# Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan




Wael AlBayaydh

Department of Computer Science

University of Oxford

A thesis submitted for the degree of

*Doctor of Philosophy*

Hilary Term-24

# Acknowledgements

This thesis stands as a testament to the collective efforts and support of numerous individuals who have played pivotal roles in its successful completion. I extend my sincere appreciation to my family, whose unwavering support has been the cornerstone of my academic journey. Special acknowledgments go to Prof. Ivan Flechais, my esteemed supervisor, Prof. Sadie Creese, my academic advisor, and Prof. Aleks Kissenger, my college advisor, for their invaluable guidance and insights, shaping the trajectory and elevating the quality of this research.

I would like to extend my heartfelt thanks to Prof. Max Van Kleek, Prof. Reuben Binns, and Prof. Ruba Abu Salma for their insightful comments and meaningful suggestions. Their constructive feedback and guidance have been invaluable.

Central to the success of this endeavor are the dedicated participants of the research study. Their generosity in sharing time and experiences has proven indispensable, contributing significantly to our comprehension of privacy concerns in smart homes, particularly within the context of Jordan. The findings are poised to positively influence future research and interventions in this domain.

I express deep gratitude to my family members for their unwavering emotional support, providing the strength needed to navigate the complexities of this research. Their encouragement has been commendable and instrumental in this journey.

To my colleagues and peers, I extend thanks for their constructive feedback and engaging discussions that enriched various stages of the research study. Their input has been crucial in refining concepts and arguments presented in this thesis.

Finally, I am grateful to my extensive circle of friends for their enduring encouragement and understanding during the demanding hours and steadfast dedication required for this research. Their unwavering support has been a constant source of motivation.

This research is an embodiment of a collaborative effort involving diverse individuals, and I am profoundly humbled by the collective contributions that have made its realization possible.

# Abstract

The proliferation of smart home devices has raised many privacy concerns among smart home inhabitants. Previous research has mostly focused on family members and device owners in Western contexts (i.e., Europe and North America). In contrast, this research study examines the Muslim Arab Middle Eastern (MAME) context of Jordan to investigate how different cultural, social, and religious norms affect privacy concerns and practices in smart homes in Jordan.

Our research starts with a literature review of the privacy concerns of bystanders in smart homes – individuals who are subjected to the smart device use of others – identifying several gaps in this area. Our studies seek to understand the privacy concerns and expectations of smart home bystanders and households in Jordan, with a particular focus on domestic workers. We explore legal and regulatory perspectives on privacy protection and how these relate to the tensions that may arise between households and their domestic workers. We also examine the complex power dynamics between domestic workers and households, particularly in spaces that function as both a residence and a workplace. This dual-use of smart homes has created gaps in workplace protections that favor households. Finally, we explore smart device design challenges for privacy protection, and we assess how a co-designed mobile application can be used as an auxiliary tool to support privacy protection of bystanders in Jordanian smart homes.

Ultimately, the outcomes of this thesis contribute to addressing the complex and intricate issues that arise from the use of smart technology in households that employ domestic workers. We anticipate that our findings will not only inform future research and offer recommendations for social interventions but also facilitate the improvement of privacy protection measures by informing smart device design and influencing the development of policies and regulations that offer better support for the privacy protection in smart homes. It is crucial to stress that collaborative interventions are essential from all stakeholders.

# Contents

**List of Figures** **x**

**List of Tables** **xi**

**List of Abbreviations** **xii**

**1 Introduction** **1**

1.1 Problem Statement and Motivation . . . . . 2

1.1.1 Growing Adoption of Smart Home Devices . . . . . 2

1.1.2 Privacy Concerns with Smart Devices . . . . . 3

1.1.3 Research Gap . . . . . 4

1.1.4 Research Questions . . . . . 5

1.2 Research Contributions . . . . . 7

1.3 Publications . . . . . 8

1.4 Thesis Structure . . . . . 8

**2 BACKGROUND** **10**

2.1 The Research Context - The Hashemite Kingdom of Jordan . . . . 10

2.1.1 Social Structure in Jordan . . . . . 12

2.1.2 Culture and Values in Jordan . . . . . 17

2.1.3 Islam Impact on Society . . . . . 18

2.1.4 Economy and Work Force in Jordan . . . . . 19

2.2 Literature Review . . . . . 22

2.2.1 Privacy . . . . . 22

2.2.2 Human-Computer Interaction and Privacy . . . . . 31

2.2.3 Smart Home and Privacy . . . . . 36

2.2.4 Power Dynamics . . . . . 38

2.2.5 Privacy Protection Regulations . . . . . 42

2.3 Conclusion . . . . . 56

**3 Methodology** **57**
3.1 Privacy and Security Research Approaches . . . . . 57
3.1.1 Human Computer Interaction Approaches . . . . . 58
3.2 Adopted Research Approaches . . . . . 61
3.2.1 Grounded Theory . . . . . 61
3.2.2 Thematic Analysis . . . . . 65
3.2.3 Data Collection Methods . . . . . 65
3.2.4 Validity of Findings . . . . . 67
3.3 Research Approach and Methodology . . . . . 69
3.3.1 Smart Home Privacy Concerns (RQ1) . . . . . 69
3.3.2 Power Dynamics, and Data Protection Regulation (RQ2) . . 71
3.3.3 Privacy Protection with Smart Device Design (RQ3.1 and RQ3.2) . . . . . 73
3.3.4 Support Bystanders Privacy Protection in the Smart Home (RQ3.3) . . . . . 75
3.4 Ethical Considerations . . . . . 78

**4 Privacy Concerns** **79**
4.1 Motivation . . . . . 80
4.2 Methodology and Research Question . . . . . 80
4.2.1 Recruitment . . . . . 80
4.2.2 Interviews . . . . . 82
4.2.3 Analysis . . . . . 83
4.2.4 Research Ethics . . . . . 84
4.2.5 Limitations . . . . . 85
4.3 Findings and Results . . . . . 85
4.3.1 Limited Public Awareness . . . . . 86
4.3.2 Smart Home Privacy Concerns, Practices, and Expectations 89
4.3.3 Rights Perceptions and Expectations . . . . . 92
4.3.4 Contextual Influences . . . . . 95
4.3.5 Aspirations for Privacy Control . . . . . 96
4.4 Discussion and Recommendations . . . . . 97
4.4.1 Summary of Findings . . . . . 97
4.4.2 Recommendations for Public Awareness . . . . . 98
4.4.3 Recommendations for Policymakers . . . . . 98
4.4.4 Recommendations for Smart Device Designers . . . . . 99
4.5 Conclusion . . . . . 100

**5 Smart Home Power Dynamics 101**
5.1 Motivation . . . 102
5.2 Methodology . . . 102
5.2.1 Recruitment . . . 103
5.2.2 Methodology and Interviews . . . 106
5.3 Limitations . . . 109
5.4 Results and Findings . . . 110
5.4.1 Smart Home Power Dynamics . . . 111
5.4.2 Perspectives on Mitigating Smart Home Power Dynamics . . . 118
5.5 Discussion and Recommendations . . . 122
5.5.1 Summary of Findings . . . 122
5.5.2 Contextual Interventions . . . 123
5.5.3 Technical Considerations and Interventions . . . 127
5.6 Conclusion . . . 130

**6 Privacy Protection With Smart Device Design 131**
6.1 Motivation . . . 132
6.2 Methodology and Research Question . . . 132
6.2.1 Recruitment . . . 133
6.2.2 Methodology and Interviews . . . 137
6.3 Limitations . . . 143
6.4 Findings and Outcomes . . . 144
6.4.1 Privacy Protection Through Smart Device Design . . . 145
6.4.2 Perspectives and Challenges of Privacy Protection for Smart Device Design . . . 151
6.5 Discussion and Recommendations . . . 161
6.5.1 Summary of Findings . . . 161
6.5.2 Social Considerations and Interventions . . . 162
6.5.3 Technical Considerations and Interventions . . . 165
6.5.4 Business Considerations and Interventions . . . 167
6.5.5 Legal Considerations and Interventions . . . 171
6.6 Conclusion . . . 172

**7 CO-DESIGN AND TECHNOLOGY PROBE 174**
7.1 Motivation . . . 175
7.2 Methodology and Research Approach . . . 175
7.2.1 Recruitment . . . 177
7.2.2 Methodology . . . 180
7.2.3 Data Analysis . . . 183
7.2.4 Research Position and Ethics . . . 185

7.2.5 Limitations . . . 186
7.3 Findings of the Focus Groups Study . . . 187
7.3.1 Privacy Protection with the App . . . 188
7.3.2 Considerations and Challenges . . . 194
7.4 Developing and Evaluating the App . . . 197
7.4.1 The App Features and Use . . . 197
7.4.2 Evaluation of The App . . . 198
7.5 Discussion and Recommendations . . . 205
7.5.1 Summary of the Findings . . . 205
7.5.2 Recommendations . . . 209
7.6 Conclusion . . . 212

