privacy violations, and providing guidance on best privacy practices to raise awareness and support privacy protection. Additionally, we call for collaboration between social entities, policymakers, and recruitment agencies to support vulnerable and marginalized groups, such as domestic workers, through awareness campaigns for end-users. Leveraging the proposed app, social platforms, public media, and the education system in Jordan can facilitate this initiative.

While existing regulations like the European GDPR⁴, USA data protection laws (CCPA³⁶ and CPRA³⁷), Brazil's LGPD³⁸, India's DPDP³⁹, Turkey-DPL⁴⁰, and Malaysia-PDPA⁴¹ primarily address data protection with service providers, they overlook explicit privacy concerns within smart homes. We propose that governments collaborate with international organizations (ITU⁴², GSMA⁴³ and TM-Forum⁴⁴) to address these gaps. Additionally, we argue for countries similar to Jordan to enforce data protection prerequisites on devices before granting market access. Measures such as type approval certificates and data protection tests should be employed in this regard.

7 Conclusion

The study explores co-designing a technology probe mobile app for privacy protection in Jordanian smart homes, covering privacy concerns, power dynamics, adoption barriers, and stakeholder recommendations. Positive feedback from app evaluation highlights its potential in supporting privacy, communication, user education, and addressing power imbalances. Effective strategies include open discussions, emphasizing app benefits on safety, and a persuasive approach over coercion. Stakeholder collaboration is crucial for mobile apps to support privacy, focusing on user-friendly designs for all worker profiles.

We discuss app concerns, propose recommendations for enhanced privacy protection, and stress collaborative efforts. Future research should validate findings, explore contextual dynamics, address autocratic tendencies, leverage new tech, and consider variations among domestic worker types in Jordan and beyond.

³⁶CCPA: [California Consumer Privacy Act](#)

³⁷CPRA: [California Privacy Rights Act](#)

³⁸Brazil(LGPD): [Data Protection Law](#)

³⁹India: [Digital Personal Data Protection Act](#)

⁴⁰Turkey: [Data Protection Law](#)

⁴¹Malaysia: [Data Protection Law](#)

⁴²ITU: [The International Telecommunication Union](#)

⁴³GSMA: [Global ICT industry organisation](#)

⁴⁴TM Forum: [The global ICT industry association](#)

³²For more details, see: [Bluetooth Low Energy \(BLE\)](#)

³³For more details, see: [Universal Plug and Play](#)

³⁴Semiotics-[Definition of Semiotics](#)

³⁵RI-[Responsible Innovation](#)

