"Innovative Technologies or Invasive Technologies?" Exploring Design Challenges of Privacy Protection With Smart Home in Jordan

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

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

ABSTRACT

The growing adoption of smart devices has fuelled privacy concerns, and prior research has highlighted the privacy of bystanders: individuals who are subjected to the smart device use of others. Most of this research has focused on households in Western contexts (i.e., Europe and North America), but few studies have explored the design challenges of protecting bystanders, and even fewer have explored these in Muslim Arab Middle Eastern settings, such as Jordan.

We conduct 44 interviews with users (i.e., families, domestic workers), local and international business leaders, and smart device designers to explore design challenges for privacy protection in the Jordanian context. Our analysis highlights the importance of considering contextual influences and power dynamics, localization and design guidelines, innovative technologies, awareness to design, and regulation. This paper concludes with recommendations for technical, social, business, and legal interventions to improve data protection design of smart devices in Jordan.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; • **Human-centered computing → Empirical studies in HCI**; **HCI theory, concepts and models**.

KEYWORDS

Smart Home, Smart Device, Privacy, Bystanders, Data Protection Regulation

ACM Reference Format:
Wael Albayaydh and Ivan Flechais. 2024. "Innovative Technologies or Invasive Technologies?" Exploring Design Challenges of Privacy Protection With Smart Home in Jordan. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW1, Article 76 (January 2024), 39 pages. https://doi.org/10.1145/3637353

Authors' addresses: Wael Albayaydh, wael.albayaydh@cs.ox.ac.uk, University of Oxford, Oxford, United Kingdom; Ivan Flechais, ivan.flechais@cs.ox.ac.uk, University of Oxford, Oxford, United Kingdom.

2573-0142/2024/1-ART76 $15.00
https://doi.org/10.1145/3637353

1 INTRODUCTION

The growing adoption of smart devices continues to fuel privacy concerns, with many users considering them creepy and invasive technologies [1]. While users' privacy with smart devices is a key area of interest, there is also a need to consider the privacy of bystanders, as the prevalence and data collection capabilities of smart devices increase, so does the need to design solutions that address privacy needs of all stakeholders, not just users. According to Yao et al.[2] *"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"*. Under this definition, we assume that smart home bystanders can be subjected to data collection, and may not be aware of installed smart devices, or the functions of these devices. For simplicity, we will define bystanders as *'individuals who are subjected to the smart device use of others'*. An additional issue in tackling the design of more appropriate privacy solutions is that this area has been explored largely from a Western perspective: non-Western norms, values, and challenges have been generally overlooked. This paper focuses on domestic workers in Jordan as a group of smart home bystanders in a country that is witnessing increasing adoption of smart devices[1] coupled with growing concerns [3, 4] about users' privacy and specifically bystanders who were overlooked in previous studies.

We report on the findings of a qualitative study where we interview a total of 44 participants (comprising smart device designers, local and international business leaders, users, and bystander[2] domestic workers) in order to explore design challenges of privacy protection in Jordan. Using Grounded Theory, we analyse how participants understand privacy protection concerns and elicit their insights on privacy design challenges. We further examine their views on ways to achieve privacy protection, focusing on privacy protection interventions, localization of smart devices, expectations from innovative technologies, understanding of and leveraging contextual influences (i.e., social, and religious), and design guidelines.

The study outcomes are presented under two main categories; *'Privacy Protection Through Smart Device Design'*, and *'Perspectives and Challenges of Privacy Protection for Smart Device Design'*. The first category takes a design perspective, looking at the roles of designers and design processes. Here, we highlight the lack of manufacturers and designers in Jordan and the larger Muslim Arab Middle Eastern (MAME) region. We identify also that international companies and designers focus predominantly on Western contexts,

[1] Growth of smart devices in Jordan, See Jordan Digital Strategy
[2] Individuals who are subjected to the smart device use of others

and that designers are naturally skewed towards cultures and norms they are familiar with. From a design perspective, while privacy concerns are balanced against the need to consider companies' business viability, our study shows that the main target audience is overwhelmingly Western, and that innovation originates from a Western context. Non-Western contexts are addressed in the design process through localization; however, despite the fact that privacy is a highly contextual value, we found no indications that non-Western privacy concerns are part of localizing smart devices. Instead, we find that localization focuses on language, regional settings, and avoiding offensive dialects.

The second category highlights designer concerns around privacy protection, and how limited public awareness of privacy constrains design freedom. Designers also recognize the need to consider asymmetric power dynamics, especially for powerless groups (e.g., domestic workers). . We also investigate design challenges for privacy protection in Jordan and explore solutions that designers propose to address these challenges. This ranges from the need for improvements in the Semiotics of smart devices (especially the design of privacy signals), expanding the focus of localization of smart devices to include contextual privacy, design guidelines, novel regulation, adopting agile and cost-effective design practices, and the need for privacy by design (PbD) practices to be expanded.

Participants in our study emphasized the significance of regulation in addressing concerns related to asymmetric power dynamics, and powerless groups. They highlighted the need for increased international efforts and the establishment of standards to effectively tackle privacy protection challenges in Jordan. Furthermore, we delve into the broader significance of responsible innovation in designing privacy protection for smart devices. In conclusion, we propose several recommendations for interventions aimed at enhancing the design of privacy protection for smart home devices in Jordan. Additionally, we suggest several areas for further research.

2 BACKGROUND AND RELATED WORK

In the following section, we review prior work exploring user and bystander privacy concerns in smart homes, together with exploring privacy research in Muslim contexts. We then review research that highlights the interplay between privacy and power dynamics in smart homes, how privacy design contributions propose to address such problems, and conclude with a brief outline of the current state of relevant privacy regulation.

2.1 Privacy Concerns With Smart Home Devices

Smart devices raise significant concerns about privacy due to potential risks such as data leakage, abuse facilitation, and targeted burglary. Users often lack awareness of these threats, and usability issues can hinder privacy protection [5, 6]. Researchers have explored users' privacy concerns, perceptions, and expectations regarding smart home devices, uncovering vulnerabilities like smart TVs recording conversations [4, 7–17]. Privacy concerns and practices depend on contextual factors, with users perceiving public data collection as less critical than personal data. This blurring of boundaries becomes relevant in cases where domestic workers live and work in private homes [5, 18–21].

The Theory of Privacy as Contextual Integrity (CI) has provided insights into users' management of devices in negotiating boundaries between private and public settings. Power dynamics, contextual influences, and privacy concerns have emerged from this framework [22–26]. Users' awareness of privacy threats can drive their preferences and use of devices, with a need for clarity, control, and informed consent regarding data processing [19, 27–30].

2.2 Bystanders' Privacy Concerns with the Smart Home Devices

Smart home devices collect data about anyone in range of their sensors whether they are users or not (e.g., neighbours, household members, and bystanders). 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 [5, 31, 32]. Other researchers in this space have focused on multi-user privacy concerns [31, 33, 34]. There is a growing body of literature that explores smart home bystanders [35, 36]; however, more needs to be done to elicit, understand, and relate different privacy preferences—whether they come from users or bystanders [10, 34, 37–39].

There is no clear demarcation for where someone can become a bystander to smart devices, and this is happening in many social and even business settings [40–42]. Bystanders in general may not be aware of smart devices or what they are doing [43, 44]. And whether bystanders are aware or not of the presence of installed devices and what the devices are doing, they usually do not have adequate awareness of the privacy implications [4, 42, 45, 46]. Additionally, there are concerns that they may lack social or economic power to negotiate and enforce privacy preferences [2, 45, 47]. This paper aligns with some of our prior studies' findings [4, 48], which aimed to investigate privacy concerns and power dynamics of bystanders in smart homes in Jordan, however this study delves into the privacy protection design challenges associated with smart home devices in Jordan, and explores the concerns of designers regarding privacy protection challenges and proposes potential solutions.

Research studies have largely addressed bystanders primarily in Western contexts [16, 49, 50] and outlined different privacy protection strategies and actions, such as: a) Notifying users about devices; b) Permitting users to control data; and c) Using privacy-protecting default settings. However, privacy concerns remain, such as bystanders being unaware of the presence of smart devices, or the fact that control mechanisms are designed exclusively for the use of device owners. Ahmed et al. [46] have argued that smart devices should be designed to provide privacy assurances for everyone in range, and Marky et al. [42] argued that bystanders' weak awareness hinders privacy protection.

2.3 Privacy Design

Yao et al. [51] argued that socio-economic power dynamics in smart homes complicate privacy aspects, with little protection designed for bystanders. Privacy has been approached from two perspectives: focusing on home norms, practices, and values, and focusing on smart devices' technical capabilities and design characteristics. Researchers [25, 52] have studied privacy design in smart homes to enhance users' feelings of security and addressed bystanders'

concerns through new features like guest mode or voice command mute option. Responsible innovation in privacy protection design has been emphasized to mitigate negative societal impacts of technology use [53, 54].

Smart device manufacturers are urged [55] to implement reasonable security features to prevent unauthorized access, information disclosure, and modification. Artificial Intelligence (AI) is proposed for creating user profiles and monitoring behaviors. Differential privacy mechanisms have been highlighted [56] for their value in AI applications. Design semantics [57, 58] and semiotic features play a crucial role in enabling users to understand and interact with smart home devices, shaping user expectations and facilitating communication between users and devices. Moreover, Semiotic engineering has been applied to understand the appropriation of smart devices in homes and provide appropriation support [59, 60].

2.4 Privacy in Non-Western and Muslim Contexts

There is a need for privacy design to account for cross-cultural variations in users' attitudes and behaviors towards privacy, as many technologies still adopt a "one-size-fits-all" privacy design approach [61]. Cross-cultural studies often prioritize cultural factors over other measures like country and language, as cultural factors provide a framework for understanding diverse patterns of living across countries and can better predict privacy decisions [62]. Some studies have argued that privacy concepts vary substantially across cultures, time, and context [63, 64]. They note that the outcomes of privacy research studies in Western contexts may not be directly applicable to other non-Western contexts. Ahmed et al. [63], for example, highlight the social and cultural influences on the privacy of people who share mobile devices in the non-Western Muslim context of Bangladesh, and Mustafa et al. [65] highlight the importance of understanding Muslim identity, as Islam is the second-largest global religion [66], and consequently privacy research should address privacy concerns with smart devices in Muslim contexts. While some studies [67, 68] argue that human rights are embedded in Islam, and that privacy is a fundamental human right in Islam, there has been little research into how Islam influences smart device use, and we did not find any research that investigated the role of Islamic norms, practices and values on user privacy in the smart home.

2.5 Power Dynamics

Asymmetries between users in knowledge, skill and experience, in addition to imbalanced socio-economic power dynamics between smart home residents can cause multiple privacy impacts on users [69–73]. Kraemer et al. [74] argue that socio-cultural dynamics are linked to control of smart devices, and other studies argue that control over smart devices can result in domestic abuse [75, 76]. Research investigating the privacy concerns of smart home bystanders [32, 77] notes that even if bystanders could exert control over data, they would still share it because they did not feel like they could object. Another study found that bystanders' privacy protection is influenced by cultural aspects as well [78].

Other studies indicate that power dynamics among users can result in reduced privacy control for individuals with less power [50, 79, 80]. Power asymmetries within the home can create trade-offs affecting domestic workers' performance and satisfaction [81–83]. Smart devices can reinforce power dynamics among residents and lead to conflicts and distrust over device usage, raising questions about control and interpersonal dynamics [38, 74, 84–86]. Proposals to protect bystander privacy in smart homes include detecting hidden cameras [87–89], notifying users about data collection or transmission [42, 90, 91], using objects or contextual cues [52, 92–95], improving awareness [4], and promoting transparent discussion of device usage between bystanders and households [2, 41, 96]. However, trust in businesses and service providers to implement these measures remains a challenge [20, 52, 97].

2.6 Privacy Protection Regulations

At the time of writing this paper, it has been observed that Jordan lacks explicit privacy and data protection regulations. The existing applicable laws in Jordan, such as the Jordan Telecommunications Law (Article 71)[3], the Cybercrime Law (Article 3)[4], the Labour Law[5], and the Penal Code[6], partially address privacy concerns. However, the Jordanian government is in the process of developing a new data protection draft bill [98], inspired by the EU GDPR[7], which is expected [99] to establish a legal framework for personal data protection, introduce important concepts like consent, the right to be forgotten, and the right to remain anonymous. It is anticipated [99] that the new law will not specifically address privacy and data collection in smart homes, but will emphasize the identification of data ownership and the necessity of consent and awareness for data usage.

Regarding privacy protection for smart home bystanders globally, neither the data protection laws in the USA [100] nor the EU's GDPR) [101] explicitly address this issue. The US regulations are argued to place more responsibility on users for protecting their privacy, while allowing companies and government entities greater freedom to collect and trade data [102]. On the other hand, the EU GDPR [103] provides stronger protection for individual rights, encompassing various rights such as the right to be informed, right of access, and right to erasure.

3 METHODOLOGY AND RESEARCH QUESTION

This research study aims to answer the overarching research questions; "*How can we support privacy protection for domestic workers (i.e., bystanders) in the smart home in Jordan?*". To address this question, we broke it down into two questions: a) What are the design challenges of privacy protection for domestic workers in the smart home?, and b) How can design of smart home devices support privacy protection for domestic workers in the smart home?

Following similar approaches used in similar previous qualitative research studies [70, 104, 105], we designed and conducted a qualitative user research study with participants concerned with

[3]Jordan-Telecommunications Law
[4]Jordan-Cyber Crime Law
[5]Jordan-Labour Law
[6]Jordan-Penal Code – Article 348
[7]GDPR: EU-General Data Protection Regulation

smart home device design (i.e., designers, business leaders). We conducted semi-structured interviews focusing on understanding their concerns with data protection design of smart home devices. We focused on smart home devices (e.g., smart cameras, smart speakers, smart lights, smart door locks), because there are growing concerns [3, 4] about users' privacy with the increasing adoption[1] of these devices in Jordan. We engaged with local users (i.e., households and domestic workers) of smart home devices in Jordan, and with local manufacturers and importers of smart home devices in Jordan and in some neighbouring MAME countries, in order to explore their perspectives of privacy protection through smart device design.

In this paper, we use the term *Designers* to refer to participants involved in smart device design, the term *Users* to refer to local smart home device's users (i.e., households/families), and *Domestic Workers* to refer to local smart home device's passive users (i.e., domestic workers (bystanders)). We also denoted two types of business leader in our study: *International Business Leaders* who are leaders and executives of global companies that design and manufacture smart devices, and *Local Business Leaders* who are leaders and executives in local smart home device companies in Jordan and some neighbouring MAME countries.

We refer to Designers in the interview transcripts as D (e.g., [D01] being designer number 1), to International business leaders as L (e.g., [L01] being international business leader number 1), to Local business leaders as LB (e.g., [LB01] being local business leader number 1), and to Users (i.e., families/households) who own smart devices as H (e.g., [U01] being household number 1), and to Domestic Workers (i.e., bystanders) as W (e.g., [W01] being domestic worker number 1).

3.1 Recruitment

We followed a two-step process in our recruitment strategy. The first aimed at gaining an initial understanding of what smart home device design consists of, in order to guide our recruitment strategy for the second step. We have described this first step in more details in Section §5.1.1, where we discuss smart device design processes and designers in more detail. Based on this initial understanding, we developed our screening questionnaire survey as below (c.f. screening questions in Appendix-D):

- For designers. To have a minimum of two years experience with smart home device design.
- For international business leaders, To have a minimum of two years experience with managing smart home device designers and development teams
- For users (families and domestic workers), to have good knowledge of smart home devices.
- For local business leaders, to have a minimum of two years experience with smart home device industry/business.
- For all candidates, to have general knowledge of Jordan and/or MAME region contexts.
- For all candidates, to be able to communicate either in English or Arabic languages.
- For all candidates, to consent to participating in the interviews, and to being audio-recorded.

To recruit designers and international business leaders, we advertised the study on Linkedin groups (e.g., The Smart Device to Device Communications Group (Linkedin); The IBM AI, ML, IoT Group (Linkedin); IoT Design Group(Linkedin); Amazon Alexa and Google Home Professional Group (Linkedin); Smart Device Security (Linkedin); and other similar groups). Additionally, we searched the internet (i.e., Google, and Linkedin) to identify and reach out to potential candidates according to professional profiles. We experienced difficulties finding designers and international business leader participants willing to share their views and experiences with privacy and data protection, as data protection is considered sensitive, strictly confidential [106, 107], and to some extent a taboo topic [108] in many organizations. Therefore, many candidates chose not to participate, citing non-disclosure agreements (NDA) and business confidentiality obligations. To address this challenge, we used snowball sampling [109] that is commonly used to engage with hard-to-reach groups [110–113]. In the beginning, we recruited six smart device designers, and through snowball sampling, we were introduced to another 29 Designers and 22 International Business Leaders. (c.f. study poster for designers and international business leaders in Appendix-C).

To recruit users (families and domestic workers) from Jordan, we advertised the study on specialized social media groups (e.g., Ask Jordan (Facebook); Nurseries in Jordan (Facebook); Filipino in Amman (Facebook); Babysitters in Jordan (Facebook)) and we contacted smart device sellers, and domestic workers recruitment agencies in Jordan. Initially three user families got back in touch with us and using snowball sampling, we connected to another eight user families. Similarly, nine domestic workers connected with us. To recruit local business leaders we contacted local organizations and companies (e.g., Intaj[8]; Jordan Design and Development Bureau[9], Jordan Royal Scientific Society[10]; Jordan Chamber of Commerce[11]; UAE's Advanced Technology Research Council[12]; and Academy of Scientific Research and Technology in Egypt[13]) to advertise the study, and to identify and invite potential candidates from Jordan and some neighbouring MAME countries. We did not find designers or manufacturers in Jordan and neighbouring MAME countries. However, we found some participants who work in companies that import and distribute smart devices, or assemble pre-designed smart devices – originally designed in Western countries (c.f. study posters for households, workers, and local business leaders in Appendix-A, Appendix-B).

In contrast to our success in reaching international companies, our inability to find and recruit designers and local business leaders from Jordan and MAME countries is a strong indication that local companies manufacturing smart devices – if they exist – do not have tangible impact on smart device market share in MAME region. In support of this argument, we found that MAME markets are dominated by Western and East Asian smart products [114].

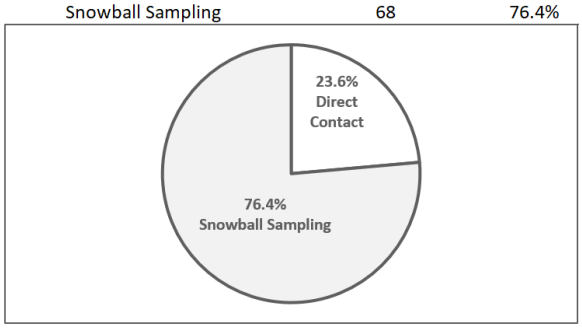
Despite not being able to recruit designers and local business leaders from Jordan and MAME countries, we engaged with smart

[8]INTAJ: The Information and Communications Technology Association of Jordan
[9]JODDB: Jordan Design and Development Bureau
[10]RSS: Jordan Royal Scientific Society
[11]JCC: Jordan Chamber of Commerce
[12]UAE Advanced Technology Research Council
[13]Egypt Academy of Scientific Research and Technology

device local agents and assemblers from Jordan and other MAME countries to identify the reasons behind lack of local manufacturers and designers, and whether they consider privacy protection for the smart products they import or assemble. We recruited three smart device local business leaders from Jordan, and using snowball sampling, we were introduced to another nine candidates practicing smart home device distribution and assembling in Jordan and other MAME countries (c.f. Fig.1 for details of recruitment channels)

Figure 1: Recruitment Channels

Recruitment Channels	Number of Candidates	%
Direct Contact [Email/Linkedin]	21	23.6%
Snowball Sampling	68	76.4%



We reached out to a total of 89 potential candidates, and 57 candidates filled in our screening questionnaire survey. From this, we recruited 44 participants (15 designers, nine international business leaders, eight local business leaders, six user families and six domestic workers) who represent 28 different companies, and 12 different households. Each of the nine international business leaders worked for a different company and the nine local business leaders worked for six companies. The 15 designers worked for 13 different companies (four large companies, and nine SMEs[14]), and the 12 users (i.e., families and domestics workers) were from 12 different households. To ensure domestic workers freedom of participation and for ethical considerations, we took steps to exclude participants (households or domestic workers) who are connected to other participants (households or domestic workers). However, we did not extend this exclusion measure to other participants (designers, business leaders, local business leaders).