**8 DISCUSSION 214**
8.1 Summary of Findings . . . 215
8.2 Bystanders' Privacy with Smart Homes in Jordan . . . 217
8.2.1 Overlooked Jordanian Context . . . 218
8.2.2 Awareness is Cornerstone for Privacy Protection . . . 221
8.2.3 Power Dynamics and Contextual Influences . . . 224
8.2.4 Vague Data Protection Regulation . . . 226
8.2.5 Technical and Business Support for Privacy Protection . . . 229
8.2.6 Design Insights for Privacy Mobile App . . . 232
8.2.7 **Responsible Innovation** . . . 233
8.3 **Moral Obligations and Ethical Responsibility** . . . 233
8.4 Conclusion . . . 234

**9 CONCLUSION 236**
9.1 Key Findings . . . 237
9.1.1 Jordanian Context Oversight . . . 237
9.1.2 Limited Awareness of Smart Technologies and Privacy . . . 238
9.1.3 Asymmetric Power Dynamics and Contextual Influences . . . 239
9.1.4 Lack of Explicit Privacy Regulation . . . 239
9.1.5 Design Challenges for Privacy Protection . . . 240
9.1.6 Auxiliary Tools for Privacy Enhancement . . . 241
9.2 Critical Review . . . 242
9.3 Future Research . . . 245
9.3.1 Explore Privacy Concerns in other MAME Contexts . . . 245
9.3.2 Explore Data Protection Regulation in MAME Region . . . 246
9.3.3 Investigate Other Bystanders . . . 246
9.3.4 Innovation in Smart Device Design . . . 246
9.3.5 Improving Communication Among Different Stakeholders . . . 247
9.3.6 Explore Innovative Ways for Consent Taking . . . 247
9.3.7 Explore Privacy-Enhancing Interventions . . . 247

**Appendices**

**A Thesis Definitions** **250**
A.1 Definitions . . . 250
A.1.1 The Smart Home Device . . . 250
A.1.2 The Smart Home . . . 251
A.1.3 The Smart Home's Bystanders . . . 252
A.1.4 Usability . . . 253
A.1.5 Designers of Smart Device and Design Process . . . 253

**B Chapter 4 Supplementary Material** **254**
B.1 First Study - Advertisement Poster . . . 255
B.2 First Study - Screening Survey Questions . . . 256
B.3 Families Interview Guideline Questions . . . 258
B.4 Workers Interview Guideline Questions . . . 261

**C Chapter 5 Supplementary Material** **264**
C.1 Second Study - Advertisement Poster . . . 265
C.2 Second Study - Screening Survey Questions . . . 266
C.3 Second Study Families Interview Guideline Questions . . . 268
C.4 Second Study Workers Interview Guideline Questions . . . 270
C.5 Second Study Regulators Interview Guideline Questions . . . 272
C.6 Second Study Activists Interview Guideline Questions . . . 274
C.7 USENIX - Distinguished Paper Award . . . 276

**D Chapter 6 Supplementary Material** **277**
D.1 Poster - Users . . . 278
D.2 Poster - Local Leaders . . . 279
D.3 Poster - Designers and Industry Leaders . . . 280
D.4 Screening Survey Questions . . . 281
D.5 Families Interview Guideline Questions . . . 284
D.6 Workers Interview Guideline Questions . . . 286
D.7 Local Leaders Interview Guideline Questions . . . 288
D.8 Designers Interview Guideline Questions . . . 290
D.9 International Leaders Interview Guideline Questions . . . 292

**E Chapter 7 Supplementary Material** **294**
E.1 Poster - Users . . . 295
E.2 Poster - Designers and Mobile Developers . . . 296
E.3 Screening Survey Questions . . . 297
E.4 Focus Group Guidelines . . . 299
E.5 App Evaluation Interview Guidelines . . . 301

**F Methodology and Approach Supplementary Material** **303**
F.1 Screenshot of NVivo Software . . . . . 303
F.2 Screenshot of Focus Group Meeting . . . . . 304
F.3 Screenshot of Posting Study Posters on Social Media Platforms . . 304

**G Ethics Applications and Approval** **305**
G.1 First Study - Ethics Application . . . . . 305
G.1.1 First Study - Advertisement Poster . . . . . 305
G.1.2 First Study - Survey Question Guidelines . . . . . 306
G.1.3 First Study - Interview Question Guidelines . . . . . 306
G.1.4 First Study Ethics Application . . . . . 307
G.1.5 First Study - Information Sheet . . . . . 319
G.1.6 First Study - Consent Form . . . . . 322
G.2 Second Study Ethics Application . . . . . 325
G.2.1 Second Study - Advertisement Poster . . . . . 325
G.2.2 Second Study - Survey Question Guidelines . . . . . 325
G.2.3 Second Study - Interview Question Guidelines . . . . . 325
G.2.4 Second Study Ethics Application . . . . . 326
G.2.5 Second Study Information Sheet . . . . . 338
G.2.6 Second Study Consent Form . . . . . 341
G.3 Third Study Ethics Application . . . . . 344
G.3.1 Third Study - Advertisement Poster . . . . . 344
G.3.2 Third Study - Survey Question Guidelines . . . . . 344
G.3.3 Third Study - Interview Question Guidelines . . . . . 344
G.3.4 Third Study Ethics Application . . . . . 345
G.3.5 Third Study Information Sheet . . . . . 357
G.3.6 Third Study - Consent Form . . . . . 360
G.4 Fourth Study Ethics Application . . . . . 363
G.4.1 Fourth Study - Advertisement Poster . . . . . 363
G.4.2 Fourth Study - Survey Question Guidelines . . . . . 363
G.4.3 Fourth Study - Interview Question Guidelines . . . . . 363
G.4.4 Fourth Study Ethics Application . . . . . 364
G.4.5 Fourth Study Information Sheet . . . . . 376
G.4.6 Fourth Study - Consent Form . . . . . 379

**References** **382**

# List of Figures


1.1 Thesis Structure . . . . . 9

2.1 Jordan Location . . . . . 11
2.2 Jordan Religious Groups, Ethnic Groups, and Urban/Rural Distributions . . . . . 12

3.1 Research Approach and Dissertation Roadmap . . . . . 70
3.2 Fourth Study Approach [Co-Design Approach] . . . . . 76

4.1 First Study Research Process and Methodology . . . . . 81
4.2 Visual Representation of Themes and Codes . . . . . 87

5.1 Visual Representation of Categories and Themes . . . . . 111

6.1 Research Process and Methodology . . . . . 136
6.2 Visual Presentation of Categories and Themes . . . . . 146
6.3 Smart Device Design Process . . . . . 148

7.1 Research Process and Applied Methodology [Co-Design Approach] . 183
7.2 Guidance on How to Use the App . . . . . 199
7.3 The Mobile App Screens . . . . . 200

F.1 Screenshot of the NVivo Software . . . . . 303
F.2 Screenshot From a Focus Group Meeting . . . . . 304
F.3 Screenshots of Posters Shared on Social Media Platforms . . . . . 304

# List of Tables


1.1 Existing Publications . . . . . 8

2.1 Status of Data Protection Regulation in World Leading Countries . 43
2.2 Existing Laws in Jordan . . . . . 50
2.3 Status of Data Protection Regulation in MAME Countries . . . . . 52

3.1 Ethics Approval Numbers . . . . . 78

4.1 Demographic Information of Participants . . . . . 82
4.2 Summary of Themes and Codes . . . . . 86

5.1 Demographic Information of Domestic Workers . . . . . 105
5.2 Demographic Information of Households . . . . . 105
5.3 Demographic Information of Policy Makers &Activists . . . . . 105
5.4 Summary of Categories and Themes . . . . . 111

6.1 Demographic Information of Users (Families and Domestic Workers) 137
6.2 Demographic Information of Local Business Leaders . . . . . 138
6.3 Demographic Information of Designers . . . . . 138
6.4 Demographic Information of International Business Leaders . . . . . 138
6.5 Summary of Categories and Themes . . . . . 145

7.1 Demographic Information of Participants . . . . . 181
7.2 Focus Groups - Categories and Themes . . . . . 188
7.3 Requirements for The App . . . . . 198
7.4 Evaluation of the App- Categories and Themes . . . . . 199