References

- [1] ABOKHODAIR, N., ABBAR, S., VIEWEG, S., AND MEJOVA, Y. Privacy and Social Media Use in the Arabian Gulf: Saudi Arabian & Qatari Traditional Values in the Digital World. Publisher: The Journal of Web Science.
- [2] AHMAD, I., FARZAN, R., KAPADIA, A., AND LEE, A. J. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction 4*, CSCW2 (Oct. 2020), 1–28.
- [3] AL-HAWARY, S., AND OBIADAT, A. Impact of Mobile Marketing on Customer Loyalty in Jordan. *International Journal of Web Applications 11*, 4 (Dec. 2019), 136.
- [4] ALAFAEEF, M., , D. S., AND , K. A. Influence of Demographic Factors on the Adoption Level of Mobile Banking Applications in Jordan. *Journal of Convergence Information Technology 6*, 12 (Dec. 2011), 107–113.
- [5] ALBAYAYDH, W., AND FLECHAIS, I. Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households. pp. 4643–4659.
- [6] ALBAYAYDH, W., AND FLECHAIS, I. “Innovative Technologies or Invasive Technologies?” Exploring Design Challenges of Privacy Protection With Smart Home in Jordan.
- [7] 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.
- [8] 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.
- [9] 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).
- [10] ALSONDOS, S. A. Will the New Jordanian Law Protect Personal Data?, Feb. 2022. Section: News.
- [11] APHTHORPE, 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.
- [12] ATKINSON, R., AND FLINT, J. Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies.
- [13] BARBOUR, R., AND KITZINGER, J. *Developing Focus Group Research: Politics, Theory and Practice*. SAGE, Dec. 1998. Google-Books-ID: sDZbOLOQB9sC.
- [14] BAXTER, K., COURAGE, C., AND CAINE, K. *Understanding Your Users: A Practical Guide to User Research Methods*. Morgan Kaufmann, May 2015.
- [15] BERNARD, H. R., AND BERNARD, H. R. *Social Research Methods: Qualitative and Quantitative Approaches*. SAGE, 2013. Google-Books-ID: 7sZHuhyzBNQC.
- [16] 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.
- [17] BERND, J., ABU-SALMA, R., AND FRIK, A. Bystanders’ Privacy: The Perspectives of Nannies on Smart Home Surveillance.. 14.
- [18] BERND, J., FRIK, A., JOHNSON, M., AND MALKIN, N. Smart Home Bystanders: Further Complexifying a Complex Context, CI Symposium, August 19–20, 2019, Berkeley, CA, USA. 6.
- [19] BIRMINGHAM, P. *Using Research Instruments : A Guide for Researchers*. ISBN 0-203-42299-6 Master e-book ISBN. Routledge, Dec. 2003.
- [20] BLOOR, M., FRANKLAND, J., THOMAS, M., AND ROBSON, K. *Focus Groups in Social Research*. SAGE Publications Ltd, 1 Oliver’s Yard, 55 City Road, London England EC1Y 1SP United Kingdom, 2001.
- [21] BOTZER, G., AND YERUSHALMY, M. MOBILE APPLICATION FOR MOBILE LEARNING.
- [22] BRAUN, V., AND CLARKE, V. Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*, APA handbooks in psychology®. American Psychological Association, Washington, DC, US, 2012, pp. 57–71.
- [23] CALDER, A. *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*. 2020.
- [24] CAMILLERI, M. A., AND CAMILLERI, A. C. THE TECHNOLOGY ACCEPTANCE OF MOBILE APPLICATIONS IN EDUCATION.
- [25] 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.].
- [26] CORBIN, J., AND STRAUSS, A. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Nov. 2014. Google-Books-ID: hZ6kQBAAQBAJ.
- [27] DELL, N., VAIDYANATHAN, V., MEDHI, I., CUTRELL, E., AND THIES, W. “Yours is better!”: participant response bias in HCI. ACM, pp. 1321–1330.
- [28] DHINGRA, N., GORN, Z., KENER, A., AND DANA, J. The default pull: An experimental demonstration of subtle default effects on preferences. *Judgment and Decision Making 7*, 1 (Jan. 2012), 69–76.
- [29] DREYFUS, S. E. A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition. Tech. rep., Feb. 1980. Section: Technical Reports.
- [30] FOLCH-LYON, E., AND TROST, J. F. Conducting Focus Group Sessions. *Studies in Family Planning 12*, 12 (1981), 443–449. Publisher: [Population Council, Wiley].
- [31] FORLIZZI, J., AND DiSALVO, C. Service Robots in the Domestic Environment: A Study of the Roomba Vacuum in the Home.
- [32] 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.
- [33] GERBER, N., GERBER, P., DREWS, H., KIRCHNER, E., SCHLEGEL, N., SCHMIDT, T., AND SCHOLZ, L. FoxIT: enhancing mobile users’ privacy behavior by increasing knowledge and awareness. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust* (Orlando Florida USA, Dec. 2018), ACM, pp. 53–63.
- [34] GHARAYBEH, K. General Socio-Demographic Characteristics of the Jordanian Society: A Study in Social Geography. 10.
- [35] GILMAN, M. E. Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice. University of Baltimore. 78.
- [36] GOODMAN, L. A. Snowball Sampling. *The Annals of Mathematical Statistics 32*, 1 (1961), 148–170. Publisher: Institute of Mathematical Statistics.
- [37] GRAY, C. M., KOU, Y., BATTLES, B., HOGGATT, J., AND TOOMBS, A. L. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC Canada, Apr. 2018), ACM, pp. 1–14.
- [38] GROUP, G. L. International Comparative Legal Guides, 2022. Archive Location: United Kingdom Publisher: Global Legal Group.
- [39] 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.