For this research study, we chose Grounded Theory [115, 115, 116] as it is a well-established methodology for studying areas that have not been widely researched, and it can be deployed to construct substantive explanatory theories via a structured process of data collection, coding, and inductive reasoning. Grounded Theory enables a detailed examination of problems and helps to uncover the perceptions and beliefs behind practices, behaviors and incidents [117] (c.f. Fig.2 for research process and the applied methodology).

3.1.1 ***Participant Demographics.*** The demographics of our 12 users (i.e., families and domestics workers) (c.f. Table.1) consisted of six male and six female participants. Of the family users, one worked in education, two in finance, two in ICT, one in Telecom.

[14]Small and medium-sized enterprises

For the six domestic workers, two were home nurses, two were maids, and two were babysitters. All user families and two domestic workers were Jordanians, and the remaining four domestic workers were from the Philippines, Ethiopia, and Bangladesh. We defined users' competence with smart devices by using Dreyfus' model of skill acquisition [118]: Novice, Competent, Proficient, Expert, and Master.

The demographics of our eight local business leaders (c.f. Table.2) consisted of all male participants, of whom six worked in SMEs assembling smart devices, and two worked for local agent companies for international smart device companies. The demographics of our 15 designers (c.f. Table.3), consisted of three female participants and twelve male participants across 13 companies. seven worked as UX designers, one as GUI designers, three as solution architects, two as localization officers, and two as firmware designers. Six designers worked in a flexible team structure, five worked in cross-functional teams, and four in centralized design teams. The demographics of our nine international business leaders (c.f. Table.4), consisted of eight male participants and one female. They represented nine different companies selling different types of smart devices (e.g., Smart Door Lock, Smart Door Bell, Smart Light, Smart Camera..etc). All described themselves as having a technical background, and worked in different executive positions (e.g., CEO, CTO, CPO, PDO, and Team Business Leaders).

3.2 Methodology and Interviews

We conducted semi-structured interviews with 15 designers, nine international business leaders, eight local business leaders, and six user families, and six domestic workers. Interview scripts were structured using the funnel technique [119], which involves a gradual progression from general to specific questions. This method is commonly employed in research interviews to encourage a natural flow of conversation and enable the interviewer to gather detailed and pertinent information while establishing a rapport with the interviewee. Starting with broad, open-ended questions and then gradually narrowing the focus ensures that all relevant topics are covered without overwhelming the interviewee with too many detailed questions at once. The funnel technique is frequently utilized in qualitative research, particularly in studies employing semi-structured or unstructured interviews. We conducted and audio-recorded all interviews remotely using Zoom and Facebook Messenger, allowing participants time to explain their views. Interviews were guided by a list of prepared questions, but leeway was given to ask follow-up questions or skip some questions that had already been covered. In order to avoid response bias [120, 121], we adopted a strategy of using non-leading, neutral, and open-ended questions to inquire about privacy concerns, while actively listening and maintaining objectivity throughout the interviews.

Qualitative research provides detailed, subjective insights into complex phenomena from different angles [122]. A trained researcher conducted the interviews in English and Arabic (seven interviews in Arabic). The recruitment advertisement clearly requested volunteers to support this study, our participants were happy to volunteer, and no participant was compensated. Participants were free to withdraw their consent at any time and for any

Figure 2: Research Process and Methodology

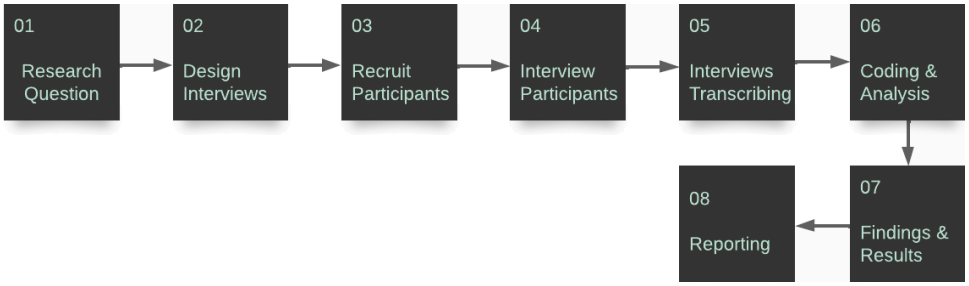


Table 1: Demographic Information of Users (Families and Domestic Workers)

P#	Gender	Nationality	Age Group	Degree	Field	Occupation	Competence	Smart Devices
U01	Male	Jordan	20-29	M.Sc.	ICT	Support Telecom Engineer	Proficient	Google Nest Audio, REOLINK Smart Camera, Sony Smart TV, Smart Door Lock
U02	Male	Jordan	30-39	B.Sc.	Finance	Accountant	Expert	Google Home, Roku Smart Camera, YeeLight Smart Light, Smart TV
U03	Male	Jordan	40-49	B.Sc.	Finance	Procurement Manager	Proficient	Nest Smart Thermostat, Hikvision Camera, Sifely Smart Door Lock, Smart Speaker
U04	Female	Jordan	30-39	B.Sc.	Education	Teacher	Expert	Google Nest Audio, Hikvision Camera
U05	Male	Jordan	30-39	M.Sc.	ICT	Software Engineer	Proficient	Amazon Echo Dot, Merkury Smart Camera, YeeLight Smart Light
U06	Male	Jordan	40-49	B.Sc.	Telecom	Telecom Service Manager	Expert	Amazon Echo Dot, Samsung Smart TV
W01	Female	Jordan	40-49	B.Sc.	Medical	Home Nurse	Competence	Amazon Echo Dot, LIFEX Smart Light, LG Smart TV, Hikvision Smart Camera
W02	Female	Philippines	20-29	High School	Home Care	Babysitter	Competence	Google Home, Samsung Smart TV, Hikvision Smart Camera
W03	Female	Philippines	20-29	Diploma	Home Care	Babysitter	Competence	Google Home, LG Smart TV, REOLINK Smart Camera
W04	Male	Jordan	30-39	B.Sc.	Medical	Home Nurse	Expert	Amazon Echo Dot, Sony Smart TV
W05	Female	Ethiopia	20-29	High School	Home Care	Domestic Worker- Maid	Novice	Google Home, Smart Camera
W06	Female	Bangladesh	20-29	High School	Home Care	Domestic Worker- Maid	Novice	Smart Camera

Table 2: Demographic Information of Local Business Leaders

P#	Gender	Age Group	Education	Role	Experience (Years)	Company Size (Type)	Company Location	Products
LB01	Male	30-39	BSc	Technical Support Manager (Assembly)	6	10-100 (SME)	Jordan	Smart Electric Plugs
LB02	Male	30-39	BSc	Assembly Line Supervisor	8	250-500 (SME)	Jordan	Smart TV
LB03	Male	50-59	MSc	CTO (Local Agent)	9	10-100 (SME)	Jordan	Smart Cameras
LB04	Male	40-49	BSc	CEO & Founder(Assembly)	6	10-100 (SME)	Jordan	Smart Electric Plugs
LB05	Male	40-49	MSc	Technical Support Manager (Assembly))	7	10-100 (SME)	UAE	Smart Security Systems
LB06	Male	40-49	BSc	CTO (Local Agent)	7	10-100 (SME)	UAE	Smart Security Systems
LB07	Male	30-39	MSc	Production Lead Engineer(Assembly)	6	250-500 (SME)	Egypt	Smart Home Appliances
LB08	Male	30-39	BSc	Assembly Line Team Leader	9	250-500 (SME)	Egypt	Smart Home Appliances

Table 3: Demographic Information of Designers

P#	Gender	Age Group	Education	Role	Experience (Years)	Company Size (Type)	Company Location	Products
D01	Male	20-29	BSc	UX Designer	6	250-500 (SME)	UK	Smart Activity Tracker
D02	Male	20-29	BSc	Solution Architect	12	10-100 (SME)	USA	Smart Door Locks, Smart Door Bell
D03	Female	30-39	PhD	UX Designer	8	250-500 (SME)	Germany	Smart Security System, Smart Lights, Smart Sensors
D04	Male	20-29	BSc	Solution Architect	7	250-500 (SME)	UK	Smart Door Locks, Smart Door Bell
D05	Male	30-39	BSc	Localization Team Leader	7	>1000 (LE)	Germany	Smart Home Automation
D06	Female	40-49	BSc	Solution Architect	11	>1000 (LE)	UK (Chinese Company)	Smart Camera, Smart Baby Camera
D07	Male	20-29	BSc	Firmware Designer	6	250-500 (SME)	UK	Smart Security System, Smart Sensors
D08	Female	40-49	PhD	GUI Designer	12	>1000 (LE)	USA	Smart Speaker, Smart Home Hub
D09	Male	20-29	BSc	UX Designer	6	>1000 (LE)	USA	Smart Speaker, Smart Home Hub
D10	Male	20-29	BSc	UX Designer	4	>1000 (LE)	Holland	Smart Camera, Smart Light
D11	Male	30-39	BSc	Localization Officer	7	10-100 (SME)	UK	Smart Thermometer
D12	Male	40-49	BSc	Firmware Designer	10	>1000 (LE)	UK (Chinese Company)	Smart Indoor/Outdoor Camera
D13	Male	20-29	PhD	UX Designer	5	100-250 (SME)	Germany	Smart Toys, Smart Baby Monitors
D14	Male	20-29	BSc	UX Designer	4	100-250 (SME)	USA	Smart Light, Smart Electric Plugs, Smart Home Automation
D15	Male	30-39	MSc	UX Designer	9	10-100 (SME)	UK	Smart Baby Camera

reason. No participants withdrew.

3.2.1 Pilot Study: We conducted a pilot study of five semi-structured interviews to check that the questions in the five interviews scripts (e.g., user families, domestic workers, local business leaders, designers, and international business leaders) were clear

Table 4: Demographic Information of International Business Leaders

P#	Gender	Age Group	Education	Background	Role	Experience (Years)	Company Size (Type)	Company Location	Products
L01	Male	30-39	PhD	Electronic Engineering	Product Manager	9	10-100 (SME)	UK	Smart Door Lock
L02	Male	50-59	BSc	Electronic Engineering	CEO & Founder	7	10-100 (SME)	UK	Smart Light
L03	Female	20-29	PhD	Computer Science	Design Team Leader	4	100-250 (SME)	USA	Smart Camera
L04	Male	30-39	BSc	Digital Electronics	CTO	10	10-100 (SME)	USA	Smart Activity Trackers
L05	Male	40-49	BSc	Mechanical Engineering	Technology Lead	12	10-100 (SME)	USA	Smart Heating System
L06	Male	30-39	BSc	Electronic Engineering	Chief Product Officer	10	100-250 (SME)	UK	Smart Mops
L07	Male	50-59	MSc	Digital Electronics	CEO & Founder	9	10-100 (SME)	USA	Smart Cups, Smart Mugs
L08	Male	30-39	BSc	Computer Science - AI	CTO	8	100-250 (SME)	UK	Smart Door Lock
L09	Male	40-49	MsC	Computer Science	CEO	12	10-100 (SME)	Spain	Smart Tracking Sytems

and easy to understand, and to identify any problems in the interviews scripts. We selected five experienced researchers from our institution who have backgrounds relevant to the study domain, and conducted one pilot interview for each participant group. As a result, the pilot study feedback was centered on improving question phrasing, the sequence of questions, and enhancing the comprehensibility of some questions.

3.2.2 User Families' Interviews: We asked family users to describe their smart devices, how they use them, what data they thought was collected, and about their understanding of data protection rights and regulation. We also asked about how they thought smart home device companies use their data, how much they trust these companies, and whether they have any concerns with the functions and design of their smart devices. All the families involved in the study were of Jordanian nationality. Three of the families opted to conduct the interviews in English, whereas the other three families chose to conduct the interviews in their native Arabic (c.f. families' interview guidelines in Appendix-E)

3.2.3 Domestic Workers' Interviews: We asked domestic workers to describe the smart devices in the homes they work in, whether families had informed them about devices, how they found out about the devices, whether they were allowed to use devices and how they used them. We also asked about the data they thought was collected about them, whether they could discuss using smart devices with households, and their understanding of data protection rights. We also asked about how families and companies use their data, how much they trust families and companies, and whether they have any concerns with the functions and design of the devices. The study involved domestic workers from multiple nationalities including Jordan, the Philippines, Bangladesh, and Ethiopia. While the non-Jordanian workers chose to conduct the interviews in English, the Jordanian domestic workers opted to do the interviews in their native Arabic language (c.f. workers' interview guidelines in Appendix-F).

3.2.4 Local Business Leaders' Interviews: We started by asking general questions regarding the participant's role, what their companies do, and about the challenges of designing and developing smart devices in Jordan and MAME countries. We asked questions about the smart products they sell, their future plans, their customer base, their technology partners, and their markets. In addition, we asked about localization of smart devices, challenges of manufacturing smart devices locally, their experience with local data protection regulations, whether their companies comply with them and their wider data protection strategy. We also asked about whether data protection was discussed with their technology partners, and about compliance with international and local regulation. Of the local business leaders who participated in the study, six participants opted to do the interviews in English, while two participants opted to do their interviews in Arabic (c.f. local leaders' interview guidelines in Appendix-G).

3.2.5 Designers' Interviews: We started by asking designers general questions about their roles, the type of smart devices they design, and their experiences with design and with data protection. We then asked questions about requirements gathering, localization of smart devices, how design processes address data protection (e.g., data protection design decisions, techniques and algorithms, and artifacts) and about compliance with regulation. Given that all designers in the study were either of Western or non-Arabic origin, all these interviews were conducted in English (c.f. designers' interview guidelines in Appendix-H).

3.2.6 International Business Leaders' Interviews: We started by asking participants general questions regarding their role, their business goals and objectives, their future expansion plans, the smart products they produce and sell, their customer base and markets, localization of smart devices, and adoption of innovative technology outcomes. Additionally, we asked about experience with data protection, business challenges, compliance with regulation (e.g., GDPR[7], CCPA[15]), and how to ensure and improve data protection with current and future products for customers in international markets—especially those in non-Western contexts (Jordan and MAME). All the international business leaders in the study were of Western or non-Arabic origin, and the interviews were conducted in English (c.f. international business leaders' interview guidelines in Appendix-I).

3.2.1 ***Data Analysis.*** Following Strauss and Corbin's Grounded Theory procedure [115, 115, 116], we transcribed the audio recordings. Using NVivo 12 Pro[16] software, we analyzed a total of 44 semi-structured interviews. Two researchers analyzed the interview scripts. Author#1 (the primary researcher) and author#2 (the principal investigator of this research study) independently did the

[15]CCPA: California Consumer Privacy Act
[16]NVivo Pro 12: An application that lets users organize, analyze and visualize information

initial coding of all interview scripts. During the coding process, author#2 discussed, asked and requested some clarifications and insights, and author#1 annotated the study scripts to provide additional data and context. 356 codes emerged forming the study codebook from the initial coding (c.f. Table.5). Then we applied the emerged codes across other interviews through constant comparison. New emerged codes were added as they were deemed relevant and necessary. Then the two researchers grouped the emerged codes into themes (axial coding) and categories (selective coding), based on the dimensions and properties of every theme. For constant comparison, codes were shared across all interviews. Axial coding allowed grouping different perspectives and experiences from all participants: user (families, and workers), designers, international business leaders, and local business leaders. The two researchers held regular meetings to discuss emerging codes and to group them together.

We observed data saturation separately for all our participant groups. We observed data saturation [117, 123, 124] between the 7th and the 8th interview for international business leaders, the 13th and the 14th interview for designers, the 6th and 7th interview for local business leaders, the 5th and the 6th interview for families, and between the 5th and the 6th interview for domestic workers. As a methodological principle in qualitative research, data saturation is used as an indication that no further data collection is needed. After completing the final codebook, and to verify the reliability of the study codebook, we tested for inter-rater reliability and found that the average Cohen's kappa coefficient (κ) for all codes in our data was 0.84, indicating perfect agreement [125]. Moreover, we tested the identified codebook for reliability and credibility using grounded theory triangulation [126] by randomly selecting 13 participants (i.e., four designers, three international business leaders, two local business leaders, two user families, and two domestic workers) and asking them to comment on the generated codes and themes, and to establish whether they agreed with the findings. We found a clear consensus between participants on the identified categories and themes; however, their comments enabled us to identify some additional insights, which we used to increase and clarify our existing codes. This added more detail but did not generate new themes, and in total we identified 372 codes which we organised into the categories and themes presented in Section §5.

In total, the interviews consisted of six hours and 36 minutes for international business leaders (average of 44 minutes per interview), 13 hours and 15 minutes for designers (average of 53 minutes per interview), four hours and 40 minutes for local business leaders (average 35 minutes per interview, and seven hours and 24 minutes for users (average 37 minutes per interview). The main researcher translated the Arabic interviews, and made a conscientious effort to preserve the participants' views and ideas in the translations without any bias or alteration.

3.2.2 ***Research Ethics.*** Our study was reviewed and approved by the University of Oxford - Central University Research Ethics Committee (CUREC) [Approval: CS_C1A_22_007]. Before every interview, we asked interviewees to read the study information sheet explaining the high-level purpose of this study and outlining our data-protection practices. We also asked participants to read the study information sheet before asking for consent, and all participants agreed to record their verbal consent. Due to the sensitive topic of this study (e.g., privacy, security, compliance), we asked interviewees not to name specific companies, people, products, or sites. All interview scripts were password protected and stored in a physical safe in our university site. Participants had the option to participate or to withdraw at any point without providing an excuse or explanation. We explained to all participants that in case of their withdrawal, none of their collected data would be used in the study analysis. No participant withdrew.

4 LIMITATIONS

Similar to all qualitative research studies, this study has some limitations:

Language: Participants were given the choice to conduct interviews in English or Arabic. Most interviews were conducted in English, except for seven interviews conducted in Arabic with participants who preferred their native language. These interviews were translated into English while taking care to maintain the participants' views. Some non-native English speakers faced difficulties expressing themselves clearly, but we believe it did not significantly impact our analysis when we cross-verified the study outcomes through triangulation.

Research Quality: The quality of qualitative research depends on researchers' skills and can be influenced by personal biases. Inexperienced researchers may struggle with conducting effective interviews and probing into important topics, potentially resulting in missing relevant data [127, 128]. To mitigate this, the primary researcher conducting all 44 interviews, is trained in how to design and conduct interviews carefully, asking questions in an neutral and open manner in order to avoid influencing interviewees.

Bias: Self-reporting bias is common in interview studies [129]. Participants may forget details or respond inaccurately, influenced by their desired perception [130]. To enhance validity and minimize self-reporting bias, we used open-ended questions and encouraged participants to provide detailed answers. For participants with brief responses, the researcher requested additional details.

Recruitment: As discussed in the methodology section, we experienced difficulties in finding and recruiting participants willing to share their views due to legal or company obligations, and the sensitivity and confidentiality of the research topic. Also, despite significant effort, we were unable to recruit any international business leaders from large organizations. As a result, this qualitative research study is limited by the size and diversity of recruited sample.

Topic Sensitivity: Due to the sensitivity of security, privacy, and regulatory topics, participants may have provided biased or incomplete answers out of concern for corporate responsibilities and reputation. To address this, we explained our security and privacy measures, emphasizing data anonymization, encryption, and compliance with the GDPR[7].

Generalization: It is important to note that our study is qualitative in nature, and therefore does not aim to quantify findings or make generalized observations applicable to a wider population. The insights we present reflect the perspectives of our 44 participants and are not generalizable. The primary focus of this qualitative

research is to provide a deep understanding of the subject matter rather than producing generalizable outcomes. Any hypotheses derived from our findings and grounded-theoretic analysis would require further testing in a confirmatory study to determine their broader applicability and generalizability.