# List of Abbreviations

**MENA** . . . . Middle East North Africa.

**MAME** . . . . Muslim Arab Middle East.

**DpbD** . . . . . Data Protection by Design.

**PbD** . . . . . Privacy by Design.

**SbD** . . . . . Security by Design.

**GDPR** . . . . . General Data Protection Regulation.

**NDA** . . . . . Nondisclosure Agreement.

**GT** . . . . . Grounded Theory.

**HCI** . . . . . Human-Computer Interaction.

**IoT** . . . . . Internet of Things.

**IT** . . . . . Information Technology.

**ICT** . . . . . Information Communication Technology.

**UI** . . . . . User Interface.

**UX** . . . . . User Experience.

**SOUP** . . . . . Symposium on Usable Privacy and Security.

**CHI** . . . . . ACM Conference on Human Factors in Computing Systems.

**CSCW** . . . . Computer-Supported Cooperative Work.

**PDE** . . . . . Personal Data Economy.

**ITU** . . . . . International Telecommunication Union.

**GSMA** . . . . International Mobile Industry Organization.

**TMForum** . . ICT International Organization.

**MODEE** . . . International Data Corporation.

**CNIL** . . . . . French National Data Protection Commission.

**AI** . . . . . Artificial Intelligence.

**ML** . . . . . Machine Learning.

**SEMIOTICS** . The Study of Signs, Symbols, and Their Meaning.

**RI** . . . . . Responsible Innovation.

**PIPEDA** . . . Personal Information Protection and Electronic Documents Act.

**Turkey DPL** . Data Protection Law.

**Brazil LGPD** General Data Protection Law.

**HIPAA** . . . . Health Insurance Portability and Accountability Act.

**GLBA** . . . . . Gramm-Leach-Bliley Act.

**CCPA** . . . . . California Consumer Privacy Act.

**CPRA** . . . . . California Privacy Rights Act.

**NYPA** . . . . . New York Power Authority.

**COPPA** . . . . Children's Online Privacy Protection Rule.

**FERPA** . . . . Family Educational Rights and Privacy Act.

**China PIPL** . The China Personal Information Protection Law.

**India DPDP** . Digital Personal Data Protection Bill.

**India DPA** . . India Data Protection Authority.

**Malaysia PDP** Malaysia Personal Data Protection.

**SDAIA** . . . . Saudi Data and Artificial Intelligence Authority.

**Saudi-PDPL** . Personal Data Protection Law.

**UAE** . . . . . United Arab Emirates.

**UAE PDP** . . Personal Data Protection.

**QFC** . . . . . Qatar Financial Center.

**Qatar PDPPL** Qatar Data Protection Law.

**MTCIT** . . . . Oman Ministry of Transport, Communications and Information.

**Bahrain MoJ** Ministry of Justice, Islamic Affairs and Waqf.

**Bahrain PDPL** Bahrain Personal Data Protection Law.

**Egypt PDPC** Egypt Personal Data Protection Law.

**KVKK** . . . . Turkey-Personal Data Protection Authority.

**EDPS** . . . . . The European Data Protection Supervisor.

**CAC** . . . . . Cyberspace Administration of China.

**ANPD** . . . . . Brazil-National Data Protection Authority.

**OPC** . . . . . Office of the Privacy Commissioner of Canada.

# 1 Introduction

Smart technologies continue to raise concerns about privacy protection for both households and bystanders[1] who may be targets of incidental or intentional monitoring. Domestic workers[2] are an example of bystanders in smart homes who experience complex power dynamics and can be subjected to exploitative practices that are further facilitated through smart technology. While past research has focused on Western contexts to explore how smart technologies and power dynamics affect the privacy of households and smart home bystanders, there is a limited understanding of the impact of such factors within non-Western contexts.

This thesis aims to explore the privacy concerns and expectations of smart home bystanders in Jordan, with a particular emphasis on domestic workers. We examine the legal and regulatory perspectives on privacy protection and their implications for the potential tensions between households and their domestic workers. Additionally, we investigate the complex power dynamics between domestic workers and households, especially in spaces serving as both residences and workplaces. Finally, we investigate the challenges in smart device design for privacy protection and evaluate the potential of a co-designed technology probe (mobile application) as an auxiliary tool to support the privacy protection of bystanders in Jordanian smart homes.

[1] Individuals who are subjected to the smart device use of others

[2] Domestic workers in this thesis refer to babysitters, nannies, home nurses, caregivers, and maids.

In Section §1.1, we discuss the problem domain, characterize the existing research gap, and formulate a series of research questions. Our contributions are summarized in Section §1.2, and the publications resulting from this work are documented in Section §1.3. The overall thesis structure is then presented in Section §1.4.

## 1.1 Problem Statement and Motivation

### 1.1.1 Growing Adoption of Smart Home Devices

According to the Fortune Business Insights Report[3], the global smart home market is projected to grow from USD 99.89 billion to USD 380.52 billion at a CAGR of 21.1% from 2021 to 2028. Additionally, the Statista Report[4] indicates that connected smart home devices, including cameras, smart TVs, smart speakers, thermostats, and smart doorbells, are present in 175 million households globally and are expected to reach 478 million households by 2025. This global proliferation of smart home devices is reshaping the internet landscape, with smart homes expected to generate 79.4 zettabytes (ZB) of data globally by 2025, as projected by IDC's[5] forecast[6].

Another report[7] from GSMA[8] forecasts that licensed cellular IoT connections will globally reach 4 billion by 2025, with 32 million connected smart devices in the MENA[9] region. Concurrently, the Jordan Digital Strategy[10] reports a growing adoption of smart devices in the country, in addition to a report from Statista[11] on the Smart Home market in Jordan that anticipates that the number of active smart homes is expected to reach 0.2 million users by 2027, with a penetration rate of 8.9% by the same year.

[3]Report-Fortune Business Insights Report
[4]Report-Statista Report- Number of Smart Homes forecast in the World until 2025
[5]IDC-International Data Corporation
[6]IDC Report-A forecast by International Data Corporation
[7]Report-GSMA Report: Realising the potential of IoT in ME
[8]GSMA: Global ICT industry organisation
[9]MENA - Middle East and North Africa
[10]Growth of smart devices in Jordan, Jordan Digital Strategy
[11]Statista Report-Forecast of smart home growth in Jordan until 2027

### 1.1.2 Privacy Concerns with Smart Devices

The social and economic landscape of modern homes has been transformed by the growing adoption of smart technologies (cf. Section §1.1.1). As pointed out by Yao et al. [1], the integration of multiple smart devices has led to the evolution of traditional homes into smart homes. This integration has blurred the boundaries of private spaces, leaving individuals uncertain about who may have access to their private activities within their homes.

Households are increasingly adopting smart devices, which promise to enhance convenience and functionality. However, the connected nature of smart devices and the sheer volume of data they collect can pose significant privacy risks for users [1, 2]. In fact, a 2015 report[12] by the USA Federal Trade Commission[13] found that a small number of households with smart home devices can "generate 150 million discrete data points a day". This data can be analyzed in ways that were previously impossible [3]. Numerous studies have explored the privacy concerns of smart home users, revealing fears over sensitive data collection [4], data sharing [5], and the potential for data misuse and repurposing [6]. However, little is currently known about how other stakeholders, such as domestic workers, visitors, tenants, and passive family members perceive privacy in the context of smart homes.

Domestic workers are an example of bystanders[1] in smart homes who experience complex power dynamics and can be subjected to privacy breaches and exploitative practices that are further facilitated through smart technology. Such power dynamics are rooted in complex social norms and customs, religious beliefs, and economics. Prior research has identified the difficulty in controlling and managing data collection of individuals living or existing as a bystanders in the smart homes [7]. One significant issue is that smart devices can be configured intentionally or incidentally to collect data or to monitor people against their explicit wishes. While prior research has focused on Western contexts (Europe and North America) to explore how smart technologies affect households and smart home bystanders, there has

[12]Report-Federal Trade Commission Report
[13]USA - Federal Trade Commission

been significantly fewer research in non-Western contexts such as Jordan, which is a Muslim Arab Middle Eastern (MAME[14]) country with a moderate Islamic background [8]. We present definitions of key terms such as smart home, smart device, privacy, and bystanders in Section §A.1. Additionally, specific details about Jordan as the context of this research are provided in Section §2.1.

### 1.1.3 Research Gap

Our literature review has identified the following research gaps:

- The need for further investigation into various aspects of privacy in the smart home context, as research in this area is still relatively new.
- Most research on privacy concerns focuses on households, with little research regarding privacy concerns of smart home bystanders.
- The scarcity of research on smart home users' privacy concerns in MAME[14] region (e.g., Jordan).
- Insufficient research on the impact of contextual factors such as social norms, customs, and religious background on privacy concerns, practices, and expectations of smart home users.
- Insufficient research of the interplay between socioeconomic power differentials and privacy concerns and how to mitigate the imbalanced power dynamics.
- There is a lack of explicit data protection regulation for smart home users in Jordan, which can result in passive users (e.g., domestic workers) being subjected to data collection by smart devices without their permission, or their awareness.

Throughout this dissertation, the following terms are used interchangeably: Firstly, *'households'* and *'families'* refer to families employing domestic workers. Secondly, *'domestic workers,'* *'workers,'* and *'bystanders'* refer to smart home

[14]Muslim Arab Middle Eastern

workers engaged in smart home device use, representing a vulnerable user group due to socioeconomic power imbalances favoring households. Thirdly, *'mobile application'* and *'app'* are used synonymously to denote the proposed technology probe in Chapter 7.