- [40] HABIB, H., AND CRANOR, L. F. Evaluating the Usability of Privacy Choice Mechanisms.
- [41] HOYLE, R., TEMPLEMAN, R., ARMES, S., ANTHONY, D., CRANDALL, D., AND KAPADIA, A. Privacy behaviors of lifeloggers using wearable cameras. *ACM*, pp. 571–582.
- [42] HUY, N. P., AND VAN THANH, D. Evaluation of mobile app paradigms. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM '12* (Bali, Indonesia, 2012), ACM Press, p. 25.
- [43] 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.
- [44] ILO. Jordan: Regulatory framework governing migrant workers.. Private sector workers vs domestic workers., 2022.
- [45] JORDAN, D. L. Jordan issues first personal data protection law : Clyde & Co, 2023.
- [46] 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.
- [47] KEANE, E. The GDPR and Employee's Privacy: Much Ado but Nothing New. *King's Law Journal* 29, 3 (Sept. 2018), 354–363.
- [48] KELLEY, P. G., BRESEE, J., CRANOR, L. F., AND REEDER, R. W. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View California USA, July 2009), ACM, pp. 1–12.
- [49] KIGER, M. E., AND VARPIO, L. Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher* 42, 8 (Aug. 2020), 846–854.
- [50] KIM, S., CHO, J. I., MYEONG, H. W., AND LEE, D. H. A Study on Static Analysis Model of Mobile Application for Privacy Protection. In *Computer Science and Convergence*. Springer, Dordrecht, 2012, pp. 529–540. ISSN: 1876-1119.
- [51] KITZINGER, J. Qualitative Research: Introducing focus groups. *BMJ* 311, 7000 (July 1995), 299–302. Publisher: British Medical Journal Publishing Group Section: Education and debate.
- [52] KLEIN, G. A. *Sources of Power, 20th Anniversary Edition: How People Make Decisions*. MIT Press, Sept. 2017. Google-Books-ID: JW01DwAAQBAJ.
- [53] 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.
- [54] 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).
- [55] KOVACH, D. K. A., JORDAN, J., TANSEY, K., AND FRAMIÑAN, E. The Balance Between Employee Privacy And Employer Interests. *Business and Society Review* 105, 2 (2000), 289–298. _eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/0045-3609.00082>.
- [56] 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.
- [57] LIPFORD, H. R., BESMER, A., WATSON, J., AND LIPFORD, H. Understanding Privacy Settings in Facebook with an Audience View.
- [58] LIU, T., LIU, Z., HUANG, J., TAN, R., AND TAN, Z. Detecting Wireless Spy Cameras Via Stimulating and Probing. *ACM*, pp. 243–255.
- [59] LOPEZ, V., AND WHITEHEAD, D. Sampling data and data collection in qualitative research.
- [60] LUPTON, D. Self-tracking cultures: towards a sociology of personal informatics. *ACM*, pp. 77–86.
- [61] MADDEN, M. Opinion | The Devastating Consequences of Being Poor in the Digital Age. *The New York Times* (Apr. 2019).
- [62] 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.
- [63] 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.
- [64] MATHUR, A., ACAR, G., FRIEDMAN, M. J., LUCHERINI, E., MAYER, J., CHETTY, M., AND NARAYANAN, A. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–32.
- [65] MCDONOUGH, O. A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices.
- [66] MCHUGH, M. L. Interrater reliability: the kappa statistic. *Biochemia Medica* (2012), 276–282.
- [67] MENG, N., KEKÜLLÜOĞLU, D., AND VANIEA, K. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (Apr. 2021), 1–29.
- [68] MORGAN, D. L., KRUEGER, R. A., AND SCANNELL, A. U. *Planning Focus Groups*. SAGE, 1998. Google-Books-ID: 6P7mdhtuzBEC.
- [69] NADIN, M. Semiotic Engineering – An Opportunity or an Opportunity Missed? In *Conversations Around Semiotic Engineering*, S. Diniz Junqueira Barbosa and K. Breitman, Eds. Springer International Publishing, Cham, 2017, pp. 41–63.
- [70] NISSENBAUM, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Jan. 2009.
- [71] PRIVAT, G. A system-architecture viewpoint on smart networked devices. *Microelectronic Engineering* 54, 1-2 (Dec. 2000), 193–197.
- [72] SANDERS, E. B.-N., AND STAPPERS, P. J. Co-creation and the new landscapes of design. *CoDesign* 4, 1 (Mar. 2008), 5–18.
- [73] SCHEUERMANN, P., WEIKUM, G., AND ZABBACK, P. Data partitioning and load balancing in parallel disk systems. *The VLDB Journal The International Journal on Very Large Data Bases* 7, 1 (Feb. 1998), 48–66.
- [74] SEYMOUR, W., KRAEMER, M. J., BINNS, R., AND VAN KLEEK, M. Informing the Design of Privacy-Empowering Tools for the Connected Home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu HI USA, Apr. 2020), ACM, pp. 1–14.
- [75] SHAHEEN. Clients Acceptance towards Mobile Banking Application in Jordan Based on TAM Mode, 2021.
- [76] SMEX. Jordan's personal data protection draft bill: is it enough? · Global Voices, 2022.
- [77] STERN, T., AND KUMAR, N. Improving privacy settings control in online social networks with a wheel interface. *Journal of the Association for Information Science and Technology* 65, 3 (2014), 524–538. _eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.22994>.
- [78] TABASSUM, M., KOSINSKI, T., AND LIPFORD, H. R. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks.
- [79] TAMKEEN. Tamkeen for Legal Aid and Human Rights is an independent Jordanian non-governmental civil society organization, 2019.
- [80] TENHOUTEN, W. D. Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-reach Populations. *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique* 134, 1 (Apr. 2017), 58–61.
- [81] TRUEMAN. Structured Interviews - History Learning Site, 2015.
- [82] VAISMORADI, M., TURUNEN, H., AND BONDAS, T. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences* 15, 3 (Sept. 2013), 398–405. Publisher: John Wiley & Sons, Ltd.