5 FINDINGS AND OUTCOMES

This section presents the findings of our study into smart home device design challenges for data and privacy protection in Jordan. We present and discuss these under two key categories: 1) Privacy Protection Through Smart Device Design (Section §5.1), and 2) Perspectives and Challenges of Privacy Protection With Smart Home Device Design (Section §5.2) (see Fig.3, and Table.5).

5.1 Privacy Protection Through Smart Device Design

We focus on exploring the design perspective on privacy protection for smart devices by first exploring design processes and the role of designers. We then outline key challenges for local design and production of smart devices in Jordan and MAME region. Next we identify and explore how smart devices are made more contextual through the process of localization. We conclude that Jordan and the wider MAME region are overlooked both in the design process of smart home devices and the representation of the region in the design profession and manufacturing of smart devices.

5.1.1 ***Design Process and Designers.*** As discussed in Section §3.1, to recruit the right sample of participants for this study, we conducted preliminary research on the design profession and processes of smart home devices. We interviewed three individuals who identified themselves as smart device designers to gain insights into their roles and the tasks they perform. Through open-ended questions, we explored their responsibilities, required skills, the design tasks related to security and privacy protection, and their understanding of smart device design processes. Drawing from our findings and relevant literature on smart device design [131–133], we define smart home device designers as *"the executives, individuals and teams involved in the design processes of smart home devices, including members of creativity teams, product development teams, and technical development teams (such as GUI Designers, UX Designers, Software and Firmware Designers, Localization Officers, and Solution Architects)"*.

The design process can be summarized in five key steps: 1) *Concept Generation*: Marketing and creativity teams define the device's concept and functions, consulting with the technical team. 2) *User Modeling*: Marketing and creativity teams identify the target audience and group users based on factors like age, gender, socioeconomic status. 3) *Visualization Sketch*: Imagining the device and user interactions. 4) *Design*: Technical Product Development Team determines cost, logic, appearance, GUI, UX, localization, and compliance. 5) *Prototyping*: The team creates MVP (minimum viable product) or prototypes categorized as visual, proof-of-concept, and presentation models (c.f. Fig.4).

5.1.2 ***Lack of Manufacturers and Designers in Jordan and MAME Region.*** Local business leaders and designers (N=12) emphasized the value of local design and manufacturing of smart devices in addressing user concerns within the specific context. [LB08] said: *"We can make devices more suitable for users when we design and make them locally"*, and [D09] said: *"I was born here, and I know what users want"*. Our findings reveal a lack of smart device manufacturers (involved in designing and producing smart devices) in Jordan, which poses a challenge in developing contextually tailored devices for the country.

Local business leaders pointed to Research & Development costs, the limited size of nascent MAME markets[17], and economies-of-scale[18] were impediments to production of smart devices in Jordan and the wider MAME region. [LB04] said: *"I do not think there is a business case for that"*. Participants argued that it is more feasible (i.e., cost, time, quality) for local manufacturers of smart devices to assemble pre-designed smart devices from international companies. [LB07] said: *"We manufacture smart TVs, but we do not design and develop them [TVs] from A-Z. We import all parts from our international partners, and we assemble them locally"*. Another participant highlighted that Jordan and MAME markets are dominated by international smart home products (e.g., Western & East Asian), as users tend to place more trust in international brands rather than locally produced or assembled products. [LB06] said: *"Markets in our region [MAME] are dominated by foreign smart products"*, and [LB08] said: *"Customers generally trust foreign smart products [Western and East Asian]. And even foreign brands assembled locally are not really trusted"*. He added that design and innovation mainly come from the Western world [LB08]. However, [LB04] argued that there are some start-ups in Jordan and other MAME countries, however, it will take time before they have tangible market share and become able to compete with international players.

5.1.3 ***Muslim Arab Middle Eastern Contexts Are Overlooked.*** Designers (N=8) argued that smart device manufacturers, and the target audience for design processes, are largely Western (e.g., North America, Europe). [D13] said: *"Most smart device manufacturers and customers are mainly Western"*, and another designer argued that companies and designers focus on Western contexts. [D14]. This finding indicates that the Jordanian context is overlooked within design processes. In support of this conclusion, another local business leader argued that social, religious, and geopolitical sensitivities in MAME region are not considered within the functionalities of available smart devices in local markets. [LB02] said: *"I believe smart devices in the markets are not designed for our region. Just recently, some smart home assistants can understand some Arabic phrases in Egyptian and Saudi dialects, but its abilities are not good enough to fully understand what users say. When they respond in Arabic, you feel the Western way of saying things"*.

Designers (N=5) argued that with the absence of organizational strategy to address certain contexts, the impact of employees' culture on design processes is minimal, and added that in large companies, the role of organizational strategy, business culture, and business processes has greater importance [D01]. However, participants added that designers could have some influence on design processes in SMEs [D07]. It is worth mentioning that during the recruitment phase of this study, we found some designers and executives from MAME origins working in Western companies, but they

[17] Report-Smart Homes Devices Market in the Middle East, Turkey, and Africa
[18] Economies-of-Scale relates cost of production to production volume and market size.

Figure 3: Visual Presentation of Categories and Themes

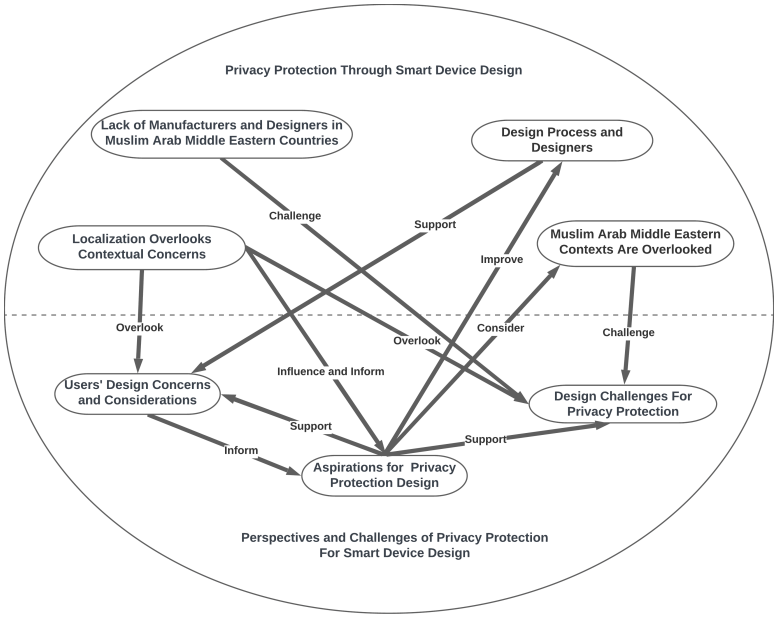


Table 5: Summary of Categories and Themes

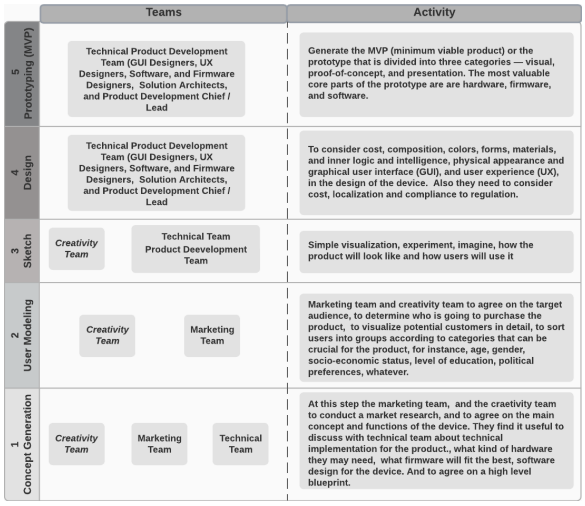
Categories	Themes	Sun-Themes
Privacy Protection Through Smart Device Design	**Design Process and Designers**	Five Steps Design Process and Who Are Designers
	Lack of Manufacturers and Designers in Muslim Arab Middle Eastern Countries	Easy to Design For Your Context
		Context Based Design
		Context Aware Devices
		Local Production of Smart Devices
	Muslim Arab Middle Eastern Contexts Are Overlooked	Designers Are Skewed Toward Cultures They Know
		Target Audience For Design, and Manufacturers Are Largely Western
	Localization Overlooks Contextual Concerns	Localization of Smart Home Devices in Muslim Arab Middle Eastern Markets
		Users are Mainly Concerned about Device's Functions More Than Data Protection
		Short Sighted Localization of Smart Devices
		Cost of Localization
		Users Buy Smart Home Devices From International E-Commerce Platform
Perspectives and Challenges of Privacy Protection For Smart Device Design	**Users' Design Concerns and Considerations**	Privacy and Security Concerns with Smart Device Design
		Concerns of Smart Home Bystanders and Power Dynamics
		Concerns About Default Deceptive Privacy Settings
		Tricky Privacy Policies
	Design Challenges For Privacy Protection	Design Cost
		Aligning Data Protection with Business Viability
		Limited Awareness Constrains Design Freedom
		Lack of Explicit Regulations, and Standard Design Guidelines
		Privacy Protection Design Challenges For Muslim Arab Middle Eastern Countries
		Feasible Solutions For Privacy Protection Design
	Aspirations for Privacy Protection Design	Awareness, Regulation, and Users' Feed backs
		Privacy by Design
		Semiotics For Smart Devices' Signals
		Innovative Technologies
		Empower Companies to Become Responsible Stewards of Users' Data

were unable to participate due to being bound by NDA[19] contracts, and due to the sensitivity of the study (e.g., privacy and security issues). However, based on the findings of this study, we believe that their influence on design processes is minimal unless there is an organizational direction to study and accommodate other contexts.

5.1.4 ***Localization Overlooks Contextual Concerns.*** Participants (N=9), including both local and international business leaders and designers, emphasized the significance of localization in the context of smart devices. Localization encompasses various aspects such as language translation, regional settings, avoiding offensive content, and considering local geopolitical sensitivities. According to [LB06]: *"We [companies] ensure that devices have Arabic language and time zone settings"*, and participants acknowledged that users

[19]Non-Disclosure Agreement

Figure 4: Smart Device Design Process



primarily prioritize device functions, price, and ease of use. Designers also highlighted the importance of *Inclusive*[20], *Accessible*[21], *Non-Offensive*[22], *Ethical*[23], and *Relevant*[24] design [D04].

Moreover, designers argued that manufacturers employ self-censorship to address taboo topics or subjects that are incompatible with the local culture. [D05] expressed: *"I think they [companies] do the minimum, and sometimes they do kind of self-censorship to avoid upsetting the local population"*. International business leaders argued that smart device localization overlooks most contextual sensitivities (social, religious, cultural), but if companies become aware of an issue, they may try to manage it subject to cost considerations [L01]. However, [LB05] explained that localization is business driven, costly, and companies will invest only when it is feasible for them. From another side, local business leaders described current localization practices as *'Short Sighted Localization'* of Smart Devices [LB06], and in another discussion, international business leaders highlighted that many users are buying smart devices from international e-Commerce platforms (e.g., Amazon, Alibaba, ebay) which makes it difficult for manufacturers to preconfigure devices to fit certain contexts [L09]. To address localization challenges, they added that it is important to have a kind of *'Universal Design Settings'* that automatically tuned to users' context (i.e., location) .

[20]Inclusive design considers the full range of human diversity with respect to ability, language, culture, gender, age, and other forms of human difference.
[21]Accessible design aims to make sure that people with disabilities can access and use smart products effectively.
[22]Non-Offensive design avoid causing someone to feel resentful, upset, or annoyed.
[23]Ethical design refers to design that resists manipulative patterns, respects data privacy, encourages co-design, and is accessible and human-centered.
[24]Relevant design is connected with its context in ways that satisfy users and societal needs and concerns.

5.2 Perspectives and Challenges of Privacy Protection for Smart Device Design

Our second category of findings explores concerns and challenges with smart device design and privacy protection. International business leaders argued that data protection is costly and dependent on 'economies-of-scale', adding that SMEs cannot afford it. Designers and international business leaders highlighted some privacy protection design considerations and challenges such as limited awareness of stakeholders (i.e., users, companies, and regulators), lack of explicit regulation and standard design guidelines, and the impact of the asymmetrical smart home power dynamics. Finally, local business leaders discussed privacy protection design challenges for MAME region, and designers highlighted some practices to mitigate privacy protection design challenges.

5.2.1 ***Users' Design Concerns and Considerations.*** Users mentioned some security and privacy concerns with smart home device design: they experienced dark patterns, tricky privacy policies, asymmetrical power-dynamics, and wondered if devices could recognize bystanders in range.

5.2.1.1 Privacy and Security Concerns with Smart Device Design Users (both families and domestic workers) (N=12) mentioned that they are mainly concerned about audio-visual smart devices, and showed interest in learning about the potential impact of other types of smart devices on them [U04][W05][W06][U03], and added that they did not know if devices could be remotely accessed by criminals or hackers [U04]. A worker also mentioned that she is not sure if the family records her [W05]. Users recognized that privacy threats in the smart home exist on two fronts: external threats originating from outside the home, such as companies, hackers, criminals, and curious individuals, and internal threats posed by users who have control over the devices within the home and target individuals with limited device usage, including passive family members and bystander domestic workers [U06]. Participants emphasized the importance of designing privacy protection measures that address both types of threats.

5.2.1.2 Concerns of Smart Home Bystanders and Power Dynamics: Users (N=10) mentioned that privacy rights are compromised in exchange for using devices and receiving benefits. [U04] said: *"I would not care too much about my data, if that will prevent me from using the device"*, and [U01] confirmed that by saying: *"We need to be less sensitive about our data when we use smart devices"*. Participants highlighted the unique situation of domestic workers (e.g., maids, babysitters, nurses) and the challenges they face in discussing privacy rights with the families they work for. They emphasized that domestic workers are primarily present in the home as employees rather than as family members, which can create barriers to open discussions about privacy rights. This asymmetrical power dynamic between families and domestic workers was evident in the statement of [U04] who said, *"I have a maid. I do not discuss with her about my cameras. This is my home and she is working here"*. Additionally, participants mentioned that their domestic workers do not use the smart devices [U03].

A female worker mentioned that she adopts some practices to protect her privacy such as refraining from speaking or hiding her

face with her veil when she is close to devices in obedience to her beliefs as Muslim woman. [W01] said: *"I do not speak and I put my veil on my face when I am close to the cameras, I am Muslim and I do not accept recording my voice and my face without hijab*[25] *"*. Users have shown concerns about device's capabilities to recognize non-profiled users (e.g., bystanders). [U03] said: *"I do not think my Alexa recognizes her [the maid]"*, and another domestic worker [W04] wondered whether devices are designed to recognize people in range. A female domestic worker also argued that female foreign domestic workers are considered a powerless group in Jordan, and she wondered if smart devices could be designed to protect this group. [W02] said: *"Governments and big companies need to protect us [female foreign domestic workers]"*, and as a result of the asymmetrical power dynamics, she said she had to compromise her privacy rights in order to keep her job. In contrast, another worker argued that workers have complete rights in smart homes, and households treat them well [W03]. While acknowledging the challenges of doing so, one designer [D04] argued that design of smart devices should identify and mitigate the socioeconomic power dynamics negative impacts on users' agency.

5.2.1.3 Concerns About Deceptive Privacy Settings and Lack of Trust. Users (N=8) expressed concerns about hidden deceptive and invasive privacy default settings. [U01] said: *"Google Nest uses records of coughing and snoring event information to inform us about sleep quality, and it [Google Nest] used data of our interaction with our smart door lock to offer automatic locking of doors at identified times"*. Users expressed their concerns about the intrusive nature of collecting and analyzing personal data. [U06] highlighted the issue with smart TVs automatically connecting to Wi-Fi and having default settings that require manual adjustment to disable certain features. He said *"Some smart TVs connect automatically to Wi-Fi— everything is by default ON and you have to go digging into settings to turn some of it off"*. When asked about users' awareness of Data Subject Access Requests (SAR[26]), one user shared his experience of submitting a SAR to find out what data companies hold about him, how his data is collected and used, and with whom it is shared. However, he did not receive any responses [U05]. This lack of response may be attributed to the absence of explicit data protection regulation in Jordan. Nonetheless, users expressed their desire for companies to consider SAR requests from any region, as they perceive a sense of regional discrimination [U05]. In contrast, international business leaders affirmed that companies, especially larger ones, address SARs from any region [L03].

Moreover, users expressed distrust in smart device companies, as they believe that making profits outweighs anything else. [U01] said: *"I do not trust them [manufacturers], they would do anything to grow their businesses"*. Workers also expressed a lack of trust in companies, but also in their employer families. [W03] said: *"they use cameras because they do not trust us, and I do not trust what they can do to me. They are good family, but may be they put it [data] on social media... I don't know, but I do not trust social media [companies]"*. This situation represents a critical issue of *lack of trust* for smart home users, bystanders, and smart devices companies.

5.2.1.4 Tricky Privacy Policies. Users (N=7) raised concerns regarding the lack of freedom of choice when using smart devices. They expressed that the terms and conditions in privacy policies tend to favor service providers, leaving users feeling compelled to accept and agree to them [U03]. Additionally, users noted that companies employ persuasive tactics to encourage users to accept privacy policies, which can be challenging for lay users to understand them [U05]. Furthermore, users mentioned that they use a single account for their devices, without creating individual accounts for each household member. They explained that their workers do not have personal accounts on the devices as they do not use them [U03]. Consequently, the consent provided by the account owner applies to all users within the device's range, including family members and bystanders, which represents a privacy protection challenge in multi-user settings where no restrictions are placed on how the account owner (the administrator) uses others' data.

5.2.2 ***Design Challenges For Privacy Protection***. International business leaders, local business leaders, and designers (N=18) argued that data protection is costly, business driven, and geopolitical dependent. They showed how explicit data protection regulation, standard design guidelines, and stakeholder's' awareness are important to privacy protection design. Finally, they mentioned some interventions and aspirations to overcome privacy protection design challenges.

5.2.2.1 Design Cost International business leaders (N=6) highlighted that companies consider data protection to gain and maintain customers' trust, and to comply with existing data protection regulation [L06][L07]. However, international business leaders explained that considering data protection within the design of smart devices increases production cost as it requires investments in R&D, in addition to recruitment of skilled human resources [L03], and added that many SMEs do not have the financial capabilities to handle the costs of data protection with smart device design. In the same discussion, international business leaders mentioned that economies-of-scale, company size, and financial power affect their ability to consider data protection with smart device design [L01]. They argued that SMEs cannot bear the high non-compliance fines compared to giant players, highlighting that fines are the same for all small and big companies. [L04] said: *"The ICO*[27] *is fining companies like Amazon*[28] *for non-compliance with GDPR. For us, we are small company, we will go bankrupt if we receive such fines"*, and L08] said: *"regulators do not differentiate between small and big companies when they fine them"*. Moreover, international business leaders said that data protection is a secondary consideration for some companies, and they would only take some steps in that direction to comply with specific regional requirements or to add a feature list [L08].

5.2.2.2 Feasible Solutions For Privacy Protection Design Designers (N=11) mentioned that they used different approaches

[25] A head cover garment worn by Muslim women to cover their hair.
[26] GDPR- Art. 15: Right of access by the data subject
[27] ICO: The United Kingdom, Information Commissioner's Office
[28] For more details, see: GDPR fines against Amazon

to address privacy protection design challenges, such as using penetration tests, common sense and heuristics (e.g., generalizations). Additionally, they mentioned that they consulted with team leaders and other colleagues, and also copied what other manufacturers did in similar situations. [D03] said: *"We discuss with other experts, and sometimes we use common sense, or just check what other designers do in similar situations"*, and [D15] said: *"We use heuristics, and 'tried-and-tested' methods to overcome design challenges"*.