### 1.1.4 Research Questions

To address the identified research gap outlined in Section §1.1.3, this dissertation is driven by the overarching research question:

RQ: **To what extent can we understand and support the privacy needs and protection means of bystanders in the smart home in Jordan?**

To better address this research question, we broke it down into three main sub-questions:

- RQ 1. What are the privacy concerns of the households and their domestic workers (i.e., the bystanders) in the smart home in Jordan?
    i. RQ 1.1. What are the domestic workers' privacy concerns, practices, expectations, and experiences with being observed and recorded by smart home devices (e.g., smart speakers, and cameras)?
    ii. RQ 1.2. What are the households' concerns, practices, expectations, and experiences with having smart devices that observe and record the domestic workers in the smart home in Jordan?
    iii. RQ 1.3. What are the contextual influences (e.g., social norms, customs and religious background) on domestic workers' privacy concerns, practices, expectations, and perception of rights in the smart home in Jordan?
- RQ.2 How do socio-economic power dynamics affect the privacy of households and domestic workers (i.e., bystanders) in Jordanian smart homes?
    i. RQ 2.1. What are the conflicting socio-economic power dynamics in the context of the smart home in Jordan ?

ii. RQ 2.2. How do the power dynamics between households and their domestic workers (i.e., bystanders) affect domestic workers' agency, their privacy concerns with smart home devices, and the qualities of their relationship with households?

iii. RQ 2.3. How effective are the existing public privacy protection regulations in protecting privacy of households and domestic workers (i.e., bystanders) in the smart home in Jordan?

- RQ.3 How can we support privacy protection for domestic workers (i.e., bystanders) in the smart home in Jordan?

  i. RQ 3.1. How can design of smart home devices support privacy protection for domestic workers in the smart home?

  ii. RQ 3.2. What are the design challenges of privacy protection for domestic workers in the smart home?

  iii. RQ 3.3. How can we support the privacy protection of domestic workers in the smart home in Jordan?

To address the research questions, we conducted four research studies which are outlined in Chapters 4, 5, 6, 7. The first study was informed by our literature review as detailed in Chapter 2. Subsequent studies were developed iteratively, each building upon the findings of the preceding ones. Together, the collective outcomes of these four studies form a cohesive framework that enriches the theoretical foundations of the thesis. We adopted research approaches guided by grounded theory and thematic analysis. Our data collection approach consists a mix of qualitative semi-structured interviews and a participatory design (co-design) approach, utilizing qualitative focus groups. These studies investigate the impact of smart home devices on the privacy of domestic workers (bystanders) in the Jordanian context. Jordan, as a MAME country, offers a unique perspective on privacy issues. The surge in smart home devices in Jordan[10], coupled with limited data protection regulations, poses potential privacy risks. Our research specifically examines domestic workers as bystanders in

smart homes, highlighting the complex dynamics of their dual role as employees and inhabitants. Moreover, we examine smart device design challenges, and we gain design insights on privacy and protection strategies to co-design and evaluate a privacy-focused mobile application. This thesis concludes with recommendations for social, technical, and legal interventions aimed at enhancing privacy protection.

## 1.2 Research Contributions

The research reported in this dissertation is a topic that has not been extensively studied in the non-Western contexts, and specifically none in Jordan. In summary, this dissertation offers several main contributions:

1. An **exploratory interview study** of how smart home devices impact privacy concerns, practices, and expectations of domestic workers and households in Jordan, and the impact of the contextual influences on users' privacy concerns (cf. Figure 4.2, and Table 4.2 in Chapter 4).

2. An **examination study** of the socioeconomic power dynamics between households and their domestic workers in smart homes in Jordan, and how these dynamics impact the qualities of relationships between the two groups. Our second study also examines how these dynamics affect domestic workers' privacy concerns, practices with smart home devices, and their perceptions of rights (cf. Figure 5.1, and Table 5.4 in Chapter 5).

3. An **investigation analysis** of smart device design challenges with bystander privacy protection in Jordanian smart homes (cf. Figure 6.2, and Table 6.5 in Chapter 6).

4. A **technology probe study** of a privacy-focused mobile app, to explore design insights into bystander privacy, and to explore how the app as an auxiliary tool can enhance the privacy protection of domestic workers in Jordanian smart homes (cf. Table 7.2, and Table 7.3 in Chapter 7).

## 1.3 Publications

Table 1.1 outlines components of the collective research, as presented in this thesis, that have been published in peer-reviewed conference proceedings. Notably, the paper from our second study published in USENIX'32[9] has received the Distinguished Paper Award (cf. Appendix C.7).

**Table 1.1:** Existing Publications

| Title of Paper | Venue | Status | RQ | Chapter | Notes |
|---|---|---|---|---|---|
| Exploring Bystanders Privacy Concerns with Smart Homes in Jordan | CHI-2022 | Published[10] | RQ.1 | Chapter.4 | - |
| Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households | USENIX Security -2023 | Published[9] | RQ.2 | Chapter.5 | Distinguished Paper Award Winner |
| " Innovative Technologies or Invasive Technologies?" Exploring Design Challenges of Privacy Protection with Smart Home in Jordan | CSCW-2023 | Published[11] | RQ.3 | Chapter.6 | - |
| Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape | USENIX Security -2024 | Published[12] | RQ.3 | Chapter.7 | - |

## 1.4 Thesis Structure

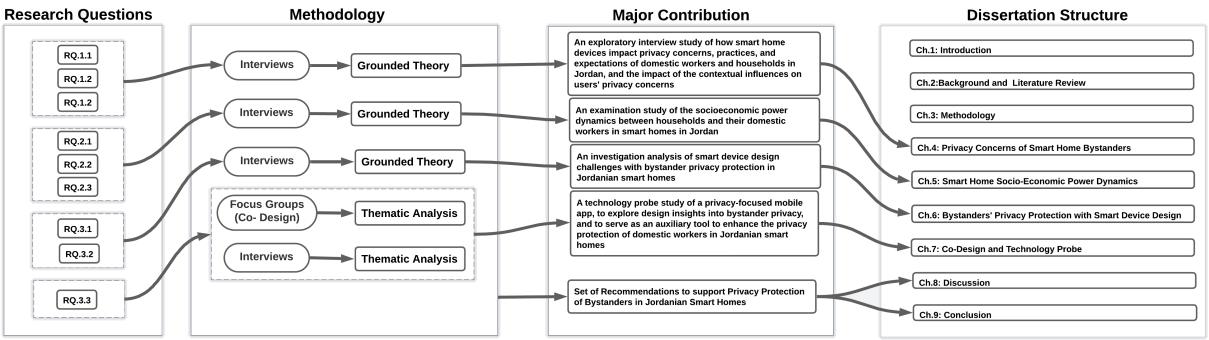
After this introductory chapter, this dissertation comprises a total of eight chapters, each covering a specific aspect of the research. Chapter 2 provides a background and literature review in three parts. The first part offers information about the research context, specifically Jordan. The second part reviews interdisciplinary literature on smart home bystanders' privacy concerns and provides information about data protection regulations globally, in MAME countries, and in Jordan. The third part provides information about privacy and security research approaches. Chapter 3 focuses on the methodology and research approaches adopted for data collection and analysis. It justifies these approaches, explaining why these methods were selected and how they were used.

Chapters 4, 5, 6, 7 present the outcomes of the research studies conducted. Chapter 4 reports on the first research study, which addresses smart home privacy concerns. Chapter 5 presents the outcomes of the second research study, which addresses smart home power dynamics and the status of data protection regulation.

Chapter 6 presents the outcomes of the third research study, which addresses smart device design challenges with data protection. Chapter 7 aims to present the outcomes of the fourth research study, which gained design insights to co-design and present a mobile application as an auxiliary tool for improving the privacy protection of domestic workers in Jordanian smart homes. Chapter 8 provides a comprehensive discussion of the research studies, offering recommendations for social, technical, and legal interventions to support privacy protection. Subsequently, Chapter 9 draws conclusions from the collective findings, emphasizing their implications for the privacy of smart home bystanders within the non-Western Muslim Arab Middle Eastern (MAME) context of Jordan. The chapter also explores the limitations of the current research, concluding with suggestions for future endeavors in this dynamic and evolving field of study.

Figure 1.1 provides an overview of this thesis structure, showing how the research questions in Section §1.1.4 and the contributions in Section §1.2 are written up as chapters, in addition to the adopted research approach and methodology. The appendices contain supplementary information and details related to this dissertation.

**Figure 1.1:** Thesis Structure



# 2
# BACKGROUND

In this chapter, we present a background and literature review in three parts. The first part offers a thorough exploration of the research context (cf. Section §2.1). The second part provides an extensive background review of smart home privacy, emphasizing smart home bystanders[1]. Our focus extends beyond Western contexts, specifically targeting non-Western regions like MAME[14]. We also provide an overview of existing data protection regulations globally, within the MAME region, and in Jordan (cf. Section §2.2). The third part provides information about research approaches adopted in privacy research studies (cf. Section §3.1). Additionally, we provide definitions of key terminology used throughout this thesis in Section §A.1.