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

[84] VOLLMER, N. Recital 32 EU General Data Protection Regulation (EU-GDPR), Apr. 2023. Publisher: SecureDataService.

[85] WILLIS, L. E. Deception by Design. *Harvard Journal of Law & Technology (Harvard JOLT)* 34, 1 (2020), 115–190.

[86] 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.

[87] WONG, R. Y., AND MULLIGAN, D. K. Bringing Design to the Privacy Table: Broadening “Design” in “Privacy by Design” Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow Scotland Uk, May 2019), ACM, pp. 1–17.

[88] WOODRUFF, A., SCHMIDT, L., PIHUR, V., BRANDIMARTE, L., CONSOLVO, S., AND ACQUISTI, A. Would a privacy fundamentalist sell their DNA for \$1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences.

[89] 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.

[90] YAO, Y., XIA, H., HUANG, Y., AND WANG, Y. Free to Fly in Public Spaces: Drone Controllers’ Privacy Perceptions and Practices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver Colorado USA, May 2017), ACM, pp. 6789–6793.

[91] YAO, Y., XIA, H., HUANG, Y., AND WANG, Y. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver Colorado USA, May 2017), ACM, pp. 6777–6788.

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

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

[94] ZHU, T., AND YU, P. S. Applying Differential Privacy Mechanism in Artificial Intelligence. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (Dallas, TX, USA, July 2019), IEEE, pp. 1601–1609.

Appendix-Figure 2: Poster (Designers)

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF OXFORD

Researcher
Wael Albayadh


VOLUNTEERS NEEDED FOR FOCUS GROUP STUDY
CUREC Approval Reference: [CS_C1A_23_012]
Focus Group Study - Mobile Application to Support Privacy Protection in Smart Home

What: -

- 60-90 minutes of audio recorded group discussion.
- Do you use smart devices, or deal with it in the home?
- Are you a smart device designer?
- Are you a mobile application developer?
- Do you manage smart device design teams?
- What concerns do you have with smart home devices?
- Do you have general understanding of MENA Arab culture?
- How could a mobile application protects users' privacy in the smart home?

Who: A participant, who knows about smart home devices, and has insights about how a mobile application support privacy protection of bystanders in the smart home.
Where: Online
When: will agree on a convenient time with the participants.

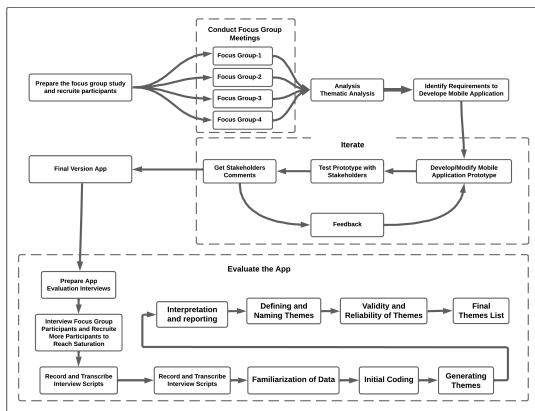
If you agree to participate in the interviews, we do appreciate filling this online questionnaire:

 <https://oxford.onlinesurveys.ac.uk/oxford-online-surveys-focus-group-study-mobile-applicat>

We thank you for your time. You will not be compensated for your participation, but your input will support better understanding of privacy concerns with smart devices which will improve users' privacy protection in future devices.