5.2.2.3 Aligning Data Protection with Business Viability International business leaders (N=5) emphasized the challenge of balancing data protection with business viability. They acknowledged that companies view data as a valuable asset for generating revenue and sustaining their operations [L02]. While companies benefit from user data to drive business growth, aligning data protection requirements with their goals poses a challenge. However, international business leaders highlighted ongoing efforts to enhance data collection processes, ensuring both business viability and privacy risk mitigation [L04]. Moreover, some participants expressed the view that *'companies prefer an opaque regulatory environment to continue exploiting users' data'* [L05]. In a broader sense, a designer pointed out the inconsistency between companies' practices towards data and the design processes for privacy protection. Some companies prioritize minimal compliance with existing regulations [D11], while others aspire to provide comprehensive protection that goes beyond regulatory requirements [D06].

5.2.2.4 Limited Awareness Constrains Design Freedom Users (families and domestic workers) (N=9), showed limited awareness regarding the purpose of data collection, its usage, storage locations, and retention periods. This lack of awareness, coupled with limited competence in using smart devices, has resulted in an underestimation of the value of personal data and a disregard for privacy threats and potential risks. For example, [U02] said: *"I really do not know why they collect it. I believe there is nothing special about me"*. Similarly, [W05] mentioned: *"I do not know how to use smart devices in a good way... I do not mind if they record me... They are just recording me while I am doing my work"*. On the other hand, some users expressed curiosity about the value of their data and how organizations profit from it [U03].

International business leaders (N=3) drew attention to the concept of data as the *"New Oil"* for revenue generation and the *"New Uranium"* due to potential security and privacy risks [L02]. However, the value of data is not evident to many users, and they lack knowledge about privacy rights and whether such rights exist [U05]. Moreover, international business leaders emphasized the importance of considering context and geopolitics in privacy design, urging companies to be mindful of these sensitivities [L05]. Designers (N=7) explained that stakeholders' (users, international business leaders, designers, and regulators) limited awareness of smart technologies, contextual privacy concerns, and regulation could constrain design freedom and limit design capabilities in identifying and addressing users' privacy protection needs [D08]. Additionally, designers argued that companies and designers tend to address privacy concerns of contexts they are aware of as it is easier for them to identify and address privacy protection needs. [D05] said: *"Companies and designers are skewed toward cultures and norms they are familiar with"*.

5.2.2.5 Lack of Explicit Regulations and Standard Design Guidelines. International business leaders, designers, and local business leaders (N=22), emphasized the importance of explicit data and privacy protection regulations in shaping smart device design. They highlighted the need for regulations to inform the design process and provide guidance to smart device designers [L04]. However, despite the existence of data protection laws in Europe (GDPR[7]), USA, and other countries (such as Brazil-LGPD[29], Turkey-DPL[30], Malaysia-PDPA[31]), there is a lack of explicit smart home privacy protection regulations at the international level, particularly for bystanders as a user group [L06], which results in unclear obligations for smart device manufacturers, and uncertainty around the legal consequences of non-compliance with applicable laws [L03]. Similarly, Jordan lacks the same [LB01], where participants argued that the existence of such regulation would enforce manufacturers to prioritize users' data protection in smart home device design [LB01]. In the same discussion, [LB04] highlighted the ongoing efforts of the Jordanian government to issue the new data protection law[98], although its specifics remain uncertain.

In addition to advocating for global standard data protection regulation, international business leaders emphasized the desire for minimal regulations that are business-friendly and easy to implement and comply with [L09]. They also pointed out the challenges faced by small companies in understanding and complying with regulations, as well as the inconsistency of data protection regulations across countries. [L06] shared the experience of his company, which encountered inconsistencies between GDPR[7] and laws in the USA (e.g., CCPA[15], CPRA[32], NYPA[33], HIPAA[34], TCPA[35], and FERPA[36]). To ensure compliance, participants mentioned various approaches, including personal judgment, understanding of regulations, and reliance on compliant third-party services to alleviate the regulatory burden (e.g., Amazon Web Services, Made Trade, Better World Books, and Wix eCommerce) [L07]. Designers also highlighted the lack of standard design guidelines for privacy protection, resulting in manufacturers adopting a wide variety of design processes [D03]. They argued that data protection regulations could encourage or enforce companies to agree on standard design guidelines [D03]. Furthermore, designers emphasized that existing data protection regulations (such as GDPR[7], CCPA[15], CPRA[32]) overlook inter-personal data protection [D10]. Similar to international business leaders, designers argued that companies are unlikely to take proactive measures to protect user data unless enforced by regulations or driven by market pressure such as customer complaints and competition [D11]. From another side, designers and international business leaders emphasized that privacy protection is a shared responsibility among all stakeholders, including users, international

[29]Brazil(LGPD): Data Protection Law
[30]Turkey: Data Protection Law
[31]Malaysia: Data Protection Law
[32]CPRA: California Privacy Rights Act
[33]USA NYPA: New York Power Authority
[34]HIPAA: USA-Health Insurance Portability and Accountability Act of 1996
[35]TCPA: USA-Telephone Consumer Protection Act 47
[36]FERPA: USA-Family Educational Rights and Privacy Act

business leaders, designers, and regulators [D08].

5.2.2.6 Privacy Protection Design Challenges in Jordan and MAME Region. Local business leaders (N=5) explained that smart home devices have limited usage in Jordan and MAME region. [LB02] described the smart device penetration rate in Jordan as *"low"*, and [LB05] mentioned that these devices are not designed specifically for MAME region. However, [LB03] noted a growing adoption of smart home devices in the region. Participants highlighted that economies of scale hinder the consideration of contextual privacy concerns, and added that manufacturers prioritize user privacy based on market size [LB04]. They argued that the economies of scale in Jordan and MAME region do not support customization of smart devices for this region [LB04]. However, the increasing adoption of smart devices may encourage manufacturers to address contextual privacy concerns in the future [LB01]. In support of this argument, [LB03] highlighted the evolving telecom infrastructure in Jordan, to support IoT devices.

5.2.3 ***Aspirations for Privacy Protection Design***. Participants (N=23) outlined some interventions and aspirations for privacy protection design from technical, social, economic, and legal perspectives. From a technical design perspective, [D02] discussed adopting Privacy by Design principles (PbD)[37]. However, [D09] highlighted that many designers are not aware of the principles of privacy by design, and [D11] argued that companies also have a role in putting in place appropriate organisational and technical measures to ensure that user data is effectively protected. Designers discussed how semiotics is an important design perspective for privacy protection, highlighting the importance of designing specific contextual compliant signals [D04] and banners [D11] to engage users about privacy issues. However, they cautioned that signals should consider context sensitivities (i.e.,social, religious, and cultural), and to avoid frequent alerts that might lead users to discard signals [D03]. Designers further noted this was a complex design challenge as signals depend on whether users *"notice them* [D07], *"trust them"* [D07], or *"understand them"* [D09], and they highlighted that *"signals are not enough"* [D10] as *"some users are deaf or blind, and so there's an aspect of inclusivity here"* [D11].

Designers also thought that innovative technologies (e.g., AI) could provide designers with new tools to protect users' data and privacy [D04]. This would allow devices to interact intelligently with users by *"accepting their commands, hand movements, or face gestures"* [D05]. However, it was noted that using features like hand movements or face gestures might be problematic for accessibility purposes [D01]. It was also proposed that innovative technologies could allow multiple user groups (e.g., bystanders) to create their own profiles [D07] *"by tagging"* [D11], or *"based on time spent in front of the device"* [D12], and they stated that *"smart devices can learn and identify users by their behaviors"* [D13]. Additionally, designers proposed partitioning data and to only collect the required data to provide the services instead of blanket data collection [D14].

Designers and international business leaders also argued for social interventions such as raising awareness for different stakeholders (e.g., users, designers, international business leaders, and regulators). They argued that improving awareness of smart technologies, laws, and contextual concerns would facilitate privacy protection design for smart home users [D11]. [D02] also thought that social change could also follow from an economic intervention. One example given was to inform end users of manufacturers' business models for data monetisation. [D05] also argued for the need for ethical and transparent company practices about how data is used and monetized, and added that this would enable users to adopt appropriate practices with smart home devices to protect their data. Designers also thought it critical for companies to effectively consider user feedback [D07], and [D01,D05] added that companies should adopt processes to involve users in the design process.

Finally, both users and designers have discussed the use of mobile applications to enhance workers' privacy protection [U03,D03]. They have also emphasized the need for government intervention through the enactment of explicit data protection laws to protect users' privacy, highlighting the need for companies to ensure compliance with existing laws to avoid the consequences of non-compliance [D05]. Another designer proposed making companies legally responsible stewards of users' data, such that companies would need to help manage and oversee users' data assets to help provide users with services and protect their data [D09].

6 DISCUSSION AND RECOMMENDATIONS

Our study focuses on exploring the design challenges for privacy protection with smart home devices in Jordan. We engaged with users, local and international business leaders, and designers in order to explore their perspectives of privacy protection design. While some of our findings align with those of prior studies [4, 48, 70, 104], our work both reaffirms prominent findings and solutions and also introduces new proposals to enhance privacy protection in smart home device design specifically for the Jordanian context.

6.1 Summary of Findings

The findings can be categorized into two main categories. Firstly, the category of "Privacy Protection Through Smart Device Design" encompasses various aspects such as the designers and design processes involved in developing smart home devices. The study highlights the lack of manufacturers and designers in the MAME region, posing challenges for localizing smart devices. Moreover, the localization of imported and assembled smart devices often overlooks contextual privacy concerns and focuses more on superficial aspects like language and regional settings. Additionally, the study highlights the lack of attention given to Jordan and MAME region in the design of smart home devices.

The second category, "Perspectives and Challenges of Privacy Protection for Smart Device Design," explores the concerns and considerations of users regarding smart device design. It delves into privacy and security concerns expressed by users, including those related to smart home bystanders and the complex power dynamics that exist within these contexts. The study also sheds light on users' frustrations with deceptive privacy settings and complex privacy policies. Furthermore, it examines the challenges faced in privacy protection design, such as the high cost associated with implementation and the difficulty in aligning data protection with

[37] PbD: Privacy by design through the lens of HCI

business goals. Limited awareness among users poses another constraint, as does the lack of explicit regulations and standard design guidelines for privacy protection globally and regionally. Finally, the study suggests potential mitigations for these challenges, and discusses participants' aspirations for privacy protection design. While some overlap exists between privacy protection challenges on a global scale and those specific to Jordan, the study reveals that privacy protection design of smart home devices does not address the needs of Jordan and the broader MAME region. Participants provide suggestions for improving this situation, and further research is necessary to gain a comprehensive understanding and develop context-specific solutions for Jordan.

Moreover, we found that privacy protection in the smart home context in Jordan is a shared responsibility between three key stakeholder groups: companies (i.e., designers and international business leaders), regulators and policy makers, and users (i.e., households and domestic workers). As a result, we discuss the elicited findings of this study in the next sections, and outline a number of recommendations for social, technical, business, and legal interventions to improve privacy protection design for domestic workers with smart home devices in Jordan. Some of the proposed interventions have universal applicability and are not restricted to Jordan.

6.2 Social Considerations and Interventions

Here we discuss and present the identified social considerations for privacy protection design in Jordan, and propose some interventions for improvements.

6.2.1 ***Increase Data Literacy and Educate Stakeholders.*** As presented in Section §5.2.2.4, stakeholders' limited awareness constrains design freedom and hinders privacy protection design capabilities. Prior studies [134–136] highlighted that designing context-aware devices depends on those who design the devices as well as on those who use them, which means that the levels of awareness of stakeholders affects design outcomes. Moreover, our findings note that designers and companies are skewed toward cultures and norms they are aware of: without any clear incentive to engage with unfamiliar cultures, it is unsurprising that these are not considered. Drawing on the findings in Section §5.2.3, we argue that awareness needs to be improved among all stakeholder groups in order to improve the design of privacy protection for smart devices. We argue that companies need to educate their staff (i.e., business leaders and designers) about users' privacy concerns, innovative technologies, and regulation in Jordan. Moreover, companies should collaborate with regulators, international and local entities, and the wider private sector to run awareness campaigns, for example through educational material in schools and universities, and through targeted messages in the media (TVs, Newspapers, and Social Media). Domestic worker recruitment agencies should educate new domestic workers about smart devices, the potential privacy threats they entail, and the recommended privacy protection practices they should adopt. In addition, agencies should facilitate discussions on privacy concerns between the recruiting families and the workers, encouraging open and transparent communication regarding these concerns.

Regulators in Jordan should also work to educate policy makers and to incorporate public awareness in their regulatory strategies. Users also have a responsibility to educate themselves about smart technologies and privacy implications, in addition to providing feedback and reporting privacy breaches to service providers and government entities (i.e., regulators). Finally, it is important for all stakeholders to be particularly aware of bystanders and how their privacy is impacted by smart device design, regulation, and usage patterns in Jordan. Furthermore, in line with prior studies [137, 138], international business leaders described data as the "new oil" for revenue generation and the "new uranium" due to the associated security and privacy risks. Moreover, other studies [139, 140] have described data as the "new currency" in the evolving information economy. Notably, our findings have highlighted a significant lack of understanding and awareness among users regarding the value of their data, highlighting an interesting disparity in how the value of data is perceived. To address this issue, we argue there is a need to enhance users' awareness regarding the value of their data, and we suggest that companies should transparently inform users about their adopted monetization models for the data they collect.

6.2.2 ***Alleviate Power Dynamics.*** Failure in addressing contextual privacy concerns (e.g., social, religious, cultural) in the design of smart devices can have privacy and security implications [141]. Similarly to smart home device users in Western contexts [5, 36, 75, 76, 142–144], users in Jordan also showed security and privacy design concerns as presented in section §5.2.1 (e.g., design flaws, inability to recognize bystanders, concerns about privacy policies and consent). Prior studies [4, 44, 85] have noted these concerns and presented broad recommendations to facilitate privacy protection.

As presented in sections §5.2.1.1 and §5.2.1.2, users expressed how privacy concerns interplay with the differential power dynamics between families and their domestic workers, and how families adopt autocratic practices in their homes, which results in reduced worker agency and limits their freedom of choice. This leads workers to compromise their privacy rights for perceived benefits (e.g., salary and job). We argue that designers need to consider smart home asymmetrical power dynamics in the Jordanian context to either reduce or balance its impact on powerless users' agency. Moreover, and complementing the suggestions of Bernd et al. [70], we argue that a set of technical, social, business, and legal interventions to promote user agency and improve design guidelines could help to balance power dynamics between domestic workers and families in the smart homes in both Western and non-Western settings such as Jordan.

6.2.3 ***Empower Women Workers for Privacy Protection.*** In conformity with prior studies [145–147], users highlighted that despite the efforts the Jordanian government and societal entities make to empower women and workers, and despite the significant improvements in women's rights in Jordan, which have empowered women and allowed them to work in many fields, some female foreign domestic workers are considered a powerless group in smart homes. They called for more collaboration among governments, social organizations, and companies to support protecting their privacy. To empower this user group, we propose several recommendations for governmental entities and recruitment agencies. Firstly, they should prioritize raising awareness among households and workers about smart technologies and associated privacy risks.

This can be achieved by providing information about smart devices in workers' native languages (such as Bengali, Filipino, and Ethiopian), incorporating this information into work contracts, and obtaining workers' informed consent before they travel to Jordan. Secondly, it is crucial to consider workers' cultural and religious beliefs and inform employing families about their specific needs prior to hiring them. Clear communication channels should be established with workers, and encouraging families to discuss privacy requirements. Furthermore, families should be encouraged to contemplate the ethical implications of undermining workers' rights, while societal entities advocate for legal protections and support networks for workers. By implementing these measures, we believe that female domestic workers can gain agency, make informed decisions, and protect their privacy rights within the smart home context. Additionally, we argue that design can contribute to privacy protection by enhancing workers' agency and restraining autocratic practices within households, as discussed further in Section §6.3.

6.3 Technical Considerations and Interventions

Our findings also indicate a number of technical interventions that could enhance privacy protection for domestic workers in smart homes in Jordan. We believe that a significant part of these proposed technical interventions can be beneficial on a global level and not only in the local context of Jordan.

6.3.1 ***Utilize Innovative Technologies.*** Designers should leverage emerging technologies, such as artificial intelligence (AI), to enhance data protection in smart home devices. This includes features like profiling bystanders (e.g., domestic workers), erasing or protecting their data, and user recognition. Differential privacy algorithms [56] and data partitioning techniques [148] should be adopted by companies to minimize unnecessary data collection and store user data locally on edge devices instead of centralized cloud storage. Furthermore, we argue for the use of mobile applications to enhance the protection of workers' privacy. We also urge the adoption of perturbation methods and differential privacy, as these approaches have shown their effectiveness in protecting privacy [73, 149]. However, achieving a balance between privacy protection and household security requirements poses challenges.

6.3.2 ***Semiotics For Smart Devices.*** Designers should engage more deeply with semiotics[38] to help them design culturally sensitive and appropriate signals for smart devices. Semiotics encompasses the study of signs and symbols, including verbal and nonverbal communication. Smart devices introduce novel and more sophisticated interaction methods compared to previous technologies. As a result, a diverse range of stakeholders, including children, adults, the elderly, disabled users, as well as bystanders such as neighbors, guests, or domestic workers, interact with these devices. To ensure effective communication about privacy concerns with smart devices, it is crucial for these devices to employ consistent signs, symbols, and a privacy language that resonates with the target audience. Accommodating the complexities of different languages, educational levels, religious and cultural norms, as well as leveraging the emerging possibilities offered by machine learning (ML), natural language processing, and AI, pose significant challenges. Thus, and in conformity with other studies [48, 59] we assert that exploring the field of semiotics holds substantial potential for advancing the state of the art in the design of smart devices.

6.3.3 ***Adopt Privacy by Design (PbD).*** We argue that companies and designers need to engage more deeply with the principles and practices of Privacy by Design (PbD) [48, 141, 150, 151]. We believe this is an important cornerstone for sharing and improving good practices in how to consider privacy protection in the design of smart home devices. Given how designers report looking to one another as inspiration for good practice, it is critical for PbD to be on-going process of learning and improving through considering users' feedback and reported incidents in the Jordanian context. Rubenstien et al. [152] investigated how Google and Facebook address privacy by design through incorporating reported incidents and regulations, and suggested that the main challenge to effective privacy by design is not the lack of design guidelines, rather it is that business interests overshadow privacy interests. In support of what they suggested, we believe that governments need to collaborate with the private sector to provide companies with clear guidance about design principles, and that regulators should provide companies with guidance on how to balance privacy with business interests, along with adopting robust oversight mechanisms. Finally it is necessary for a global set of Privacy by Design principles and practices to be developed that include important MAME contextual considerations.

6.3.4 ***Responsible Innovation.*** We note that many of the issues we have uncovered are strongly aligned with the principles of responsible innovation (RI) [53, 54]. This specifically highlights the importance of considering security and privacy when designing new technologies. Our overarching recommendation is that designing innovative smart devices should follow established RI principles. One example of this is the AREA framework [153], which encourages innovators to anticipate unintended impacts, Reflect on the purposes and motivations for the innovation, Engage with affected communities and invite dialogue, and Act to influence the trajectory and direction of the innovation. We also argue that certification could help to spotlight those who employ ethical and responsible practices with data protection and incorporate data protection within their design processes. We believe such certification system will be supportive of global efforts for more ethical design [154–156].

6.4 Business Considerations and Interventions

Here we discuss how business considerations could affect and improve privacy protection design.

6.4.1 ***Address Cost Challenges in Privacy Protection Design.*** As presented in Sections §5.2.2.1, §5.2.2.2, and §5.2.2.3, findings showed that cost represents a challenge for considering non-Western contextual privacy concerns (MAME) in the design of smart home devices for all manufacturers, and especially for SMEs. Prior studies have investigated how financial strength enables better consideration of data protection [157, 158]. To overcome these financial challenges, and informed by outcomes of prior studies and the discount usability engineering movement [104, 159–161],

[38] Semiotics-Definition of Semiotics

we argue that more needs to be done both by researchers and businesses to develop, improve, and apply cost effective design practises (e,g,. heuristics (e.g., generalizations [162]), workarounds, common sense, short cuts) that mitigate privacy protection design challenges. Our argument is that the proposed business interventions can effectively address the MAME context of Jordan, as well as other overlooked contexts.