## 2.1 The Research Context - The Hashemite Kingdom of Jordan

This research aims to explore bystanders (e.g., domestic workers) privacy concerns with the smart homes in the non-Western Muslim Arab Middle Eastern (MAME) context of The Hashemite Kingdom of Jordan (Jordan). Jordan [13] is an Arab country of southwest Asia that exists in the Middle-East region (cf. Figure 2.1) and has majority of Muslim population. Jordan is a young country that bears the traces of many civilizations, and it was part of the Islamic Ottoman Empire until

1918. Jordan was established in 1921, the capital city is Amman which is one of the region's principal commercial and transportation centers as well as one of the Arab world's major cultural capitals. Jordan has one seaport in the city of Aqaba in the southern part of the country. Jordan has a middle-eastern social norms and customs which are coloured by the moderate Islamic background of the country [8].

**Figure 2.1:** Jordan Location



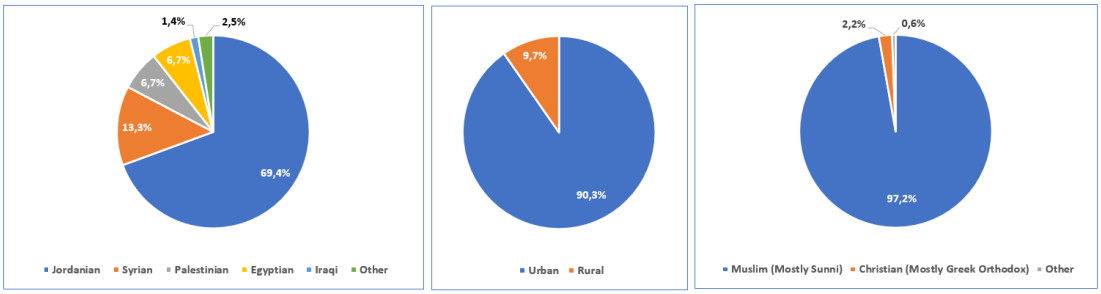

The constitution[15] declares Jordan to be a constitutional, hereditary monarchy with a parliamentary form of government. Islam is the official religion, and Jordan is declared to be part of the Arab Nation and the Islamic world. Jordan has relatively small area of 89,342 km2 (Slightly smaller in area than the country of Portugal). Jordan landscape falls into two regions; the desert zone and the cultivated zone, each of which is associated with its own mode of living. The tent-dwelling nomads (Bedouin), who make up less than one-tenth of the population, generally inhabit the desert. There are some semi nomads, in whom the modes of life of the desert and the cultivated zones merge. These people adopt a nomadic existence during part of the year but return to their lands and homes in time to practice agriculture. The Rural residents, including small numbers of Bedouin, constitute about 20% of the population.

[15]Jordan-Constitution of Jordan

### 2.1.1 Social Structure in Jordan

Jordan population [14] is around 10 million, and the population structure is predominantly young [15]; people under age 15 constitute more than 39% of the population. The birth rate is high, and the country's population growth rate is about double the world average. The average life expectancy is about 75 years. Internal migration from rural to urban centres has added a burden to the economy; however, a large number of Jordanians live and work abroad. There are many ethnic groups in Jordan who have immigrated and settled in the country from the surrounding countries (i.e. Palestine, Iraq, Syria, Egypt). However, these different ethnic groups share almost the same cultural and religious background. The below diagram demonstrates the distribution of the ethnic groups, and the Urban-Rural residents in Jordan (cf. Figure 2.2).

**Figure 2.2:** Jordan Religious Groups, Ethnic Groups, and Urban/Rural Distributions




The overwhelming majority of Jordanians are Arabs [16], principally Jordanians and Jordanians from Palestinian origin; there is also a significant minority of Bedouins [17], who were by far the largest indigenous group before the influx of Palestinians following the Arab-Israeli wars [18] of 1948–49 and 1967. Jordan is the only Arab country to grant wide-scale citizenship to Palestinian refugees. One-fourth to one-half of Jordan's population are Palestinians. The influx of Palestinian refugees not only altered Jordan's demographic map but has also affected its political, social, and economic life.

During the Iraqi War (1990–91), some 300,000 additional Palestinians fled from Kuwait to Jordan. Additionally, as many as 1.7 million Iraqis flooded into Jordan

during the Iraqi war in 1990 and the years that followed. Another smaller wave of Iraqi refugees arrived in 2003 after the restart of the Iraq War. Most of these Iraqis left, but perhaps 750,000 remain[16]. Other minorities include a sizeable number of Syrian refugees (around 670,000 ) [19] who fled to Jordan after the Syrian Civil War in 2011. There are also smaller Circassian [20] (known locally as Cherkess or Jarkas), Kurds, and Armenian communities. A small number of Turkmen who speak either an ancient form of the Turkmen language or the Azeri language also reside in Jordan. Nearly all the people speak Arabic language, the country's official language. The entire population is Sunni Muslim [13], with Christians constitute most of the rest. Other minorities include the Druze[17], and the Bahaii[18] which are both religious and ethnic communities and considered to be an offshoot of the Shii sect, the Circassians are another minority non-Arab Sunni Muslim group who are descendants of 19th-century immigrants from the Caucasus Mountains. With these multiple waves of refuges to Jordan from its neighbouring Muslim Arab countries (e.g., Palestine, Syria, Iraq), Jordan is colored with the cultural, social custom, and religious background of MAME region countries, thus we believe that outcomes and findings of this research are applicable to other MAME countries. However, this needs to be verified in confirmatory research studies in other MAME contexts.

K.Gharaybeh [21] discussed that Jordan's population is diversified, as Jordan was path for many Arab immigrations, and Islamic wars. Many groups of people who passed though Jordan settled in it. In general, Jordanian society, belonged to the Arab Nation and the Islamic World in terms of the religious background, history, and culture. The Jordanian society is distinguished by some characteristics: a) Strong relations among family members [22], b) High respect to Jordanian traditions, c) Empowerment of women in the Jordanian society by education, work opportunities, regulations and legislation, despite the fact that the Jordanian society is still masculine society, d) Decline in the growth of extended families in the Jordanian society [21], e) Reduced size of families, [21], f) Dominance of tribe

[16]Report-Iraqi Refugees in Jordan: Desperate and Alone
[17]Druze-Who are druze
[18]Bahaii-Who are bahaii

characteristics in the Jordanian society specially in two environments; Bedouin, and villages, g) Social solidarity [21], and h) Promoting good social behaviours such as: generosity, helping others and charity.

The Jordanian society can also be divided into [23]: a) The Family: which shapes the community basic unity and they are consisting of many brothers or cousins from the first degree, it may contain many families to discuss about matters related to land, heritage, and marriage. b) Relatives: Usually men within the same family, c) Tribes: which is the largest social group and has large role in society control beside its important role in the field of local policies. In the following sections, we explore the roles of family and women in Jordanian culture, and we delve into the tribal structure of Jordanian society.

#### 2.1.1.1 Families and Households in Jordan

Family is the domestic Unit in any society. An examination of the literature in different fields shows that some researchers have used 'household' to refer to people living "under one roof" [24], however, most use it without any specification and as a synonym of 'family' [25–27]. A household in Jordan usually consists of a married couple and their unmarried children. Each household is usually headed by a male, while the role and position of each individual in this type of structure are defined according to sex and age [28]. Some features of households in Jordan, such as size and economic characteristics, have changed over time, for various reasons. The typical family is extended, with family size decreasing since 1979 to about six members per family [29]. Kinship relationships are patriarchal, and the extended family ties govern social relationships and tribal organization.

#### 2.1.1.2 Tribal Structure in Jordan

A Jordanian tribe is a collection of families who share the same surname and for which there is a leader or head of the tribe. The tribal system retains a fundamental influence on Jordan life and practices, whereby a person's tribe is seen as a source of support and security. The tribal structure of Jordan is affecting and influencing both the economic and social dynamics of populations. K.Gharaybeh [21] discussed

that the population of Jordan are interconnected social units, despite the great diversity of their assets, demographic, sociological, and their natural environments. Alon et al. [30] discussed that the tribe was the main solidarity group in Jordan on the eve of the establishment of the modern state in 1921. As in many tribal societies in the Middle East, the creation of the state system in the aftermath of World War I brought about dramatic changes in the lives of tribes-people, and nomads in particular. The emergence of colonial governments with centralizing ambitions; the creation of international borders; rapid economic changes; and the spread of national ideologies were among the factors that threatened the survival of old tribal order and indeed put enormous pressures on tribes-people everywhere. Nevertheless, in the case of Jordan, twenty-five years after the process of state-formation and modernization had been launched, tribal identities had not disappeared. Rather, tribes remained important social and cultural categories, having adapted to new realities and transformed in the face of them.

Another study [31] discussed that tribes, clans, and extended families affect — positively and negatively — the social systems of the countries and regions of which they are a part. Watkins et al. [32] discussed that in Jordan, tribal dispute settlements have played a pivotal role in the management of various types of grievances between individuals since long before the establishment of the modern state. To varying degrees, Jordanians—from the East and West Banks, Muslim and Christian, urban and rural—cherish the kinship networks associated with these procedures, and the truce and reconciliation processes remain time-honoured mechanisms for preventing revenge and making amends for wrongs committed. Another study [32] highlighted how tribes are influencing and shaping general culture of the community. Antoun et al.[33] discussed that the scholarly and governmental conceptions of tribes and tribalism in the Middle East have discounted important action arenas of civil society by construing tribes and tribalism as a congeries of values and norms associated with hospitality, honor[19], independence, and loyalty to

[19]In MAME contexts, honor is linked with chaste female behavior. Women lose their honor when they conduct sexual affairs outside marriage, and this also affects the wider honor of their family and tribe.

the tribe. Tribal relations also have a great influence on Jordan life and practices. Islamic principles and traditions are closely intertwined with a historical tribal culture, resulting in the modern structure of Jordan.