Contact: wael.albayadh@cs.ox.ac.uk

Appendix-Figure 1: Research and Co-Design Approach



Appendix-Table 1: Requirements for The App

Requirement	Sub Requirements
The App to have Two Versions	Domestic Workers and Households (Admin)
User Account Management	Create Accounts, Reset Password, Settings, and Login
	The App to be Available in Relevant Languages
	User Recognition and Profiling Utilizing Audio-Visual Data
Facilitate Privacy Preferences Discussion	Select Privacy Preferences from List of Options
	Admin to View and Decide on Shared Privacy Preferences
	Admin to Share Decision with Domestic Worker
Discover Devices and Provide Privacy Notifications	Worker to View Admin Decision
	Scan for Devices and the Broadcasted Privacy Notifications
	Notify Workers of the Exist Smart Devices and Potential Data Collection
Provides Privacy Assistance	Connect to Devices After Getting Households' Permission
	Seek Privacy Advice by Calling Privacy Hotline
	Seek Privacy Advice by Chatting with Privacy Experts
	Web Page for Information about Smart Devices and Privacy
	Web Page for Information about Privacy Rights in Jordan
Discover Devices and Provide Privacy Notifications	View Videos about Privacy and Smart Devices
	Scan for Devices and the Broadcasted Privacy Notifications
	Notify Workers of the Exist Smart Devices and Potential Data Collection
Channel to Report Privacy Violations	Connect to Devices After Getting Households' Permission
Help and Support about the App	Write Message Describing Privacy Violation and Send to Authorized Entities
	Seek Help about the App and Provide Feedback for Future Improvements

Appendix-Table 2: Demographic Information of Participants

P#	Focus Group#	Phase	Gender	Nationality	Age	Education	Role	Experience (Years)	Company Size	Competence	Used Smart Devices
H1_1		1 & 2	Male	Jordan	40-49	B.Sc.	Teacher	10		Basic	Smart Camera, Sony Smart TV
W1_1		1 & 2	Male	Jordan	30-39	B.Sc.	In Home Nurse	5		Basic	Google Home, Smart Camera
W1_2	G1	1 & 2	Female	Ethiopia	20-29	High School	Maid	2		Basic	Smart Security, Smart Camera
D1_1		1 & 2	Male	England	50-59	B.Sc.	UX Designer	12 (SME)	SME	Proficient	Smart Thermostat, Smart Door Lock
D1_2		1	Male	England	30-39	B.Sc.	UX Designer	4 (SME)	SME	Proficient	Smart Thermostat, Smart Door Lock
M1_1		1	Male	India	20-29	B.Sc.	App Developer	4	SME	Expert	Google Nest Audio, Smart Cameras
H2_1		1 & 2	Male	Jordan	30-39	M.Sc.	ICT Manager	6		Expert	Smart Camera, Smart Light
H2_2		1 & 2	Male	Jordan	40-49	B.Sc.	Marketing Manager	11		Basic	Smart TV, Smart Camera
W2_1	G2	1 & 2	Male	Jordan	30-39	B.Sc.	In Home Nurse	7		Basic	Amazon Echo Dot, Smart Cameras
W2_2		1 & 2	Female	Ghana	20-29	High School	Maid	4		Basic	Smart Cameras, Smart TV
D2_1		1 & 2	Male	German	40-49	M.Sc.	Solution Architect	9 (SME)	SME	Expert	Smart Light, Smart TV
M2_1		1	Male	Jordan	30-39	B.Sc.	App Developer	8	SME	Expert	Smart Speakers, Smart Plugs
H3_1		1 & 2	Female	Jordan	30-39	PhD	University Professor	7		Competent	Google Home, LG Smart TV
H3_2		1	Female	Jordan	30-39	B.Sc.	Lawyer	8		Basic	Smart TV, Smart Camera
W3_1	G3	1 & 2	Female	Philippines	30-39	High School	Babysitter	6		Basic	Smart Camera, Smart Lights
D3_1		1 & 2	Male	USA	20-28	B.Sc.	Firmware Designer	5 (Large)	Large	Expert	Google Home, Smart Camera
D3_2		1	Male	USA	30-39	B.Sc.	UX Designer	9 (SME)	SME	Expert	Smart Security System, Smart Lights
M3_1		1	Male	Jordan	30-39	B.Sc.	App Developer	7	SME	Expert	Amazon Echo Dot, Smart TV
H4_1		1 & 2	Male	Jordan	30-39	M.Sc.	HR Manager	6		Competent	Smart Camera
H4_2		1 & 2	Female	Jordan	40-49	B.Sc.	Housewife	5		Basic	Smart Camera
W4_1	G4	1 & 2	Female	Bangladesh	20-29	High School	Maid	4		Basic	Smart Camera, Smart Door Bell
W4_2		1 & 2	Male	Jordan	30-39	Diploma	In Home Nurse	7		Basic	Smart TV, Smart Camera
D4_1		1 & 2	Male	USA	20-29	M.Sc.	Firmware Designer	5 (Large)	Large	Expert	Google Home, Smart Camera
M4_1		1	Male	India	20-29	B.Sc.	App Developer	4	SME	Expert	Smart Camera, Amazon Echo Dot
Rc01		2	Male	Jordan	30-39	B.Sc.	GM Recruiting Agency	4		Basic	Smart Camera
Rc02		2	Male	Jordan	50-59	B.Sc.	GM Recruiting Agency	9		Competent	Smart Camera, Smart TV
Rc03		2	Male	Jordan	40-49	B.Sc.	Director Recruiting Agency	7		Competent	Smart Camera, Smart TV
Rc04		2	Male	Jordan	50-59	M.Sc.	Director Recruiting Agency	12		Basic	Smart Camera
Rc05		2	Male	Jordan	30-39	B.Sc.	GM Recruiting Agency	6		Basic	Smart Camera, Smart TV
Rg01		2	Male	Jordan	40-49	B.Sc.	Labour Law Expert	8		Competent	Amazon Echo Dot, Smart Camera
Rg02		2	Male	Jordan	40-49	B.Sc.	Regulatory Team Leader	9		Competent	Smart Camera, Smart Heating System
Rg03		2	Male	Jordan	40-49	B.Sc.	Regulatory Expert	11		Expert	Smart Camera, Smart Door Lock
Rg04		2	Male	Jordan	40-49	B.Sc.	ICT Regulation Manager	9		Competent	Smart Lights, Smart Camera