6.4.2 ***Consider Jordanian Context***. As discussed in Section §5.1.2, and Section §5.1.3, participants emphasized that the majority of manufacturers and users of smart home devices are from Western countries (e.g., Europe, North America), with designers and companies primarily focusing on Western contexts §5.2.2.4. This, combined with various business barriers and challenges in the Jordanian and MAME region, such as limited market size and smart devices penetration rates[39], lack of local manufacturers, high localization costs, and regulatory limitations, contributes to the overlooking of the Jordanian context. Prior studies [163, 164] have highlighted the influence of unknown and hard-to-manage elements on design processes, including designers' contextual values, norms, and concerns. Other research [165, 166] has called for a shift towards context-based design that considers users' interactions with smart technologies in their own cultural contexts, leading to the development of context-aware devices. Our findings reveal the lack of manufacturers in Jordan, posing a challenge in creating contextually suitable devices for Jordan and the wider MAME region.

Aligning with McGregor et al. [167], our designers argue that without organizational strategies to address specific contexts like Jordan, the influence of employees' culture on design processes remains minimal. However, we believe that the rapidly growing smart home device markets in Jordan and MAME region[40] present an opportunity for manufacturers and designers to consider these contexts and produce devices that are compatible with the local context. Additionally, we propose the training and hiring [168, 169] of skilled designers from Jordan and MAME region as an important step in addressing contextual concerns in design processes. Nonetheless, it is important to acknowledge the limitations designers face in impacting design processes within different companies, with individual designers potentially having a greater influence in SMEs[170] compared to larger companies §5.1.3. Furthermore, we argue for the active involvement of designers in documenting and developing new design guidelines for privacy in Jordan and MAME region. This contribution will advance the field of Privacy by Design (PbD) and ensure that privacy protection aligns with the specific needs of different contexts. Additionally, it is crucial for local and international policymakers to address how contextual concerns can be effectively integrated into the design of approved devices for the markets in Jordan (e.g., type approval certification).

6.4.3 ***Adopt Ethical and Transparent Design Practices***. Sections §5.2.1.3 and §5.2.1.4 presented users' concerns regarding deceptive designs and practices that threaten privacy in smart homes in Jordan. Users reported compromising their privacy rights to use devices and experiencing reduced agency and lack of free choice when accepting privacy policies and complex terms and conditions agreements [171–178]. These deceptive and unethical design practices, also known as dark patterns, have been variously criticized as bad design, illegal, dishonest, deceptive, and manipulative [171–178]. Our study particularly highlights the issue of one user's consent affecting other users and bystanders in the device's range, specifically impacting passive users such as domestic workers and family members [179, 180]. Implementing multi-user consent mechanisms in smart home devices is essential to support user agency and free choice [179, 180]. The findings also indicated a lack of trust among users in Jordan towards companies employing tricky and dishonest data collection practices. Building trust requires companies to incorporate data protection into their corporate strategies, adopt ethical and transparent practices, and provide workers with tools to protect their data [181–185].

In order to build a sustainable and health smart device market, it is crucial for companies to explore ethical business models that respect user data, especially in the context of Jordan and MAME region. Understanding and leveraging contextual values, such as social, religious, and geopolitical factors, can inform business practices that better suit the user population. Investigating the influence of business values and practices on privacy protection is crucial, and we propose the adoption of an *'Ethical Design Framework'* by regulators and companies to demonstrate a commitment to honest, respectful, and ethical processes in smart device design across different contexts [181–185].

6.4.4 ***Expand Localization to Consider Privacy Concerns***. As presented in Section §5.1.4, our findings indicate that addressing privacy concerns in Jordan and MAME region can be achieved through local design of smart devices or by improving the localization of imported or locally assembled devices. Local business leaders prefer importing or assembling devices due to factors such as cost, lack of skilled labor, competition, and user trust issues [186–188]. International and local business leaders emphasized that it is crucial for companies to ensure business viability when localizing smart home devices to accommodate contextual sensitivities (social, cultural, religious, and geopolitical). Current localization practices [186–188] involve translating content, considering colloquialisms, dialects, geopolitical sensitivities, regulations, regional settings (currency, measurement units), and avoiding offensive signs and phrases [189, 190]. However, these practices often overlook privacy concerns [186]. Therefore, there is a need for further efforts to extend localization practices to incorporate contextual privacy concerns.

Despite potential challenges, we argue that cost-effective strategies can be implemented to minimize the impact, considering the market advantage and evolving understanding of designing solutions that meet the contextual privacy needs of the developing MAME markets.

6.5 Legal Considerations and Interventions

In Section §5.2.2.5, we highlight the lack of explicit data protection regulation in Jordan and the limited coverage of existing global data protection regulations for smart home users (e.g., European GDPR[7],

[39] GSMA Report-Realising the potential of IoT in ME
[40] IDC-Report about the demand for smart home devices across the Middle East

USA data protection laws –CCPA[15], CPRA[32], Brazil-LGPD[29], India[41], Turkey[30], Malaysia[31]), which only regulate users' data protection with service providers (e.g., Amazon, Google). These regulations primarily focus on users' data protection with service providers, overlooking the specific privacy concerns of smart home devices. The lack of explicit regulation poses a challenge for data protection design, particularly in unregulated contexts like Jordan. Furthermore, we found that non-compliance fines disproportionately affect SMEs, hindering their ability to expand their design experience and address overlooked contexts, such as Jordan, and MAME region. Another identified challenge is the inconsistency of data protection regulation across countries, making it difficult to predict the non-compliance consequences. To address this, we propose that governments take the lead in developing global standard regulations that provide consistent guidelines across countries. This would help businesses anticipate and navigate the potential consequences of non-compliance more effectively. We propose that governments collaborate with leading international organizations to address this issue. These include ITU[42], Broadband Commission[43], and some industry non-profit organizations such as GSMA[44], and TMForum[45]. Additionally, countries similar to Jordan should enforce data protection requirements on devices before allowing them into their markets through measures like type approval certificates and data protection tests.

Our findings in Section §5.2.2.5 highlight the significance of global initiatives [191, 192] in promoting privacy protection design guidelines for smart devices. One example is 'Project Connected Home over IP (CHIP)' [193], also known as Matter, initiated by Amazon, Apple, Silicon Labs, and Google. CHIP aims to develop standards for IoT device design, incorporating *'a security-first design philosophy'*, and rules to prevent security attacks (hide passwords, and hide information about connected devices). While Matter is still in development, initiatives like this can contribute to building global privacy protection design guidelines that address the security and privacy concerns of non-Western contexts, including Jordan, and MAME region.

Furthermore, collaboration between designers, international business leaders, and regulators is essential to ensure that regulation supports privacy-respecting business practices, including Jordan, without undermining important business interests. Local regulators should stay informed about the practical use of smart devices and ensure that regulations remain relevant to user and bystander needs. Efforts should continue to develop national regulations and laws for data protection in Jordan, while also working towards harmonizing data protection rules and practices internationally, and extending data protection to countries with less influence on the global stage.

7 FUTURE WORK

Future work will aim to verify our research findings, and to capitalize on them. Areas of interest include: a) To study contextual dynamics and how to leverage them, b) To study possible means of moderating autocratic tendencies and asymmetric power dynamics within smart homes in light of the absence of privacy rights and policies in MAME region, and c) To study how innovative technologies can support privacy protection for all user groups (e.g., households and bystanders).

8 CONCLUSION

Our study aimed to explore the design challenges for privacy protection of domestic workers in smart homes in Jordan, and we made a number of broad recommendations to improve privacy protection design. This paper contributes to a growing body of work on how smart device design can protect different privacy concerns of smart home users (families and domestic workers).

In addition to raising concerns about domestic workers (bystanders) privacy and asymmetrical power dynamics in smart homes in Jordan, privacy design is driven by business strategies, regulation, and contextual elements (i.e., culture, religion, and norms). Our study has identified that designers believe that limited awareness (of smart devices, privacy concerns, and data protection regulation) constrains design freedom, and that educating stakeholders is a key factor for privacy protection design of smart home devices. They point out that companies and designers are skewed towards cultures and norms they are familiar with, and highlighted that innovation and the target audience for design is largely Western, in addition to a lack of smart home device manufactures and designers in Jordan and MAME region. All of this results in design processes that overlook Jordanian context and MAME region.

We found also that current practices for localizing smart devices overlooks contextual concerns and focuses on language translation, regional settings, and avoiding offensive dialects and signs. Users experienced dark patterns in design and tricky privacy policies that undermined their agency and free choice. Additionally, we found that designers believe that standard global data protection regulation, and standard design guidelines are important for data protection design; however, Jordan lacks such explicit regulation, in addition to lack of global standard design guidelines.

As a result of this study, we propose a number of broad recommendations for interventions to help improve privacy protection design with smart home devices in Jordan. Some of our recommendations include proposals for developing design guidelines, developing ethical business models [*Ethical Design Framework*] that respect privacy and align with Jordanian and MAME region's values, and we outline how Semiotics can help shape how smart devices communicate about privacy, in addition to expanding the scope of smart device localization to include privacy concerns.

Another key concern is that power dynamics in smart homes can significantly affect the privacy of dis-empowered individuals, and we outline that tackling this challenge requires a concerted effort from all stakeholders (e.g., designers and business leaders, regulators, and users). Additionally, we propose that companies (especially SMEs) can adopt agile and cost effective approaches to overcome cost challenges, and to empower companies to become legal stewards of users data. We conclude by noting that our findings and recommendations are well aligned with the principles of

[41] India: Data Protection Bill
[42] ITU: The United Nations agency for ICT
[43] Broad Band Commission: The ITU/UNESCO Commission for Sustainable Development
[44] GSMA: Global ICT industry organisation
[45] TM Forum: A global association for telecommunications service providers and suppliers

Responsible Innovation and that more needs to be done to Anticipate, Reflect, Engage and Act to minimize negative impacts from smart technology innovations.

ACKNOWLEDGMENTS

The authors thank all the participants in this study for their efforts and all the valuable comments and feedback, and would like also to thank all the staff of the Department of Computer Science in the University of Oxford for all the support they have provided.

REFERENCES

[1] McWhorter RR, Bennett EE. Creepy Technologies and the Privacy Issues of Invasive Technologies, 2020. URL https://www.igi-global.com/chapter/creepy-technologies-and-the-privacy-issues-of-invasive-technologies/www.igi-global.com/chapter/creepy-technologies-and-the-privacy-issues-of-invasive-technologies/252320. ISBN: 9781799829140 Pages: 243-268 Publisher: IGI Global.

[2] Yao Y, Basdeo JR, Mcdonough OR, Wang Y. Privacy Perceptions and Designs of Bystanders in Smart Homes. Proceedings of the ACM on Human Computer Interaction May 2019;3(CSCW):1–24. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3359161.

[3] Gaddam A, Mukhopadhyay SC, Gupta GS. Trial & experimentation of a smart home monitoring system for elderly. In 2011 IEEE International Instrumentation and Measurement Technology Conference. May 2011; 1–6. ISSN: 1091-5281.

[4] Albayaydh WS, Flechais I. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In CHI Conference on Human Factors in Computing Systems. New Orleans LA USA: ACM. ISBN 978-1-4503-9157-3, April 2022; 1–24. URL https://dl.acm.org/doi/10.1145/3491102.3502097.

[5] Zeng21 E, Mare S, Roesner F. End User Security & Privacy Concerns with Smart Homes February 2017;17.

[6] Ali B, Awad AI. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors March 2018;18(3):817. ISSN 1424-8220. URL https://www.mdpi.com/1424-8220/18/3/817. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.

[7] Wilson C, Hargreaves T, Hauxwell-Baldwin R. Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing February 2015;19(2):463–476. ISSN 1617-4909, 1617-4917. URL http://link.springer.com/10.1007/s00779-014-0813-0.

[8] Ahmed T, Hoyle R, Shaffer P, Connelly K, Crandall D, Kapadia A. Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments. IEEE Internet Computing 2017;1–1. ISSN 1941-0131. Conference Name: IEEE Internet Computing.

[9] Brand D, DiGennaro Reed FD, Morley MD, Erath TG, Novak MD. A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities. Behavior Analysis in Practice March 2020;13(1):11–21. ISSN 1998-1929, 2196-8934. URL http://link.springer.com/10.1007/s40617-018-00329-y.

[10] Choe EK, Consolvo S, Jung J, Harrison B, Patel SN, Kientz JA. Investigating receptiveness to sensing and inference in the home using sensor proxies. Pittsburgh, Pennsylvania: ACM Press. ISBN 978-1-4503-1224-0, 2012; 61. URL http://dl.acm.org/citation.cfm?doid=2370216.2370226.

[11] Huang Y, Obada-Obieh B, Beznosov KK. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. Honolulu HI USA: ACM. ISBN 978-1-4503-6708-0, April 2020; 1–13. URL https://dl.acm.org/doi/10.1145/3313831.3376529.

[12] Ghiglieri M, Volkamer M, Renaud K. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. Lecture Notes in Computer Science. Cham: Springer International Publishing. ISBN 978-3-319-58460-7, 2017; 656–674.

[13] Winter JS. Citizen Perspectives on the Customization/Privacy Paradox Related to Smart Meter Implementation. International Journal of Technoethics IJT 2015;6(1):45–59. ISSN 1947-3451. URL https://www.igi-global.com/gateway/article/www.igi-global.com/gateway/article/124867. Publisher: IGI Global.

[14] Abdi N, Ramokapane KM, Such JM. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants 2019;.

[15] Lee L, Lee J, Egelman S, Wagner D. Information Disclosure Concerns in The Age of Wearable Computing. In Proceedings 2016 Workshop on Usable Security. San Diego, CA: Internet Society. ISBN 978-1-891562-42-6, 2016; URL https://www.ndss-symposium.org/wp-content/uploads/2017/09/information-disclosure-concerns-in-the-age-of-wearable-computing.pdf.

[16] Malkin N, Bernd J, Johnson M, Egelman S. "What Can't Data Be Used For?": Privacy Expectations about Smart TVs in the U.S. In Proceedings 3rd European Workshop on Usable Security. London, England: Internet Society. ISBN 978-1-891562-54-9, 2018; URL https://www.ndss-symposium.org/wp-content/uploads/2018/06/eurousec2018_16_Malkin_paper.pdf.

[17] Garg V, Camp LJ, Lorenzen-Huber L, Shankar K, Connelly K. Privacy concerns in assisted living technologies. annals of telecommunications annales des télécommunications February 2014;69(1-2):75–88. ISSN 0003-4347, 1958-9395. URL http://link.springer.com/10.1007/s12243-013-0397-0.

[18] Das A, Degeling M, Wang X, Wang J, Sadeh N, Satyanarayanan M. Assisting Users in a World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). Honolulu, HI, USA: IEEE. ISBN 978-1-5386-0733-6, July 2017; 1387–1396. URL http://ieeexplore.ieee.org/document/8014915/.

[19] Naeini PE. Privacy Expectations and Preferences in an IoT World. Open Access Media. USENIX, June 2015. URL https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

[20] Zheng S, Apthorpe N, Chetty M, Feamster N. User Perceptions of Smart Home IoT Privacy. Proceedings of the ACM on Human Computer Interaction November 2018;2(CSCW):1–20. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3274469.

[21] Rodden TA, Fischer JE, Pantidi N, Bachour K, Moran S. At home with agents: exploring attitudes towards future smart energy infrastructures. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Paris France: ACM. ISBN 978-1-4503-1899-0, April 2013; 1173–1182. URL https://dl.acm.org/doi/10.1145/2470654.2466152.

[22] Nissenbaum H. A Contextual Approach to Privacy Online, Information Law Institute at New York University. Daedalus October 2011;140(4):32–48. ISSN 0011-5266, 1548-6192. URL https://direct.mit.edu/daed/article/140/4/32-48/26914.

[23] Barth A, Datta A, Mitchell J, Nissenbaum H. Privacy and contextual integrity: framework and applications. In 2006 IEEE Symposium on Security and Privacy (S&P'06). May 2006; 15 pp.–198. ISSN: 2375-1207.

[24] Lorenzen-Huber L, Boutain M, Camp LJ, Shankar K, Connelly KH. Privacy, Technology, and Aging: A Proposed Framework. Ageing International June 2011;36(2):232–252. ISSN 0163-5158, 1936-606X. URL http://link.springer.com/10.1007/s12126-010-9083-y.

[25] Apthorpe N, Shvartzshnaider Y, Mathur A, Reisman D, Feamster N. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. Proceedings of the ACM on Interactive Mobile Wearable and Ubiquitous Technologies July 2018;2(2):1–23. ISSN 2474-9567. URL https://dl.acm.org/doi/10.1145/3214262.

[26] Burrows A. Privacy, boundaries and smart homes for health_ An ethnographic study | Elsevier Enhanced Reader, 2018.

[27] Gerber N, Reinheimer B, Volkamer M. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats 2018;4.

[28] SathishKumar J, R. Patel D. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications March 2014;90(11):20–26. ISSN 09758887. URL http://research.ijcaonline.org/volume90/number11/pxc3894454.pdf.

[29] Jakobi T, Ogonowski C, Castelli N, Stevens G, Wulf V. The Catch(es) with Smart Home: Experiences of a Living Lab Field Study. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Denver Colorado USA: ACM. ISBN 978-1-4503-4655-9, May 2017; 1620–1633. URL https://dl.acm.org/doi/10.1145/3025453.3025799.

[30] Tabassum M, Kosinski T, Lipford HR. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks 2019;.

[31] Yao Y, Xia H, Huang Y, 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: ACM. ISBN 978-1-4503-4655-9, May 2017; 6777–6788. URL https://dl.acm.org/doi/10.1145/3025453.3025907.

[32] Hoyle R, Templeman R, Armes S, Anthony D, Crandall D, Kapadia A. Privacy behaviors of lifeloggers using wearable cameras. Seattle Washington: ACM. ISBN 978-1-4503-2968-2, September 2014; 571–582. URL https://dl.acm.org/doi/10.1145/2632048.2632079.

[33] Geeng C, 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: ACM. ISBN 978-1-4503-5970-2, May 2019; 1–13. URL https://dl.acm.org/doi/10.1145/3290605.3300498.

[34] Zeng11 E, Roesner F. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study 2017;19.

[35] Ur B, Jung J, Schechter S. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. Seattle Washington: ACM. ISBN 978-1-4503-2968-2, September 2014; 129–139. URL https://dl.acm.org/doi/10.1145/2632048.2632107.

[36] Bernd J, Abu-Salma R, Frik A. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance, 2019;14.

[37] Cobb C, Surbatovich M, Kawakami A, Sharif M, Bauer L. How Risky Are Real Users' IFTTT Applets?. USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9–11, 2020, Virtual Conference. 2020;26. URL https://www.usenix.org/system/files/soups2020-cobb.pdf.

[38] Apthorpe N, Emami-Naeini P, Mathur A, Chetty M, Feamster N. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. ACM Transactions on Internet of Things June 2022;3539737. ISSN 2691-1914, 2577-6207. URL https://dl.acm.org/doi/10.1145/3539737.

[39] Garg R, Cui H. Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies. ACM Transactions on Computer Human Interaction April 2022;29(2):1–30. ISSN 1073-0516, 1557-7325. URL https://dl.acm.org/doi/10.1145/3485058.

[40] Meng N, Keküllüoğlu D, Vaniea K. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. Proceedings of the ACM on Human Computer Interaction April 2021;5(CSCW1):1–29. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3449119.

[41] Cobb C, Bhagavatula S, Garrett KA, Hoffman A, Rao V, Bauer L. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. Proceedings on Privacy Enhancing Technologies October 2021;2021(4):54–75. ISSN 2299-0984. URL https://petsymposium.org/popets/2021/popets-2021-0060.php.

[42] Marky K, Prange S, Krell F, Mühlhäuser M, Alt F. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. Essen Germany: ACM. ISBN 978-1-4503-8870-2, November 2020; 83–95. URL https://dl.acm.org/doi/10.1145/3428361.3428464.