#### 2.1.1.3 Women in Jordan

It is worth mentioning that neither the Holy Qur'an[20] nor the Hadith[21] forbids women from joining in public life in Jordan. However, the Qur'an does warn that the mixing of the sexes could lead to "seduction and the 'evil consequences' that might follow"[34]. The UN-Women gender discrimination report in Jordan [35] discuss that despite the fact that the constitution of Jordan states that *"Jordanians shall be equal before the law with no discrimination between them in rights and duties even if they differ in race, language or religion"*, the constitution fails to prohibit gender discrimination, and the report says that men and women in Jordan are not treated equally. Most Muslim women cover their heads with scarves (Hijab[22]). A small minority cover their heads and faces with a veil[23]. Segregation of the gender occurs in some public situations, and there is limited interaction between men and women. Most women have their lives controlled by their closest male relatives. Despite the limitations placed on them, they have made advances in education in a country where the practice of educating women only began three or four decades ago. Balancing customs and traditions at home with obedience to their husbands and the demands of a career remains a difficult challenge. When women work, they receive extensive benefits and sometimes equal pay. The UNDP[24] report [36] stated that the current proportion of women in the workforce is 14.4%, compared to 8% in 1979. However, the unemployment rate for women is 65%.

[20] Qur'an-Islamic Qur'an
[21] A collection of Prophet Mohammed's sayings
[22] A head cover garment worn by Muslim women to cover their hair.
[23] Piece of fabric used to cover face
[24] UNDP-United Nations Development Programme

### 2.1.2 Culture and Values in Jordan

Several studies [37, 38] discuss that the culture of Jordan is based on Arabic and Islamic elements, For Jordanians, Traditions [21], Habits, and Social Values are resembled in keeping their honor, and gaining the respect of society they live in. Traditions were taken in heritage from one generation to another. Habits[25] in Jordan well-known as group of deeds, behaviors, patterns which are practiced by the group in some occasions and social situations. Examples of some Jordanian habits include: dressing style, feeding, weddings, sad occasions, selling and purchasing, entertainments parties and others. Social values in Jordan reflects the country's Muslim and Arab roots. The dominant values in Jordanian society differ according to their source and we can classify them in the Jordanian society that they are values extended from[21]: 1- Religion: which are classified as basic high rank values such as: believe in God, veracity, benediction, equity, contentment and others. 2- Family: modesty, and make the women far away from any deeds may offense to her honor. 3- Social class: shame, competition and take in authority. 4- Living style: manhood, magnanimity, and consumer guidance. 5- Political system and orientations: patriotism and citizenship. Many of Jordan's laws are based on the Qur'an and the Hadith. These laws are enforced in religious courts called Sharia courts, which have jurisdiction over personal matters. Chastity is demanded of all single women.

Mahadeen [39] highlighted that Jordan is a patriarchal society within which men monopolised power, resources, and decision-making, and women were deprived, marginalised, and castigated if they dissented. The researcher added, Jordan is conservative, Arab and Muslim-majority country with a rich history and a dynamic social country as a result of changing economic conditions, waves of refugees, ever-evolving internal and external political dynamics, advanced information and communication technologies, and an overwhelmingly young and educated population. Another study[40] discussed that in Jordan, the household is likely to be headed by a man. By law and customs, men are responsible for women , and Islamic law

[25]Habits are the behavioral line continued for a long time even it became fixed and stable

states that it is a man's responsibility to provide financially for the household and specifically for his wife, whose participation in funding household expenditure is optional. Men are responsible for solving any difficulties that may arise and they are responsible for family members' behaviour. It is therefore crucial to monitor the behaviour of family members to maintain family honour, whose significance is clear from the idea that a family which loses its honour loses everything [41]. This notion of family honour is strongly associated with the chastity of female members [41, 42], that is, any improper behaviour by a woman may "raise suspicion or provoke an attack on her morality, the consequences of which the entire family would suffer" [43]. This, in turn, has resulted in the need to prevent the disclosure of female identities, voices and photos [43]. People consider it an invasion of privacy if anyone takes pictures of women in public spaces [44], and that he is requested to ask for permission before photographing women in any context, even in public areas, and if that person is in or near a family house or tent, he should ask permission of the men too. Some people don't mind, others do.

### 2.1.3 Islam Impact on Society

Jordan's constitution (Article-2)[15] states that Islam is the religion of the country, and Arabic is its official language. According to PEW Research Center Report [45], 97.2% of the population adheres to the Sunni branch, and about 2.2% of the people are Christian. Many of the Jordan's laws [46] are based on the Qur'an and the Hadith. These laws are enforced in religious courts called Sharia courts, which have jurisdiction over personal matters. Badeau et al.[47] has discussed that Islam is the constituent of the social structure in the Middle East, and that attitudes toward authority, the customs of family life and the relations of individuals to their fellows are still set by the classic Muslim. Abukhodair et al. [48] has explored the meaning of "privacy" among citizens of the Gulf states of Qatar and Saudi Arabia as it manifests in digital environments, and found that privacy is an essential and widely respected value in many cultures, and the way in which it is understood and enacted depends on context. Their findings reveal that the need and pursuit of privacy

stems from the Islamic faith, in addition to the use of paternalistic language by men when discussing women's privacy. Above all, privacy is framed as a communal attribute, including not only the individual, but the behavior of those around them; it even extends beyond one's lifespan. The results of their study expand and enrich the Western-centric privacy notion inscribed in system design by providing the perspective of privacy as practiced in the everyday life in the Gulf region. They contribute the following observations specific to the Qatari and the Saudi society: (1) The notion and expression of privacy is highly gendered, such that the specific requirements for privacy differ greatly between males and females due to the socially constructed role of each gender within the society. (2) Privacy includes what people are exposed to, not only what they are themselves exposing. That is, in one's environment, the behavior of others around them—reflects on one's own honor, making privacy a highly communal concept that is shaped by the collective. (3) An individual's privacy should be preserved and accounted for even after death, in accordance with the Muslim belief in the afterlife. (4) Privacy is a moral value highly influenced by religion. It is defined in religious texts and by the cultural norms that have been largely shaped by the interpretation of the Islamic faith in MENA[9] region.

### 2.1.4 Economy and Work Force in Jordan

The majority of the workforce in Jordan is men. The UNDP Human Development Report 2020[26] shows that the labour force participation rate for population aged more than 15 years is 14.4% for females, and 63.7% for males of the total work force. The government employs nearly half of those [13], and about 15% of the population is unemployed. Although Jordan's economy is relatively small and faces numerous obstacles, it is comparatively well diversified. Trade and finance combined account for nearly one-third of Jordan's gross domestic product (GDP); transportation and communication, public utilities, and construction represent one-fifth of total GDP, and mining and manufacturing constitute nearly that proportion. Remittances from Jordanians working abroad are a major source of foreign exchange.

[26]UNDP-Human Development Report 2020

However, although Jordan's economy is ostensibly based on private enterprise, services—particularly government spending—account for about one-fourth of GDP and employ roughly one-third of the workforce. In addition, Jordan has increasingly been plagued by recession, debt, and unemployment since the mid-1990s, and the small size of the Jordanian market, fluctuations in agricultural production, a lack of capital, and the presence of large numbers of refugees have made it necessary for Jordan to continue to seek foreign aid. The Jordan Small Businesses and Human Development report[27] shows that one of the factors that distort job creation is the employment of non-Jordanians. The foreign labor force in Jordan, which stands at 260 thousand or 24.3% relative to a total of 1,172,701 is evidently large. However, only 1.9% of these foreign workers are university graduates, which implies that the majority of foreign workers are employed in low skill jobs. Almost half of business owners stated that they employed foreigners due to a lack of available Jordanian labor that is willing to perform certain tasks.

#### 2.1.4.1 Domestic Workers in Jordan

According to the International Labor Organization[28] database of national labour, social security and related human rights legislation, and the Jordanian Regulation NO 90/2009 of domestic workers [49], domestic workers are those who perform works for the household members cleaning, cooking, ironing, preparing food, providing care for family members, purchasing household necessities and transporting children. According to this definition, any worker performing tasks within a household for the benefit of the household or its members is considered a domestic worker. This includes occupations such as nannies, babysitters, home nurses, home maintenance workers, gardeners, and similar roles. Additionally, in accordance with the same regulations [49], both households and domestic workers are obligated to respect and protect each other's security and privacy, and must refrain from breaching the privacy and security of either party.