Appendix-Table 3: Focus Groups - Categories and Themes

Categories	Themes	Sub-Themes	Prominent Codes
Privacy Protection with the App	Privacy Concerns & Power Dynamics	Privacy Concerns	Benefits and Concerns with Smart Technologies
		Autocratic Dynamics Within Domestic Settings	Awareness Among Users
			Tensions Between Workers and Households
	Proposed Features and Protection Strategies	Proposed Features for the App	Marginalization and Contract Slavery
		Privacy Protection Strategies	Educate Users
			Facilitate Structured Privacy Discussion
Considerations and Challenges	Concerns with the App	Feasibility and Adoption	Technical Features and Functions
		Legal and Ethical Considerations	Improve Awareness
			Aleviate Power Dynamics and Trust Building
	Development of the App	Technical Requirements	Feasibility Depends on App Features
		Challenges with the App Development	Feasibility Depends on App Adoption
			Feasibility Depends on Users' Competence to Use the App
		Lack of Explicit Regulation in Jordan	
		Ethical Considerations	
		Technical Support for Proposed Features	
		Absence of Design Guidelines	
		Usability and Intuitiveness	

Appendix-Table 4: App Evaluation- Categories and Themes

Categories	Themes	Sub-Themes
The App Supports Privacy Protection	Facilitate Privacy Discussion	The App Establishes a Structure for Privacy Preferences Discussion
		Households Hold the Ultimate Decision
	Educate Stakeholders	Provide Information about Smart Devices and Privacy Risks
		Facilitate Reporting Privacy Violations
Barriers Confronting the App	Households' Restrictions	Notify Workers of Existing Smart Devices and Potential Privacy Threats
		Facilitates Users' Profiling and Data Segregation
	Strategies for Promoting App Adoption	Households Restrict Worker Access to the Internet and Smartphones
		Households Decline to Engage in Discussions with Workers
Workers Limited Experience and Agency	Promote the Adoption of the App Among Households	
	Recruitment Agencies to Incorporate the Use of the App into Work Contracts	
Technical Challenges	Encourage Workers to Consider Accepting Job that Permit them to Use the App	
	Weak Awareness of Smart Devices and Privacy Threats	
	Lack of Consideration of Bystanders Privacy	
	Lack of Standard Privacy Protection Design	