[43] Madden M. Opinion | The Devastating Consequences of Being Poor in the Digital Age. The New York Times April 2019;ISSN 0362-4331. URL https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

[44] Mare S, Roesner F, Kohno T. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. Proceedings on Privacy Enhancing Technologies April 2020;2020(2):436–458. ISSN 2299-0984. URL https://petsymposium.org/popets/2020/popets-2020-0035.php.

[45] Marky K, Voit A, Stöver A, Kunze K, Schröder S, Mühlhäuser M. "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. Tallinn Estonia: ACM. ISBN 978-1-4503-7579-5, October 2020; 1–11. URL https://dl.acm.org/doi/10.1145/3419249.3420164.

[46] Ahmad I, Farzan R, Kapadia A, Lee AJ. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. Proceedings of the ACM on Human Computer Interaction October 2020;4(CSCW2):1–28. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3415187.

[47] Johnson M, Lee M, McCahill M, Mesina MR. Beyond the 'All Seeing Eye': Filipino Migrant Domestic Workers' Contestation of Care and Control in Hong Kong. Ethnos March 2020;85(2):276–292. ISSN 0014-1844, 1469-588X. URL https://www.tandfonline.com/doi/full/10.1080/00141844.2018.1545794.

[48] Albayaydh W, Flechais I. Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households. ISBN 978-1-939133-37-3, 2023; 4643–4659. URL https://www.usenix.org/conference/usenixsecurity23/presentation/albayaydh.

[49] Chalhoub G, Flechais I. "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In Moallem A (ed.), HCI for Cybersecurity, Privacy and Trust, volume 12210. Cham: Springer International Publishing. ISBN 978-3-030-50308-6 978-3-030-50309-3, 2020; 305–325. URL http://link.springer.com/10.1007/978-3-030-50309-3_21. Series Title: Lecture Notes in Computer Science.

[50] Lupton D. Self-tracking cultures: towards a sociology of personal informatics. Sydney New South Wales Australia: ACM. ISBN 978-1-4503-0653-9, December 2014; 77–86. URL https://dl.acm.org/doi/10.1145/2686612.2686623.

[51] Yao Y, Basdeo JR, Kaushik S, Wang Y. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. Glasgow Scotland Uk: ACM. ISBN 978-1-4503-5970-2, May 2019; 1–12. URL https://dl.acm.org/doi/10.1145/3290605.3300428.

[52] Lau J, Zimmerman B, Schaub F. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. Proceedings of the ACM on Human Computer Interaction November 2018;2(CSCW):1–31. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3274371.

[53] Koops BJ, Oosterlaken I, Romijn H, Swierstra T, van den Hoven J (eds.). Responsible Innovation 2. Cham: Springer International Publishing, 2015. ISBN 978-3-319-17307-8 978-3-319-17308-5. URL http://link.springer.com/10.1007/978-3-319-17308-5.

[54] van den hoven J, Doorn N, Swierstra T, Koops BJ, Romijn H. Responsible Innovation Volume 1: Innovative Solutions for Global Issues. Responsible Innovation Volume 1. ISBN 978-94-017-8955-4 ISBN 978-94-017-8956-1 (eBook) DOI 10.1007/978-94-017-8956-1. January 2014. ISBN 978-94-007-7843-6. URL https://www.researchgate.net/profile/Tsjalling-Swierstra/publication/263932307_Responsible_Innovation_Volume_1_Innovative_Solutions_for_Global_Issues/links/5f2febff458515b729100653/Responsible-Innovation-Volume-1-Innovative-Solutions-for-Global-Issues.pdf.

[55] Manheim K, Kaplan L. Artificial Intelligence: Risks to Privacy and Democracy.Heinonline.. 21 YALE J.L. & TECH. 106 (2019;21. URL https://heinonline.org/HOL/Page?handle=hein.journals/yjolt21&div=4&g_sent=1&casa_token=&collection=journals.

[56] Zhu T, Yu PS. Applying Differential Privacy Mechanism in Artificial Intelligence. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, TX, USA: IEEE. ISBN 978-1-72812-519-0, July 2019; 1601–1609. URL https://ieeexplore.ieee.org/document/8885331/.

[57] B. J.J. Vlist VD, Niezen G, Hu J, Feijs LMG. Design semantics of connections in a smart home environment. Creation and Design 2011;13(2):18–24. URL https://research.tue.nl/en/publications/design-semantics-of-connections-in-a-smart-home-environment-2.

[58] Resnick ML, Montania R. Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store. International Journal of Human Computer Interaction October 2003;16(2):211–234. ISSN 1044-7318, 1532-7590. URL http://www.tandfonline.com/doi/abs/10.1207/S15327590IJHC1602_05.

[59] Nadin M. Semiotic Engineering – An Opportunity or an Opportunity Missed? In Diniz Junqueira Barbosa S, Breitman K (eds.), Conversations Around Semiotic Engineering. Cham: Springer International Publishing. ISBN 978-3-319-56290-2 978-3-319-56291-9, 2017; 41–63. URL http://link.springer.com/10.1007/978-3-319-56291-9_6.

[60] Chagas BA, Redmiles DF, de Souza CS. Observed Appropriation of IoT Technology: A Semiotic Account. In Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems. Belém Brazil: ACM. ISBN 978-1-4503-6601-4, October 2018; 1–10. URL https://dl.acm.org/doi/10.1145/3274192.3274225.

[61] Wilkinson D, Namara M, Badillo-Urquiola K, Wisniewski PJ, Knijnenburg BP, Page X, Toch E, Romano-Bergstrom J. Moving Beyond a "one-size fits all": Exploring Individual Differences in Privacy. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal QC Canada: ACM. ISBN 978-1-4503-5621-3, April 2018; 1–8. URL https://dl.acm.org/doi/10.1145/3170427.3170617.

[62] Li Y, Kobsa A, Knijnenburg BP, Carolyn Nguyen MH. Cross-Cultural Privacy Prediction. Proceedings on Privacy Enhancing Technologies April 2017;2017(2):113–132. ISSN 2299-0984. URL https://petsymposium.org/popets/2017/popets-2017-0019.php.

[63] Ahmed SI, Haque MR, Chen J, Dell N. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. Proceedings of the ACM on Human Computer Interaction December 2017;1(CSCW):1–20. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3134652.

[64] Palen L, Dourish P. Unpacking "Privacy" for a Networked World. Ft. Lauderdale, Florida, USA. Privacy and Trust. NEW HORIZONS 2003;(5):8. URL https://dl.acm.org/doi/pdf/10.1145/642611.642635.

[65] Mustafa M, Lazem S, Alabdulqader E, Toyama K, Sultana S, Ibtasam S, Anderson R, Ahmed SI. IslamicHCI: Designing with and within Muslim Populations. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu HI USA: ACM. ISBN 978-1-4503-6819-3, April 2020; 1–8. URL https://dl.acm.org/doi/10.1145/3334480.3375151.

[66] Lipka M. Muslims and Islam: Key findings in the U.S. and around the world, 2017. URL https://www.pewresearch.org/fact-tank/2017/08/09/muslims-and-islam-key-findings-in-the-u-s-and-around-the-world/.

[67] Hayat MA. Privacy and Islam: From the Quran to data protection in Pakistan. Information Communications Technology Law June 2007;16(2):137–148. ISSN 1360-0834. URL http://www.tandfonline.com/doi/abs/10.1080/13600830701532043.

[68] Norwawi NM, Alwi NHM, Ismail R, Wahid F, Alkaenay NM. Promoting Islamic Ethics on Privacy in Digital Social Network for User Data Protection and Trust. Ulūm Islāmiyyah Journal 2014;13:115–127. ISSN 16755936. URL http://Platform.almanhal.com/CrossRef/Preview/?ID=2-67320.

[69] Hagen L. Overcoming the Privacy Challenges of Wearable Devices: A Study on the Role of Digital Literacy. In Proceedings of the 18th Annual International Conference on Digital Government Research. Staten Island NY USA: ACM. ISBN 978-1-4503-5317-5, June 2017; 598–599. URL https://dl.acm.org/doi/10.1145/3085228.3085254.

[70] Bernd J, Abu-Salma R, Choy J, Frik A. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships 2022;21.

[71] Peppet SR. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Texas Law Review 2014;93.

[72] Baldini G, Botterman M, Neisse R, Tallacchini M. Ethical Design in the Internet of Things. Science and Engineering Ethics June 2018;24(3):905–925. ISSN 1353-3452, 1471-5546. URL http://link.springer.com/10.1007/s11948-016-9754-5.

[73] Eckhoff D, Wagner I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions 2018;20(1):489–516. ISSN 1553-877X. Conference Name: IEEE Communications Surveys & Tutorials.

[74] Krämer M. Disentangling Privacy in Smart Homes. Privacy. Computer Science Department, University of Oxford 2019;URL https://www.martin-kraemer.net/presentations/2018-10-cdt-showcase.pdf.

[75] Newyork T. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse (Published 2018), June 2018. URL https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. Section: Technology.

[76] Leitão R. Digital Technologies and their Role in Intimate Partner Violence. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal QC Canada: ACM. ISBN 978-1-4503-5621-3, April 2018; 1–6. URL https://dl.acm.org/doi/10.1145/3170427.3180305.

[77] Koelle M, Kranz M, Möller A. Don't look at me that way!: Understanding User Attitudes Towards Data Glasses Usage. Copenhagen Denmark: ACM. ISBN 978-1-4503-3652-9, August 2015; 362–372. URL https://dl.acm.org/doi/10.1145/2785830.2785842.

[78] Price BA, Stuart A, Calikli G, Mccormick C, Mehta V, Hutton L, Bandara AK, Levine M, Nuseibeh B. Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers June 2017;1(2):1–18. ISSN 2474-9567. URL https://dl.acm.org/doi/10.1145/3090087.

[79] Manovich L. Trending: The Promises and the Challenges of Big Social Data. In Gold MK (ed.), Debates in the Digital Humanities. University of Minnesota Press. ISBN 978-0-8166-7794-8, January 2012; 460–475. URL https://academic.oup.com/minnesota-scholarship-online/book/29340/chapter/243999993.

[80] Andrejevic M. Big Data, Big Questions| The Big Data Divide. International Journal of Communication 2014;17. URL https://ijoc.org/index.php/ijoc/article/view/2161.

[81] Watkins Allen M, Coopman SJ, Hart JL, Walker KL. Workplace Surveillance and Managing Privacy Boundaries July 2017;21(2):172–200. ISSN 0893-3189, 1552-6798. URL http://journals.sagepub.com/doi/10.1177/0893318907306033.

[82] Ball K. Workplace surveillance: an overview. Kirstie Ball (2010) Workplace surveillance: an overview, Labor History. Labor History February 2010;51(1):87–106. ISSN 0023-656X, 1469-9702.

[83] Lee S, Kleiner BH. Electronic surveillance in the workplace. Management Research News March 2003;26(2/3/4):72–81. ISSN 0140-9174. URL https://www.emerald.com/insight/content/doi/10.1108/01409170310784014/full/html. Publisher: MCB UP Ltd.

[84] J Kraemer M, Flechais I, Webb H. Exploring Communal Technology Use in the Home. Nottingham United Kingdom: ACM. ISBN 978-1-4503-7203-9, November 2019; 1–8. URL https://dl.acm.org/doi/10.1145/3363384.3363389.

[85] Leitão R. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. San Diego CA USA: ACM. ISBN 978-1-4503-5850-7, June 2019; 527–539. URL https://dl.acm.org/doi/10.1145/3322276.3322366.

[86] Lopez-Neira I, Patel T, Parkin S, Danezis G, Tanczer L. 'Internet of Things': How Abuse is Getting Smarter. SSRN Electronic Journal 2019;ISSN 1556-5068. URL https://www.ssrn.com/abstract=3350615.

[87] Liu T, Liu Z, Huang J, Tan R, Tan Z. Detecting Wireless Spy Cameras Via Stimulating and Probing. Munich Germany: ACM. ISBN 978-1-4503-5720-3, June 2018; 243–255. URL https://dl.acm.org/doi/10.1145/3210240.3210332.

[88] Patel SN, Summet JW, Truong KN. BlindSpot: Creating Capture-Resistant Spaces. In Senior A (ed.), Protecting Privacy in Video Surveillance. London: Springer London. ISBN 978-1-84882-300-6 978-1-84882-301-3, 2009; 185–201. URL http://link.springer.com/10.1007/978-1-84882-301-3_11.

[89] Song Y, Huang Y, Cai Z, Hong JI. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu HI USA: ACM. ISBN 978-1-4503-6708-0, April 2020; 1–13. URL https://dl.acm.org/doi/10.1145/3313831.3376585.

[90] Egelman S, Kannavara R, Chow R. Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. Seoul Republic of Korea: ACM. ISBN 978-1-4503-3145-6, April 2015; 1669–1678. URL https://dl.acm.org/doi/10.1145/2702123.2702251.

[91] Portnoff RS, Lee LN, Egelman S, Mishra P, Leung D, Wagner D. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. Seoul Republic of Korea: ACM. ISBN 978-1-4503-3145-6, April 2015; 1649–1658. URL https://dl.acm.org/doi/10.1145/2702123.2702164.

[92] Schiff J, Meingast M, Mulligan DK, Sastry S, Goldberg K. Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns. In Senior A (ed.), Protecting Privacy in Video Surveillance. London: Springer London. ISBN 978-1-84882-300-6 978-1-84882-301-3, 2009; 65–89. URL http://link.springer.com/10.1007/978-1-84882-301-3_5.

[93] Aditya P, Sen R, Druschel P, Joon Oh S, Benenson R, Fritz M, Schiele B, Bhattacharjee B, Wu TT. I-Pic: A Platform for Privacy-Compliant Image Capture. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services. Singapore Singapore: ACM. ISBN 978-1-4503-4269-8, June 2016; 235–248. URL https://dl.acm.org/doi/10.1145/2906388.2906412.

[94] Moncrieff S, Venkatesh S, West G. Dynamic Privacy in a Smart House Environment. In 2007 IEEE International Conference on Multimedia and Expo. July 2007; 2034–2037. ISSN: 1945-788X.

[95] Ballendat T, Marquardt N, Greenberg S. Proxemic interaction: designing for a proximity and orientation-aware environment. In ACM International Conference on Interactive Tabletops and Surfaces - ITS '10. Saarbrücken, Germany: ACM Press. ISBN 978-1-4503-0399-6, 2010; 121. URL http://portal.acm.org/citation.cfm?doid=1936652.1936676.

[96] H. Tan N, Y. Wong R, Desjardins A, A. Munson S, Pierce J. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In CHI Conference on Human Factors in Computing Systems. New Orleans LA USA: ACM. ISBN 978-1-4503-9157-3, April 2022; 1–25. URL https://dl.acm.org/doi/10.1145/3491102.3517617.

[97] Koelle M, Wolf K, Boll S. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. Stockholm Sweden: ACM. ISBN 978-1-4503-5568-1, March 2018; 177–187. URL https://dl.acm.org/doi/10.1145/3173225.3173234.

[98] MODEE J. New Data Protection Bill, Draft. Ministry of Digital Economy And Entrepreneurship, Jordan., 2021. URL https://www.modee.gov.jo/AR/NewsDetails/%D9%82%D8%A7%D9%86%D9%88%D9%86_%D8%AD%D9%85%D8%A7%D9%8A%D8%A9_%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA_%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D9%91%D9%8E%D8%A9_%D9%84%D8%B3%D9%86%D8%A9_2021%D9%85.

[99] Alsondos SA. Will the New Jordanian Law Protect Personal Data?, February 2022. URL https://smex.org/will-the-new-jordanian-law-protect-personal-data/. Section: News.

[100] Group GL. International Comparative Legal Guides, 2022. URL https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa. Archive Location: United Kingdom Publisher: Global Legal Group.

[101] Bastos D, Giubilo F, Shackleton M, El-Mousa F. GDPR Privacy Implications for the Internet of Things. December 2018. URL https://www.researchgate.net/profile/Daniel-Bastos-6/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things/links/5ca4e0df299bf1b86d6322a6/GDPR-Privacy-Implications-for-the-Internet-of-Things.pdf.

[102] Gilman ME. Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice. University of Baltimore 2020; 78. URL https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=2111&context=all_fac.

[103] Hoofnagle CJ, van der Sloot B, Borgesius FZ. The European Union general data protection regulation: what it is and what it means January 2019;28(1):65–98. ISSN 1360-0834, 1469-8404. URL https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501.

[104] Chalhoub G, Flechais I. Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives. Proceedings of the ACM on Human Computer Interaction November 2022; 6(CSCW2):1–36. ISSN 2573-0142. URL https://dl.acm.org/doi/10.1145/3555537.

[105] Merriam SB. Qualitative Research and Case Study Applications in Education. Revised and Expanded from "Case Study Research in Education.". Jossey-Bass Publishers, 350 Sansome St, San Francisco, CA 94104; phone: 415-433-1740; fax: 800-605-2665; World Wide Web: www.josseybass.com ($21.95)., 1998. ISBN 978-0-7879-1009-9. URL https://eric.ed.gov/?id=ED415771.

[106] Keane E. The GDPR and Employee's Privacy: Much Ado but Nothing New. Kings Law Journal September 2018;29(3):354–363. ISSN 0961-5768, 1757-8442. URL https://www.tandfonline.com/doi/full/10.1080/09615768.2018.1555065.

[107] Calder A. EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition. 2020. URL https://books.google.com/books/about/EU_General_Data_Protection_Regulation_GD.html?id=LicDEAAAQBAJ.

[108] Veil W. The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law December 2018;URL https://papers.ssrn.com/abstract=3305056.

[109] Goodman LA. Snowball Sampling. The Annals of Mathematical Statistics 1961;32(1):148–170. ISSN 0003-4851. URL https://www.jstor.org/stable/2237615. Publisher: Institute of Mathematical Statistics.

[110] Atkinson R, Flint J. Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies 2001;.

[111] TenHouten WD. Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-reach Populations. Bulletin of Sociological MethodologyBulletin de Méthodologie Sociologique April 2017;134(1):58–61. ISSN 0759-1063, 2070-2779. URL http://journals.sagepub.com/doi/10.1177/0759106317693790.

[112] Sadler GR, Lee HC, Lim RSH, Fullerton J. Research Article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. Nursing Health Sciences 2010;12(3):369–374. ISSN 1442-2018. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1442-2018.2010.00541.x. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1442-2018.2010.00541.x.

[113] Faugier J, Sargeant M. Sampling hard to reach populations. Journal of Advanced Nursing 1997;26(4):790–797. ISSN 1365-2648. URL https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2648.1997.00371.x. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2648.1997.00371.x.

[114] Bridge D. Middle East and Africa Smart Home Market Size, Scope, Growth, Analysis, & Forecast Trends By 2029, April 2022. URL https://www.databridgemarketresearch.com/reports/middle-east-and-africa-smart-home-market.

[115] Strauss A, Corbin JM. Grounded Theory in Practice. SAGE, March 1997. ISBN 978-0-7619-0748-0. Google-Books-ID: TtRMolAapBYC.

[116] Glaser BG, Strauss AL. The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine Transaction, 1967. ISBN 978-0-202-30260-7. Google-Books-ID: oUxEAQAAIAAJ.

[117] Corbin J, Strauss A. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. SAGE Publications, November 2014. ISBN 978-1-4833-1568-3. Google-Books-ID: hZ6kBQAAQBAJ.

[118] Dreyfus SE. A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition. Technical report, February 1980. URL https://apps.dtic.mil/sti/citations/ADA084551. Section: Technical Reports.

[119] Cannell CF, Miller PV, Oksenberg L. Research on Interviewing Techniques. Sociological Methodology 1981;12:389–437. ISSN 0081-1750. URL https://www.jstor.org/stable/270748. Publisher: [American Sociological Association, Wiley, Sage Publications, Inc.].

[120] Baxter K, Courage C, Caine K. Understanding Your Users: A Practical Guide to User Research Methods. Morgan Kaufmann, May 2015. ISBN 978-0-12-800609-2.

[121] Dell N, Vaidyanathan V, Medhi I, Cutrell E, Thies W. "Yours is better!": participant response bias in HCI. Austin Texas USA: ACM. ISBN 978-1-4503-1015-4, May 2012; 1321–1330. URL https://dl.acm.org/doi/10.1145/2207676.2208589.