[27]The Jordan -Small Businesses and Human Development report
[28]ILO-International Labour Organization

According to a 2019 report published by Tamkeen [50, 51] a legal organization combating human trafficking in the kingdom, the number of migrant domestic workers in Jordan is estimated at 70,000, with only 54,000 legally registered as domestic workers. Unregistered workers are susceptible to being arrested and jailed because of their illegal status. Most of Jordan's stay-in migrant domestic workers come from the Philippines, Ethiopia, Ghana, Indonesia, and Bangladesh. According to the International Labor Organization, and the Jordan regulatory framework governing migrant workers [52], The minimum wage is 260 Jordanian dinars (JOD) (US$367) for nationals and 245 JOD (US$346) for migrant workers, except for domestic workers, the minimum wage is 125 JOD (US$176) plus providing food and accommodation. Foreign domestic workers enter the country under the sponsorship of the family (usually one of the parents), which gives the employer (the household) the right to control the worker's legal residency status. Under the household sponsorship, some domestic workers are required to stay at the family's homes for most of the contract period, and families often seize the workers' passports. Domestic workers cannot resign from their positions, transfer employment, or leave the country without obtaining written permission from their employers. The report mentioned that hundreds of the domestic workers run away and seek help from human rights organizations, and when the domestic worker runs away, the employer can go to the police station to report the missing worker. The report [50] mentioned also that Tamkeen [51] has received 328 complaints in 2019 of domestic workers working in different cities in the kingdom. These complaints included the confiscation of passports, full or partial pay-cuts, and the denial of vacation days.

Despite the fact that domestic workers need the job and suffer limited rights in their employers' homes, a study by International Labor Organization [53] found that families' (employers') behaviours towards domestic workers include: fear of material losses such as running away or theft, dehumanization of the workers, empathy, pity, and a desire to motivate good work performance. Fear of material losses was commonly used as a justification for restrictions on the domestic worker's freedom and, in some cases, violations of their rights. The study [53] showed

that employers are keen to control the power dynamics in their relationship with the domestic workers to ensure that they retain a significant power advantage. This is evident from the discourse about not wanting the domestic worker to become strong-willed, the preference of some employers for inexperienced domestic workers, and the reasons given by employers for restricting the communication and mobility of the domestic workers.

## 2.2 Literature Review

At the beginning of this research, we undertook a systematic review of over 300 academic publications that specifically address topics such as usable privacy, smart homes, bystanders, socioeconomic power dynamics in the smart home, and data protection. Initially, we conducted a search on various platforms including ACM digital library and Google Scholar, which yielded more than 800 articles. Subsequently, we performed several sifts by excluding articles with low citation counts (with the exception of newly published papers) and by reviewing titles and abstracts. These sifts helped us reduce the number of articles to 380. Finally, we conducted a last sift to filter in articles that primarily discuss privacy in the smart home, which brought the total number of relevant articles down to 235. Additionally, given that our study is based in Jordan, we reviewed the privacy regulations and policies in the country, as well as Islamic statutes, as the majority of the population is Muslim and local social norms and practices are influenced by religious beliefs. The inclusion of these additional sources brought the total number of reviewed papers and documents to over 300. As the research studies progress, we were adding more papers to our reference list, which makes the total number of referenced papers more than 500, as we can see from the References.

### 2.2.1 Privacy

Privacy is considered a fundamental human right that has driven security and privacy researchers to develop techniques to protect it. Privacy is a broad term with various connotations rooted in larger cultural practices, legal frameworks,

ethical considerations, and social theories. According to the Oxford English dictionary, privacy is the state of being alone and not watched or interrupted by other people [54]. The proliferation of smart-home technologies, such as surveillance cameras and other smart devices has become expected common practice in many environments [10]. This kind of new practice is creating a complex set of privacy challenges for the workers in these contexts. Additionally, it is affecting the inter-personal relationship between domestic workers (i.e., bystanders) and their employers (i.e., the households).

The origins of the concept of privacy are arguably ancient, however privacy has become a much more important issue in light of recent technological developments and data-driven industry. Whereas privacy originates from the mindset of protecting one's body, and home [55], the history of privacy shows a strong relationship with technology evolution. The more modern preoccupation with privacy started in the late 19th century with the use of cameras and continued with the developments that led to information revolution, the advent of computers, the internet, and smart devices. Over time, and in light of the technological developments, the concept has evolved to protect one's information and intangible assets. In 1880 Godkin defined privacy as *"the right of every person to keep their affairs private and determine to what extent they should be open to public observation and discussion [56], [57]"*. In 1891, Warren and Brandeis [58] [56] published their seminal work 'The Right to Privacy', where they argued about protecting oneself form other people's interference. Posner defined privacy as the ability to keep secrets and prevent others from using information to one's disadvantage [56, 59]]. Others see that privacy is the control of personal data, whereby individuals, groups, or institutions claim the right to determine when, how, and to what extent information about them is disclosed to others [54, 56]]. Moreover, Rouse [[60]] defined privacy in the context of information technology (IT) as the capability of an organization or individual to determine what data in a computer system can be shared with other third parties.

Furthermore, privacy can be viewed in different states; for example In 1967, Westin [54, 61]] published 'Privacy and Freedom' where he defined privacy in

terms of self-determination adding that privacy consists of four states: reserve, intimacy, anonymity, and solitude, and Altman [62] argued that privacy is a dialectic process where users make selective choices. In the theory of Contextual Integrity (CI), Nissenbaum [63] linked privacy to contextual social and cultural elements. Solove [56] suggested to protect information collection, and Waldman [64] discussed protecting individuals from legal perspectives. Additionally Kattina et al[65] see that privacy encompasses various factors such as data collection and distribution, technology, user expectations, and regulatory concerns. Moreover, privacy is also referred to as data privacy [66], or data protection [67].

#### 2.2.1.1 Privacy Theories

The landscape of privacy theories in smart home research encompasses a spectrum of conceptual frameworks aimed at comprehensively understanding and addressing privacy concerns within connected environments. One fundamental conceptualization is rooted in informational self-determination, which posits privacy as the ability of individuals to exert control over their personal information [54, 62]. This theory underscores the critical role of privacy-enhancing technologies that empower users to manage how their data is collected, utilized, and portrayed, thereby fostering a sense of autonomy and control over their informational selves. Complementing this view, contextual integrity (CI) theory delves deeper into the regulation of information transmission within specific contexts to preserve the contextual norms governing data sharing [68]. The CI framework emphasizes the importance of aligning technological interventions with users' contextual expectations and established privacy norms.

Empirical studies have provided valuable insights into the multifaceted nature of privacy perceptions and behaviors, revealing the nuanced interplay between social contexts, relationships, disclosure purposes, and individual privacy preferences [69–72]. These studies demonstrate that violations of context-specific norms can elicit negative emotional responses such as feelings of betrayal and loss of control, underscoring the psychological ramifications of privacy breaches [73, 74]. Moreover, the observed disparities between individuals' stated privacy preferences

and their actual behaviors underscore the complexity and variability of privacy decision-making processes [75–77]. Effectively understanding and addressing these discrepancies necessitates considering the diverse array of real-world pressures, incentives, and contextual factors that shape individuals' privacy choices.

In response to the challenges posed by these complex privacy dynamics, there has been a growing emphasis on accountability-driven design approaches within the scholarly discourse [78, 79]. Proponents of accountability-driven design argue for systems that empower users to hold technology manufacturers and service providers accountable for their data practices, thereby promoting transparency and trust [80–82]. Additionally, initiatives such as privacy labels and fact sheets have been proposed as practical tools to enhance transparency by providing users with clear information about data collection, retention, and disclosure practices [83]. However, these approaches face inherent limitations, including the need for ongoing refinement to capture dynamic data usage scenarios and to bridge the gap between users' privacy preferences and their actual behaviors in real-world contexts [84].

#### 2.2.1.2 Privacy Concept

Privacy concepts are dependent on moral and normative reasoning. With ongoing debate between scholars about whether privacy is a right or a state. Nissenbaum [63] and DeCew [85] have discussed the issue from a philosophical point of view. If privacy is a right, then its practice is tied to moral values and thus aligns with normative approaches. If it is viewed as a state, then instead it aligns better with descriptive approaches. Ohara [86] discussed descriptive privacy using seven-layer approach 'The Seven Veils of Privacy'. Regan [87] discussed privacy values as (1) common (e.g. right of belief), (2) public (e.g. right for voting), and (3) collective (e.g. rights within regulated space). Some thinkers argued that in the context of socio-technical system, some practices motivate discussions of information and access control, and empowering the users [63, 77, 85]. From another point of view, privacy is a common good, and unattainable. For example, a person cannot avoid being pictured randomly in public areas [63, 85]. Furthermore, privacy laws and regulations in the

USA are typically based on the principle of preventing harmful interventions [56], whereas in the EU, there is a stronger emphasis on consumer protection [85]. The introduction of the EU General Data Protection Regulation (GDPR[29]) [88] is a noteworthy event that has significantly changed the international data landscape.