[122] Kurniawan S. Interaction design: Beyond human?computer interaction by Preece, Sharp and Rogers (2001), ISBN 0471492787. Universal Access in the Information Society October 2004;3(3-4):289–289. ISSN 1615-5289, 1615-5297. URL http://link.springer.com/10.1007/s10209-004-0102-1.

[123] Guest G, Bunce A, Johnson L. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. Field Methods February 2006; 18(1):59–82. ISSN 1525-822X. URL https://doi.org/10.1177/1525822X05279903. Publisher: SAGE Publications Inc.

[124] Collingridge DS, Gantt EE. The Quality of Qualitative Research. American Journal of Medical Quality September 2008;23(5):389–395. ISSN 1062-8606. URL https://doi.org/10.1177/1062860608320646. Publisher: SAGE Publications Inc.

[125] McHugh ML. Interrater reliability: the kappa statistic. Biochemia Medica 2012; 276–282. ISSN 18467482. URL http://www.biochemia-medica.com/en/journal/22/3/10.11613/BM.2012.031.

[126] Jonsen K, Jehn KA. Using triangulation to validate themes in qualitative studies August 2009;4(2):123–150. ISSN 1746-5648. URL https://www.emerald.com/insight/content/doi/10.1108/17465640910978391/full/html.

[127] Koskei BK, Simiyu C. Role of Interviews, Observation, Pitfalls and Ethical Issues in Qualitative Research Methods. Journal of Educational Policy and Entrepreneurial Research October 2015;URL https://www.semanticscholar.org/paper/Role-of-Interviews%2C-Observation%2C-Pitfalls-and-in-Koskei-Simiyu/19036cfb1bf7ebab3ce2048bd18e53db7e76c2df.

[128] Birmingham P. Using Research Instruments : A Guide for Researchers. ISBN 0-203-42299-6 Master e-book ISBN. Routledge, December 2003. ISBN 978-0-203-42299-1. URL https://www.taylorfrancis.com/books/mono/10.4324/9780203422991/using-research-instruments-peter-birmingham-david-wilkinson.

[129] Jupp V. The SAGE Dictionary of Social Research Methods. 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom: SAGE Publications, Ltd, 2006. ISBN 978-0-7619-6298-4 978-0-85702-011-6. URL https://methods.sagepub.com/reference/the-sage-dictionary-of-social-research-methods.

[130] Trueman. Structured Interviews - History Learning Site, 2015. URL https://www.historylearningsite.co.uk/sociology/research-methods-in-sociology/structured-interviews/.

[131] Harrold C. Practical Smart Device Design and Construction: Understanding Smart Technologies and How to Build Them Yourself | SpringerLink, 2020. URL https://link.springer.com/book/10.1007/978-1-4842-5614-5.

[132] McCann J, Hurford R, Martin A. A design process for the development of innovative smart clothing that addresses end-user needs from technical, functional, aesthetic and cultural view points. In Ninth IEEE International Symposium on Wearable Computers (ISWC'05). October 2005; 70–77. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1550788. ISSN: 2376-8541.

[133] Pelykh A. 6-Steps To Create A Smart Device From An Idea To Prototype | Brainbean Apps, 2020. URL https://brainbeanapps.com/blog/6-steps-to-create-a-smart-device-from-an-idea-to-prototype/.

[134] Dey AK. Context-Aware Computing. In Ubiquitous computing fundamentals. Chapman and Hall/CRC, 2018; 335–366.

[135] Dey AK, Salber D, Futakawa M, Abowd GD. An architecture to support context-aware applications. Technical report, Georgia Institute of Technology, 1999.

[136] Sommer R. Design Awareness. ISBN-10 : 0030802989 ISBN-13 : 978-0030802980. San Francisco: Rinehart Press, January 1972. ISBN 978-0-03-080298-0. URL https://www.amazon.com/Design-Awareness-R-Sommer/dp/0030802989.

[137] Hirsch DD. The Glass House Effect: Big Data, the New Oil, and the Power of Analogy. Maine Law Review 2013;66:373. URL https://heinonline.org/HOL/Page?handle=hein.journals/maine66&id=391&div=&collection=.

[138] MAGNiTT. The world's most valuable resource is no longer oil, but data | MAGNiTT, September 2017. URL https://magnitt.com/news/worldâĂŹs-most-valuable-resource-no-longer-oil-data-21035.

[139] Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th ACM conference on Electronic commerce. New York NY USA: ACM. ISBN 978-1-58113-771-2, May 2004; 21–29. URL https://dl.acm.org/doi/10.1145/988772.988777.

[140] Gates C, Matthews P. Data Is the New Currency. In Proceedings of the 2014 New Security Paradigms Workshop. Victoria British Columbia Canada: ACM. ISBN 978-1-4503-3062-6, September 2014; 105–116. URL https://dl.acm.org/doi/10.1145/2683467.2683477.

[141] Perera C, Barhamgi M, Bandara AK, Ajmal M, Price B, Nuseibeh B. Designing privacy-aware internet of things applications. Information Sciences February 2020;512:238–257. ISSN 00200255. URL https://linkinghub.elsevier.com/retrieve/pii/S0020025519309120.

[142] Talwana JC, Hua HJ. Smart World of Internet of Things (IoT) and Its Security Concerns. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). December 2016; 240–245.

[143] Pandey RK, Misra M. Cyber security threats — Smart grid infrastructure. In 2016 National Power Systems Conference (NPSC). December 2016; 1–6.

[144] Brush AB, Lee B, Mahajan R, Agarwal S, Saroiu S, Dixon C. Home automation in the wild: challenges and opportunities. Vancouver BC Canada: ACM. ISBN 978-1-4503-0228-9, May 2011; 2115–2124. URL https://dl.acm.org/doi/10.1145/1978942.1979249.

[145] Al-Wer E. Language and Gender in the Middle East and North Africa. In The Handbook of Language, Gender, and Sexuality. John Wiley & Sons, Ltd. ISBN 978-1-118-58424-8, 2014; 396–411. URL https://onlinelibrary.wiley.com/doi/abs/. Section: 20 _eprint: https://onlinelibrary.wiley.com/doi/pdf/.

[146] Peters SJ. Review of marginalisation of people with disabilities in Lebanon, Syria and Jordan, Background paper prepared for the Education for All Global Monitoring Report 2010 Reaching the marginalized 2009;.

[147] Almasri S. The Political Economy of Nationality-Based Labor Inclusion Strategies: A Case Study of the Jordan Compact. Middle East Critique April 2021;30(2):185–203. ISSN 1943-6149. URL https://doi.org/10.1080/19436149.2021.1911459. Publisher: Routledge _eprint: https://doi.org/10.1080/19436149.2021.1911459.

[148] Scheuermann P, Weikum G, Zabback P. Data partitioning and load balancing in parallel disk systems. The VLDB Journal The International Journal on Very Large Data Bases February 1998;7(1):48–66. ISSN 1066-8888, 0949-877X. URL http://link.springer.com/10.1007/s007780050053.

[149] Dwork C, Naor M, Reingold O, Rothblum GN, Vadhan S. On the complexity of differentially private data release: efficient algorithms and hardness results. Bethesda MD USA: ACM. ISBN 978-1-60558-506-2, May 2009; 381–390. URL https://dl.acm.org/doi/10.1145/1536414.1536467.

[150] Wong RY, Mulligan DK. 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: ACM. ISBN 978-1-4503-5970-2, May 2019; 1–17. URL https://dl.acm.org/doi/10.1145/3290605.3300492.

[151] GDPR P. Privacy by Design - General Data Protection Regulation (GDPR). Intersoft Consulting, "Privacy by Design" and "Privacy by Default", 2018. URL https://gdpr-info.eu/issues/privacy-by-design/.

[152] Rubinstein IS, Good N. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal 2013;28:1333. URL https://heinonline.org/HOL/Page?handle=hein.journals/berktech28&id=1367&div=&collection=.

[153] UKRI. Framework for responsible innovation – UKRI, 2022. URL https://www.ukri.org/about-us/epsrc/our-policies-and-standards/framework-for-responsible-innovation/.

[154] Resources ED. Ethical Design Resources, 2022. URL https://www.ethicaldesignresources.com/.

[155] Network ED. Ethical Design Network, 2022. URL https://ethicaldesignnetwork.com/.

[156] ICO. About this guidance, October 2022. URL https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/about-this-guidance/. Publisher: ICO.

[157] Journal TWS. GDPR Has Been a Boon for Google and Facebook - WSJ, 2022. URL https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.

[158] Sobers R. A Year in the Life of the GDPR: Must-Know Stats and Takeaways, 2020. URL https://www.varonis.com/blog/gdpr-effect-review.

[159] Experience WLiRBU. Discount Usability for the Web: Article by Jakob Nielsen, 1997. URL https://www.nngroup.com/articles/web-discount-usability/.

[160] LaTouche LW. Usability Issues in the User Interfaces of Privacy-Enhancing Technologies. Ph.D. thesis, ProQuest LLC, 2013. ISBN: 9781303370267 Publication Title: ProQuest LLC ERIC Number: ED560349.

[161] Experience WLiRBU. Agile Development Projects and Usability, November 2008. URL https://www.nngroup.com/articles/agile-development-and-usability/.

[162] Arca S, Hewett R. Privacy Protection in Smart Health. In Proceedings of the 11th International Conference on Advances in Information Technology. Bangkok Thailand: ACM. ISBN 978-1-4503-7759-1, July 2020; 1–8. URL https://dl.acm.org/doi/10.1145/3406601.3406620.

[163] Razzaghi M, Ramirez MJ. The influence of the designers' own culture on the design aspects of products. Hochschule für Künste Bremen. ISBN 978-3-89757-290-4, 2005; URL http://hdl.handle.net/1959.4/11576.

[164] Julier G. The Culture of Design. Publisher SAGE, 2013 ISBN 144629692X, 9781446296929. SAGE, December 2013. ISBN 978-1-4462-9692-9. Google-Books-ID: _QdPAgAAQBAJ.

[165] Gay G, Hembrooke H. Activity-Centered Design: An Ecological Approach to Designing Smart Tools and Usable Systems. MIT Press, February 2004. ISBN 978-0-262-26286-6. Google-Books-ID: 5eRITE5tfvcC.

[166] Haya PA, Montoro G, Alamán X. A Prototype of a Context-Based Architecture for Intelligent Home Environments. In On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE. Springer, Berlin, Heidelberg, 2004; 477–491. URL https://link.springer.com/chapter/10.1007/978-3-540-30468-5_30.

[167] McGregor L, Doshi N. How Company Culture Shapes Employee Motivation. Harvard business review November 2015;URL https://classdat.appstate.edu/COB/MGT/VillanPD/OB%20Fall%202021/Unit%203%20-%20Cohesion/Org%20Culture%20Articles/How%20Company%20Culture%20Shapes%20Employee%20Motivation.pdf.

[168] Dell'era C, Verganti R. The impact of international designers on firm innovation capability and consumer interest. International Journal of Operations Production Management January 2009;29(9):870–893. ISSN 0144-3577. URL https://doi.org/10.1108/01443570910986201. Publisher: Emerald Group Publishing Limited.

[169] Von Stamm B. Whose Design is it? The Use of External Designers. The Design Journal March 1998;1(1):41–53. ISSN 1460-6925, 1756-3062. URL https://www.tandfonline.com/doi/full/10.2752/146069298790225235.

[170] Perry TS. How Small Firms Innovate: Designing a Culture for Creativity. Research Technology Management March 1995;38(2):14–17. ISSN 0895-6308, 1930-0166. URL https://www.tandfonline.com/doi/full/10.1080/08956308.1995.11671678.

[171] Hatchd. Design | The dangers of dishonest design, 2017. URL https://www.hatchd.com.au/blog/the-dangers-of-dishonest-design.

[172] Gawley K. Dark Patterns - The Art of Online Deception, April 2013. URL https://blog.kylegawley.com/dark-patterns-the-art-of-online-deception/.

[173] Bensinger G. Opinion | Stopping the Manipulation Machines. The New York Times April 2021;ISSN 0362-4331. URL https://www.nytimes.com/2021/04/30/opinion/dark-pattern-internet-ecommerce-regulation.html.

[174] Lamenza F. Stop calling these Dark Design Patterns or Dark UX — these are simply a**hole designs, June 2020. URL https://uxdesign.cc/stop-calling-these-dark-design-patterns-or-dark-ux-these-are-simply-asshole-designs-bb02df378ba.

[175] Agarzola. Going Dark: The Ethical Implications of Willfully Dishonest Design, September 2018. URL https://events.drupal.org/seattle2019/sessions/going-dark-ethical-implications-willfully-dishonest-design.

[176] Milanovic K. Smart Home Security: How Safe is Your Data? [Opinion]. IEEE Technology and Society Magazine March 2020;39(1):26–29. ISSN 1937-416X. Conference Name: IEEE Technology and Society Magazine.

[177] Dampier C. Cyber Week shoppers sign up, impulse buy like crazy - City, 2019. URL https://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=0affa34d-2165-4424-a65a-6d6d2111d1e0.

[178] Rieger S, Sinders C. Dark Patterns: Regulating Digital Design 2020;.

[179] Amazon Help & Customer Service. AToU. Alexa Terms of Use - Amazon Customer Service, December 2021. URL https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740.

[180] Jang W, Chhabra A, Prasad A. Enabling Multi-user Controls in Smart Home Devices. Dallas Texas USA: ACM. ISBN 978-1-4503-5396-0, November 2017; 49–54. URL https://dl.acm.org/doi/10.1145/3139937.3139941.

[181] Bugeja J, Jacobsson A, Davidsson P. On Privacy and Security Challenges in Smart Connected Homes. In 2016 European Intelligence and Security Informatics Conference (EISIC). August 2016; 172–175.

[182] J S. The trust crisis: Facebook, Boeing and too many other firms are losing the public's faith. Can they regain it? - Círculo de Directores, 2019. URL http://www.circulodedirectores.org/2019/07/18/the-trust-crisis-facebook-boeing-and-too-many-other-firms-are-losing-the-publics-faith-can-they-regain-it/.

[183] Week M. How losing trust costs brands customers – and what marketers can do to prevent it, November 2021. URL https://www.marketingweek.com/losing-trust-costs-brands-customers/.

[184] Petro G. Amazon's Crisis Of Trust, March 2019. URL https://www.forbes.com/sites/gregpetro/2019/03/08/amazons-crisis-of-trust/. Section: Investing.

[185] Ventura T. Google's Crisis of Trust Is Damaging Its Reputation, December 2019. URL https://medium.com/swlh/googles-crisis-of-trust-is-damaging-its-reputation-3d5ab1b8430e.

[186] (Alexa) A. Design for International Markets | Alexa Design Guide, February 2021. URL https://developer.amazon.com/en-US/docs/alexa/alexa-design/internationalization.html.

[187] Google. Leveraging content localization to reach new audiences, 2020. URL https://adsense.google.com/intl/ar_jo/start/resources/localizing-your-content-can-help/.

[188] Inc A. Localize your SwiftUI app - WWDC21 - Videos, 2022. URL https://developer.apple.com/videos/play/wwdc2021/10220/.

[189] Apple. Change Siri voice or language, February 2022. URL https://support.apple.com/en-us/HT208316.

[190] Hardesty L. How Alexa learned Arabic, January 2022. URL https://www.amazon.science/latest-news/how-alexa-learned-arabic. Section: News and features.

[191] Labs S. Matter Standard Aligns the Smart Home Market - Silicon Labs, 2022. URL https://www.silabs.com/applications/matter-standard-aligns-the-smart-home-market.

[192] Media O. Matter Standard – the Future of Smart Home Design, March 2022. URL https://embeddedcomputing.com/application/consumer/smart-home-tech/matter-standard-the-future-of-smart-home-design.

[193] CHOIP P. Project Connected Home Over IP, December 2019. URL https://developer.amazon.com/en-US/alexa/devices/project-chip.html.

A APPENDIX-A: STUDY POSTER - USERS

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD

VOLUNTEERS NEEDED FOR INTERVIEWS

CUREC Approval Reference: (**CS_C1A_22_007**)

Exploring Privacy Protection Means in the Smart Home

What: -

- *45-60 minutes* of audio recorded interview.
- Do you live in a home with smart devices (e.g., Smart Cameras, Smart Speakers, Smart TV, Smart Door Lock, Smart Door Bell)?
- Do we use smart devices, or deal with it in the home?
- Do you have any concerns about smart devices?

Who: **A user, who knows or use smart devices.**
Where**: Online**
When**: will agree on a convenient time with the participant.**

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

https://oxford.onlinesurveys.ac.uk/oxford-online-surveys-demographic-information-for-explori-5

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.albayaydh@cs.ox.ac.uk

B APPENDIX-B: STUDY POSTER- LOCAL LEADERS

DEPARTMENT OF COMPUTER SCIENCE

VOLUNTEERS NEEDED FOR INTERVIEWS

CUREC Approval Reference: (**CS_C1A_22_007**)

Exploring Privacy Protection Means in the Smart Home

What: -

- *45-60 minutes* of audio recorded interview.
- Do you use smart devices, or deal with it in the home?
- Are you working in an organization that deal with smart devices design and production?
- Are you a smart device designer?
- Do you manage smart device design teams?
- How could we improve the technology to protect users' privacy?

Who: **A professional, who knows about smart device design.**
Where**: Online**
When**: will agree on a convenient time with the participant.**

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

https://oxford.onlinesurveys.ac.uk/oxford-online-surveys-demographic-information-for-explori-5

To thank you for your participation, you will receive a small voucher.

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

C APPENDIX-C: STUDY POSTER- DESIGNERS AND INDUSTRY LEADERS

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD

VOLUNTEERS NEEDED FOR INTERVIEWS

CUREC Approval Reference: (**CS_C1A_22_007**)

Exploring Privacy Protection Means in the Smart Home

What: -

- *45-60 minutes* of audio recorded interview.
- Do you use smart devices, or deal with it in the home?
- Are you a smart device designer?
- Do you manage smart device design teams?
- Are you an executive or manager in a smart device manufacturing company?
- Do you have general understanding of MENA Arab culture?
- How could we improve the technology to protect users' privacy?

Who: **A professional, who knows about smart device design.**
Where**: Online**
When**: will agree on a convenient time with the participant.**

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

https://oxford.onlinesurveys.ac.uk/oxford-online-surveys-demographic-information-for-explori-5

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.albayaydh@cs.ox.ac.uk

D APPENDIX-D: SCREENING SURVEY

In the screening survey, we start with introduction of the study, and the research ethics. Then we ask candidates the following questions.

1- Do you understand, and agree to take part in this survey?
- Yes, I understand and agree
- No, I prefer not to participate [Jump to Question-18]

Language

2- What is your preferred language to communicate with?
- English
- Arabic
- Both are fine
- None [Jump to Question-18]

Age

3- Age (Only 18+ years participants can participate in this survey)
- Less than 18 years [Jump to Question-18]
- 18-34 Years
- 35-64 Years
- > 65 Years

Gender

4- Gender?
- Female
- Male
- Prefer not to say

Education

5- What is the highest level of school you have completed?
- No school completed
- High School
- Trade/technical/vocational training
- Undergraduate studies
- Graduate studies: Master's or similar
- Postgraduate studies: PhD or similar

Culture

6- How can you describe your culture?
- Western (North America, Australia, and Europe)
- Latin American
- African Culture
- MENA Culture
- Indian Culture
- Chinese
- Far Eastern Culture

Experience with smart devices

7- How many years of experience do you have with smart devices?

- No Experience [Jump to Question-18]
- Few months
- 1 Year
- 2 years

Involvement with Smart Devices

8- Describe your level of involvement with smart home devices?
- User [Jump to Question-15]
- Working in a home with smart devices [Jump to Question-16]
- Designer
- Manage design team
- Work in local company in MENA region that deals with smart devices

Job Type

9- What is your job type?
- Smart Device - UX Designer
- Smart Device - Solution Architect
- Smart Device - Firmware Designer
- Smart Device - Privacy and Security
- Smart Device - Executive Position (CEO, GM, CCO, CTO, Product Manager)
- Other Design Responsibilities, please write down in the box.

Design Experience

10- How many years of smart device design experience do you have?
- None
- Less than 2 years
- From 2 to 5 years
- More than 5 years

Privacy and Data Protection

11- Do you consider privacy and data protection when you design new smart devices?
- Yes
- Not Directly
- No

Your Company

12- Where is your company operating from?
- North America
- UK
- Europe
- China
- Far East (Korea, Japan, Taiwan. Etc)
- MENA Region
- Africa
- Latin America

13- Where is your company selling its products?
- International Market - All the World
- UK and Europe
- Far East (China, Korea, Japan, etc)
- MENA Region
- Latin America
- Africa

14- What is the size of your company?
- 01-100
- 100-250
- 250-500
- 500-1000
- 1000

Bystanders

15- Do you have domestic worker [full time/part time] in your home?
- Yes
- No [Jump to Question-18]

Permission

16- We appreciate if you allow the researcher to interview you to understand more about the data protection in Jordan. Do you allow the researcher to contact you to arrange for the interview?
- Yes
- No

Contact details

17- If you agree to participate in the research interviews, please provide your throwaway email address and nickname. (This can be a throwaway email address if you wish to remain completely anonymous)

Final page

18- Thank you for participating in this survey.

E APPENDIX-E: INTERVIEW SCRIPTS - HOUSEHOLDS

A - Warm Up Questions

1- How many people live in the house?
2- Do you have a domestic worker?
   - [If yes] Is it fulltime worker?
   - [If part-time domestic worker] How often your domestic worker work in your home?
3- Do you have smart home devices? For how long you have your devices? How do you describe your experience with your smart devices?

B- Skill Assessment. For participants who did not participate in the focus group phase of the study, we'll ask questions and observe their responses to understand their experiences with smart home devices and privacy concerns. Our questions set include:

1. Novice (Basic):
   - How would you describe your initial experiences with smart home devices?
   - What challenges did you face when first using smart home technologies?
2. Competent**:**
   - Describe a situation where you successfully configured privacy settings for multiple smart home devices.
   - How do you balance usability and privacy concerns when using smart home technologies?
3. Proficient**:**
   - Provide examples of how you've adapted smart home configurations to meet specific privacy needs.
   - In what ways have you become more efficient in managing privacy settings over time?
4. Expert**:**
   - Discuss instances where you had to troubleshoot complex privacy issues in a smart home environment.
   - How do you foresee the future evolution of privacy features in smart home technologies?

C- To explore the employer's experience with the smart device(s)

1- What are the smart devices that you use in your home? Can you describe what they do?
   - [Do they/Does it] record video/audio?
   - [Is it/are they] only live-streaming device(s)?
   - Is the data sent over the Internet?
   - Do you know why the data is collected?
   - Do you know where the data is stored?
   - How do you think companies use the collected data?
   - Do you think companies benefit from your data? How?
   - [If you think that your data is valuable] How much your data worth in your opinion?

2- On a scale of 1 to 10, how proficient do you consider yourself to be with smart devices? 1 being a beginner and 10 being an expert.

3- Do you feel comfortable having smart device in your home?
   - [If they're uncomfortable] What could make you feel more comfortable about having a smart device in your home?

4- Do you have concerns with smart devices? What are the smart devices that concerns you the most?
5- What features in your smart devices that you feel concerned about?
6- Do you have any concerns with the design of your smart devices? Please explain
7- Do you have any concerns with the functions of your smart devices? Please explain
8- Do you have specific device(s) to check on domestic worker(s) inside your home?

9- Given the concerns you have about smart devices. Why do you buy and use your smart devices?
10- Who [is/are] the admin(s) of the smart device(s)? (you, family member, vendor's team member, or/and maintenance technician(s)
11- [Is/Are] the device(s) hidden? [If yes] Where inside the home are they hidden?
12- [Does/Do] your domestic worker(s) know that they are monitored by these devices?
13- Who else use smart devices in the home?
14- Do you know about data protection rights and about recording people in your home? Does Jordan have such laws?

D- Employers' Expectations, behaviours, and attitudes with smart devices & workers.

1- Do you think that the smart devices are well designed to protect people's data?
2- Have you told your domestic worker that you are using smart device(s)in your home? Please explain.
3- Have you asked whether it is okay to leave the smart device(s) on while the domestic worker is working?
4- Is there a way that the domestic worker(s) or whoever else can tell when the device(s) [Is/Are] on?
5- [Do/Does] your domestic worker(s) use smart devices or have access to the data? Please explain
6- Are you aware of the GDPR Data Subject Access Requests (SAR)? Have you tried using it?
7- Do you think manufacturers of smart devices are serious about improving data protection capabilities in the new devices they produce? Please explain.
8- What is your experience with privacy policies? please explain.
9- [Do/Does] your smart devices request consent to data collection/sharing at the point of setting up the devices [Do/Does] your domestic workers consent to devices? Please explain
the consent taking process.
10- Do you think domestic workers need to know about devices that are collecting data about them? What exactly?
11- Do you have concerns about passive [listening/watching] of the domestic worker to you [or/and] your smart device(s)?
12- Do you think it is common for [employers/families] who employ domestic worker(s) to monitor them?
13- [In your opinion] Do you think that [employers/families] think that it is their right to use smart device(s) whit out informing their domestic worker(s) about them? [If yes] Why?
14- Do you think your domestic workers or your guest have the right to ask you to switch off your smart devices, or at least not to monitor or record them?
15- Do you think people's attitudes about smart home devices in general have changed over time?
16- [From your experience] What approaches could be effective in protecting data of domestic workers with the smart devices design?
17- Do you think, it would be good if domestic worker is notified about smart devices?
18- How could we improve data protection of people with smart devices? Who is responsible for protecting people's data in your opinion?
19- Thank you, I am done. Would you like to add anything or, do you have any comments?

F APPENDIX-F: INTERVIEW SCRIPTS - WORKERS

A- Warm Up Questions

1- What is your job type?
2- How long have you had this job?
3- What do you like and dislike about your job?
4- Can you explain what is a smart home? And a Smart Device?
5- Did you work in smart home before? When? How many times? For how long time in total?

B- Skill Assessment. For participants who did not participate in the focus group phase of the study, we'll ask questions and observe their responses to understand their experiences with smart home devices and privacy concerns. Our questions set include:

1. Novice (Basic):
    - How would you describe your initial experiences with smart home devices?
    - What challenges did you face when first using smart home technologies?
2. Competent**:**
    - Describe a situation where you successfully configured privacy settings for multiple smart home devices.
    - How do you balance usability and privacy concerns when using smart home technologies?
3. Proficient**:**
    - Provide examples of how you've adapted smart home configurations to meet specific privacy needs.
    - In what ways have you become more efficient in managing privacy settings over time?
4. Expert**:**
    - Discuss instances where you had to troubleshoot complex privacy issues in a smart home environment.
    - How do you foresee the future evolution of privacy features in smart home technologies?

C- Questions to explore domestic worker's experience of smart home and smart devices.

1- On a scale of 1 to 10 , how proficient do you consider yourself to be with smart devices? 1 being a beginner and 10 being an expert.
2- What are the smart devices that are used in the homes you are have worked in?
3- Regarding the smart device functions:
    - ・Do they record video/audio?
    - ・Are they live-streaming device(s)?
    - ・Is the data sent over the Internet?
    - ・Do you know where the data is stored? Do you know for how long the data is stored?
    - ・Do you know what they do with the data?
    - ・Do you know who can [see/hear/read] the data? …Who?
    - ・Can you access the data? [If Yes] How do you access it? How do you use it?
    - ・Do your employer [the family] keep the device turned on while you are in home?
    - ・Are the devices hidden? [If yes] Where inside the home are they hidden?
    - ・[If you think that your data is valuable] How much your data worth in your opinion?
4- Why do you think that families use smart devices?
5- Do you know, if families use specific devices to monitor you? or to monitor non-family members? Do you know why?
6- Do you know, if the smart devices are used for other purposes as well?
7- Are you aware of the laws and data protection regulation about monitoring and recording people in Jordan? Does Jordan have such laws?

G APPENDIX-G: INTERVIEW SCRIPTS - LOCAL BUSINESS LEADERS

A- Warm Up Questions

1- Can you tell me briefly about yourself and your job, your role., and your responsibilities?
2- Can you tell me what your company produce? Please explain.
3- How many years of experience do you have in this field? Please explain

B- Skill Assessment. For participants who did not participate in the focus group phase of the study, we'll ask questions and observe their responses to understand their experiences with smart home devices and privacy concerns. Our questions set include:

1. Novice (Basic):
    - How would you describe your initial experiences with smart home devices?
    - What challenges did you face when first using smart home technologies?
2. Competent**:**
    - Describe a situation where you successfully configured privacy settings for multiple smart home devices.
    - How do you balance usability and privacy concerns when using smart home technologies?
3. Proficient**:**
    - Provide examples of how you've adapted smart home configurations to meet specific privacy needs.
    - In what ways have you become more efficient in managing privacy settings over time?
4. Expert**:**
    - Discuss instances where you had to troubleshoot complex privacy issues in a smart home environment.
    - How do you foresee the future evolution of privacy features in smart home technologies?

C- Main Question

1- Do you take data protection into consideration? Please explain
2- Are you aware of any local or regional smart device manufactures/designers? Please explain.
3- What are the challenges that local/regional smart devices companies face? Please explain
4- In general, do you think users' data is protected within the functionalities of the smart products you sell/import? Do you think companies consider data protection? Please explain
5- Do you think producing smart devices locally could support data protection in the design of smart devices? How?
6- How do companies identify data protection requirements for new smart product?
7- How do companies localize smart products? What are the challenges? Please explain
8- [After we explain what do we mean by bystanders] Do you consider Bystanders' data into consideration as well?
9- Do the products you sell/import recognize bystanders from other users? Please explain
10- Do you think improving data protection within smart products reduces the efficiency and productivity of them?
11- Do you think considering users' concerns, could negatively affect the commercial and business targets for these products specifically? positively?
12- Do you consider feedback from users? How do you get it?
13- What are the challenges that the organization faces to identify and address data protection? And data protection of bystanders in the smart homes? Please explain
14- Do you think domestic workers as bystanders in the smart homes can protect their data with smart devices? How could we improve protection by design? Please explain
15- Did you receive any information about the different contexts where the devices could be used?
16- Do you – in general- take the differences between different contexts into consideration when you sell/import smart devices?

17- Are you aware of the middle east context and whether the designed devices are suitable to this context?
18- Do you know –in general- if there are in this domain designers who consider the middle east context in the design process?
19- From your experience, where are the majority of companies that perform smart devices design are located?
20- Do you know personally, or do you know of designers who are from middle east region, or are aware of the region culture and norms? Please explain
21- Do you think vendors are concerned about recruiting designers form different region to cover all contexts, cultures and norms when they design privacy setting in the smart devices?
22- Do you consider empowering powerless users in the contexts where the devices used to protect their data? Please explain
23- Can you tell me what from the below features are adopted in your products to support data protection?
- Features to notify users, such as beep sound, red light indicator, or red blinking light?
- Features to hide/delete bystanders' data?
- Features to accept command from users [hand movement, face gestures, and voice commands]
- Privacy mode settings. [Guest mode, family privacy mode, time windows]

24 Are there specific ideas or expectations from future technologies?
25 To what extent do you think that your company is responsible for data protection? Who else is responsible as well?
26 Does your organization deploy or plan to incorporate the outcomes of the new innovations in its future products to support data protection? How?
27 How confident is your organization that users who use your products are protected when it comes to data breaches?
28 Are their design guidelines that consider data protections?
29 What is your expectations for local/regional manufacturing of smart devices?
30 How data protection regulations are effective in protecting user's data? Are you aware of such laws?
31 How do you think we can orchestrate the product design, the data protection regulations, and the public awareness to ensure privacy protection of users?
32 How could laws influence/enforce smart devices vendors to produce smart devices with enhanced data protection features?
33 Thank you, I am done. Would you like to add anything or, do you have any comments?

H APPENDIX-H: INTERVIEW SCRIPTS - DESIGNERS

A- Warm Up Questions

1- Can you tell me briefly about yourself and your job, your role., and your responsibilities?
2- How many years of experience do you have in this field?
3- What are the devices that you have worked on?

B- Skill Assessment. For participants who did not participate in the focus group phase of the study, we'll ask questions and observe their responses to understand their experiences with smart home devices and privacy concerns. Our questions set include:

1. Novice (Basic):
    - How would you describe your initial experiences with smart home devices?
    - What challenges did you face when first using smart home technologies?
2. Competent**:**
    - Describe a situation where you successfully configured privacy settings for multiple smart home devices.
    - How do you balance usability and privacy concerns when using smart home technologies?
3. Proficient**:**
    - Provide examples of how you've adapted smart home configurations to meet specific privacy needs.
    - In what ways have you become more efficient in managing privacy settings over time?
4. Expert**:**
    - Discuss instances where you had to troubleshoot complex privacy issues in a smart home environment.
    - How do you foresee the future evolution of privacy features in smart home technologies?

C- Designers Questions

1- If I ask you, who is the smart device designer. What would you tell me?
2- [In general] When you design and develop devices. What are the main elements of the design and development process?
3- Does your company localize smart devices to fit in the context of use? How?
4- How do you understand users concerns with smart home devices?
5- Did you receive any information about the different contexts where the devices could be used?
6- How do you take data protection into consideration?
7- In general, do you think users' data is protected within the functionalities of the smart products your company design? Do you think companies consider data protection? Please explain
8- How do companies identify data protection requirements for new smart product?
9- Do you have a process to incorporate data protection within the design of the smart devices? Do you have any influence on these processes? Do you think employees' culture impact companies' design processes? Please explain?
10- Are manufactures are obliged by certain laws or regulation to adopt certain features? Please explain.
11- How does your organization identify data protection requirements for new product?
12- [After we explain what do we mean by bystanders] Do companies – in general- consider Bystanders concerns with the smart devices?
13- How do smart products recognize bystanders from other users?
14- Do the products you design recognize bystanders from other users? Please explain
15- Do you think improving data protection within smart products reduces the efficiency and productivity of them?
16- Do you think considering users' concerns, could negatively affect the commercial and business targets for these products specifically? positively?

17- Do you think domestic workers as bystanders in the smart homes can protect their data with smart devices? How could we improve protection by design? Please explain
18- Do you – in general- take the differences between different contexts into consideration when you design smart devices?
19- From your experience, where are the majority of companies that perform smart devices design are located?
20- Do you think vendors are concerned about recruiting designers form different region to cover all contexts, cultures and norms when they design privacy setting in the smart devices?
21- Can you tell me what from the below features are adopted in your products to support data protection?

- Features to notify users, such as beep sound, red light indicator, or red blinking light?
- Features to hide/delete bystanders' data?
- Features to accept command from users [hand movement, face gestures, and voice commands]
- Privacy mode settings. [Guest mode, family privacy mode, time windows]
- Are there specific ideas or expectations from future technologies?

22- To what extent do you think that your company is responsible for data protection? Who else is responsible as well?
23- Does your organization deploy or plan to incorporate the outcomes of the new innovations in its future products to support data protection? How?
24- How confident is your organization that users who use your products are protected when it comes to data breaches?
25- Are their design guidelines that consider data protections?
26- How data protection regulations are effective in protecting user's data? Are you aware of such laws?
27- How do you think we can orchestrate the product design, the data protection regulations, and the public awareness to ensure privacy protection of users?
28- What strategies can be employed to address the design cost, particularly when dealing with new contexts?
29- How could laws influence/enforce smart devices vendors to produce smart devices with enhanced data protection features?
30- Do manufacturers consider the imbalanced power dynamics between users in the smart home context?
31- Do you consider empowering powerless users in the contexts where the devices used to protect their data? Please explain
32- Does your company consider feedback from users? Please explain
33- How do you understand value of users' data value [in your opinion]?
34- Are you aware of the middle east context and whether the designed devices and data protection settings are suitable to this context? Do you know if vendors consider this context during the design process?
35- How do you think we can support and improve data protection of users?
36- I am done with my questions; do you like to add anything?

I APPENDIX-I: INTERVIEW SCRIPTS - INTERNATIONAL BUSINESS LEADERS

A- Warm Up Questions

1- Can you tell me briefly about yourself and your job, your role., and your responsibilities?
2- How many years of experience do you have in this field?
3- What are the devices that you sell?

B- Skill Assessment. For participants who did not participate in the focus group phase of the study, we'll ask questions and observe their responses to understand their experiences with smart home devices and privacy concerns. Our questions set include:

1. Novice (Basic):
    - How would you describe your initial experiences with smart home devices?
    - What challenges did you face when first using smart home technologies?
2. Competent**:**
    - Describe a situation where you successfully configured privacy settings for multiple smart home devices.
    - How do you balance usability and privacy concerns when using smart home technologies?
3. Proficient**:**
    - Provide examples of how you've adapted smart home configurations to meet specific privacy needs.
    - In what ways have you become more efficient in managing privacy settings over time?
4. Expert**:**
    - Discuss instances where you had to troubleshoot complex privacy issues in a smart home environment.
    - How do you foresee the future evolution of privacy features in smart home technologies?

C- Designers Question

1- If I ask you, who is the smart device designer. What would you tell me?
2- [In general] When your team develop devices. What are the main elements of the design and development process?
3- Do you take users' data protection into consideration?
4- Do you have a process to incorporate data protection within the design of the products? Do you and designers have any influence on these processes? Please explain?
5- How does your organization identify data protection requirements for new product?
6- Do you localize devices to fit in the context of use? How?
7- [After we explain what do we mean by bystanders] Do companies – in general- consider Bystanders concerns with the smart devices?
8- Do the products you design recognize bystanders from other users? Please explain
9- Do you think domestic workers as bystanders in the smart homes can protect their data with smart devices? How could we improve protection by design? Please explain
10- Do you think improving data protection within smart products reduces the efficiency and productivity of them?
11- Do you think considering users' concerns, could negatively affect the commercial and business targets for these products specifically? positively?
12- Do you – in general- take the differences between different contexts into consideration when you design smart devices?
13- From your experience, where are the majority of companies that perform smart devices design are located?
14- Do you think vendors are concerned about recruiting designers form different region to cover all contexts, cultures and norms when they design privacy setting in the smart devices?
15- Does your company consider feedback from users?
16- What are the challenges that the organization faces to address data protection?

17- Is your company aware of or consider middle east context in the design process?
18- Can you tell me what from the below features are adopted in your products to support data protection?

- Features to notify users, such as beep sound, red light indicator, or red blinking light?
- Features to hide/delete bystanders' data?
- Features to accept command from users [hand movement, face gestures, and voice commands]
- Privacy mode settings. [Guest mode, family privacy mode, time windows]
- Are there specific ideas or expectations from future technologies?

19- To what extent do you think that your company is responsible for data protection? Who else are responsible as well?
20- Does your organization deploy or plan to incorporate the outcomes of the new innovations in its future products to support data protection? How?
21- How confident is your organization that users who use your products are protected when it comes to data breaches?
22- Are their design guidelines that consider data protections?
23- How do you think we can orchestrate the product design, the data protection regulations, and the public awareness 24- ensure privacy protection of users?
24- How data protection regulations are effective in protecting users data? Are you aware of such laws?
25- How could laws influence/enforce smart devices vendors to produce smart devices with enhanced data protection features?
26- Are vendors obliged by laws/regulation to incorporate some features during the design process, especially those related to data protection?
27- Do manufacturers consider the imbalanced power dynamics between users in the smart home context?
28- Do you consider empowering powerless users in the contexts where the devices used to protect their data? Please explain
29- Did you receive any information about the different contexts where the devices could be used?
30- Are you aware of the middle east context and whether the designed devices and data protection settings are suitable to this context? Do you know if vendors consider this context during the design process?
31- How do you understand value of users' data value [in your opinion]?
32- How do you think we can support and improve data protection of users?
33- I am done with my questions, do you like to add anything?

Received January 2023; revised October 2023; accepted December 2023