#### 2.2.1.3 Privacy Design

Yao et al. [89] have argued that the socio-economic power dynamics in the smart home can complicate privacy aspects, and they found that the design of smart devices tends to protect households, with little protection designed to protect bystanders' privacy. Privacy has been addressed from two perspectives: a) focusing on the home, the norms, the practices and values of residents, and b) focusing on the smart devices' technical capabilities, design characteristics, and data management processes. From the home perspective, Apthorpe et al. [90], for example, studied privacy design in smart homes to support smart devices that make users feel more secure in their homes. From the technical perspective, Lau et al. [91] studied bystanders' concerns arising from owners' actions, and recommended new features to improve privacy protection such as guest mode or voice command mute option. Yao et al. [89] studied how to incorporate both device owner and bystander concerns in the design process. Researchers also highlighted the importance of responsible innovation[30] in the wider design of privacy protection [92, 93] to anticipate and mitigate negative impacts on society arising from technology use.

Manheim et al. [94] argued that smart device manufacturers must implement reasonable security features to prevent unauthorized access, information disclosure, or modification, and argued that companies can use AI[31] to create user profiles, monitor user behaviors, and for other purposes. Another study [95] argued that differential privacy has several attractive properties that makes it quite valuable for AI, and presented differential privacy mechanisms. Van der Vlist et al. [96] investigated using design semantics to enable users to understand and construct

[29]GDPR-EU-General Data Protection Regulation
[30]RI-Responsible Innovation
[31]AI-Artificial Intelligence

meaningful mental models of smart home devices and how to interact with them, and Resnick et al. [97] indicated that semiotic[32] design features have a strong effect on user expectation. Building on the importance of semiotics, Nadin [98] argued that without the underlying semiotics, design remains a mere problem-solving activity, as semiotics contributes to the language shared between users and smart devices. Chagas et al. [99] took Semiotic Engineering as a theoretical lens to understand the appropriation of smart devices in smart homes, and proposed a semiotic account of appropriation support.

**2.2.1.3.1 Privacy by Design.** The EU-GDPR aims to provide users with control and transparency over the use of their personal data [100]. In 2018, the UK implemented GDPR through the Data Protection Act [100]. GDPR legally requires companies to take technical and organizational measures to integrate data protection into the design process, known as "data protection by design and by default" (DpbD) [101] or "privacy by design" (PbD[33])[[67]]. DpbD ensures that companies comply with GDPR's principles and requirements and are accountable for any breaches. Similar to DpbD, PbD [102] requires that privacy must be considered throughout the engineering process. The concept of Privacy by Design is based on seven key principles [102–104], which include: 1. "Proactive not reactive", 2. "Privacy as the default", 3. "Privacy embedded into design", 4. "Full functionality", 5. "End-to-end security", 6. "Visibility and transparency", and 7. "Respect for user privacy". These principles have been widely recognized and referenced numerous times [104].

**2.2.1.3.2 Privacy Protection by Co-Design.** Several studies [105–111] have discussed using co-design to explore approaches to gain design insights for privacy protection. Co-design, also known as participatory design, is an approach that involves designers and end-users working together throughout the design process. Co-design of mobile apps has gained significant attention in recent years as an effective way to create user-centered and relevant apps as discussed in several studies[112,

[32]Semiotics-The study of signs, symbols, and their meaning
[33]PbD: Privacy by design through the lens of HCI

113]. Co-designing mobile applications that support privacy protection in the context of smart home devices is an approach that can help address these concerns. A study by Yang et al [89] investigated the use of co-design to develop a mobile application that enabled users to control their smart home devices while protecting their privacy. The co-design process [89] involved users, designers, and privacy experts, which resulted in the development of an app that incorporated privacy features such as user authentication and encryption. Users who participated in the co-design process reported feeling more confident in their ability to control their smart home devices and protect their privacy. In another study, Yao et al. [1] found that bystanders had an interest in knowing the behaviors of smart home devices in order to be informed and suggested a mobile application that would provide transparency and information about all IoT devices in a home, including who is using them, when they are running, and for what purpose, in order to help everyone around the device understand its usage. The study [1] also discussed utilizing a mobile application to receive notifications about surrounding smart devices and/or to control collected data. Another study[114] discussed the use of mobile apps to control online access to smart toys, and Van Kleek et al. [115] addressed smartphone app users' unawareness of data collection practices, discovering that transparent disclosure of apps' data collection and sharing behaviors proved beneficial. Their emphasis was on promoting informed decision-making and fostering trust in app usage. While their study [115] focuses on app users, we believe that utilizing apps to disclose privacy-related information about nearby smart devices in smart homes, especially to bystanders, would also be beneficial for their privacy protection.

In summary, these research studies showcase the efficacy of co-design in developing mobile applications that aid in protecting privacy in the realm of smart home devices. The participation of users in the design phase aids in pinpointing privacy issues and guarantees that the application satisfies the users' requirements while also protecting their privacy. Additionally, the studies emphasize the significance of engaging privacy experts in the co-design process to guarantee the integration of privacy protection best practices in the smart home device context.

#### 2.2.1.4 Privacy Protection Means

Various solutions have been proposed by researchers to mitigate privacy concerns and risks in smart homes. For instance, Apthorpe et al.[116] proposed a solution that decreases the inference of sensitive user activities by introducing a minimum amount of noise data into the smart home network traffic. Datta et al.[117] developed a Python library that enables IoT developers to easily implement privacy-preserving traffic shaping. Yoshigoe et al.[118] introduced a solution that obscures the real network traffic and reduces potential privacy vulnerabilities by injecting synthetic network packets. Wang et al.[119] developed a live video analytic tool that denatures video streams by blurring faces according to user-defined rules. To reduce improper access to users' data, Moncrieff et al.[120] developed a tool that dynamically manages access privileges based on contextual factors in smart home surveillance, such as occupants' location and the content of ongoing conversation. Arabo et al.[121] proposed a framework that ensures data security for smart home devices by providing dynamically generated policies and interfaces in which end-users can set up their privacy zones. Chakravorty et al.[122] designed a system that collects and stores users' data and only allows users to access their data upon successful re-identification. To increase transparency and user control, Das et al.[123] proposed an infrastructure that enables IoT devices and sensors to send personalized privacy notices and choices based on individual users' preferences. McReynolds et al.[114] suggested in their study on smart toys that toys should effectively communicate with both parents and children that toys could record. More broadly, to ensure an overall safe environment of smart homes, Lin et al.[124] suggested that auto-configuration support should be developed for the smart home network so that whenever a new device is plugged into the network, the supporting system could auto-configure itself and find the most secure settings for the new devices, such as security protocols and essential firmware updates.

#### 2.2.1.5 Privacy Controls

Prior research emphasizes the need to contextualize privacy preferences in users' daily lives, considering social dynamics [125, 126]. Users articulate specific privacy preferences when notifications are presented comprehensibly [127, 128]. Previous work suggested privacy labels detailing data types for devices[83]. The focus remains on accountability measures and tools for informed decision-making rather than direct control mechanisms [83, 84, 127, 128]. Seymour et al[129] developed a privacy assistant technology probe, featuring a network disaggregator, personal tutor, and firewall, empowering users in smart homes to understand and control privacy. While facing challenges, the study highlights the potential for users to navigate the smart home landscape with informed attitudes and strategies when supported by the right tools.

Service providers aim to offer privacy controls, yet "dark patterns"—deceptive design techniques—frequently lead users to unintended choices [130, 131]. While some patterns violate data protection laws, the EU-GDPR emphasizes specific, informed, and unambiguous consent [132, 133]. Usability challenges, including awareness, findability, comprehension, and trust, result in users defaulting to permissive settings [134–136]. Efforts to enhance usability involve exploring novel interfaces, privacy assistants, and machine learning tools [137–141]. Other studies argue for balancing users' privacy needs with business viability [142–144]. While mobile applications show promise for enhancing privacy by suggesting their use for providing privacy notices [145], their adoption in Jordan is influenced by factors like education, app quality, age, gender, and income [146, 147]. A prior study highlights the positive impact of mobile applications in the Jordanian context [148], yet their potential in smart home contexts, particularly for bystanders, remains under-explored, emphasizing the need for research sensitive to diverse usage contexts.

### 2.2.2 Human-Computer Interaction and Privacy

#### 2.2.2.1 Background

The emergence of the World Wide Web (WWW) prompted regulatory changes to accommodate the increased collection of personal information online [149]. This led to research in privacy, which explored how computing can be used for communication and how user data can be adapted. HCI research began to shift its focus towards the potential of IT to support social and work-groups in society [149]. Researchers then paid attention to interpersonal privacy in everyday communications such as email and internet messaging [150, 151]. The development of sensors, wireless networking, and computer devices has given rise to ubiquitous applications such as smart homes and smartwatches that operate in non-traditional environments, creating novel challenges in privacy for HCI [152, 153]. This has led researchers to revisit established principles of privacy, such as Donald Norman's "seven stages of actions" [154]. Today, HCI provides a variety of tools to evaluate how users respond to privacy threats and vulnerabilities, how people share personal information with others, and how well a given system facilitates or inhibits desired privacy practices [149].

Our research, which seeks to explore the privacy concerns of bystanders—specifically domestic workers in Jordan's smart home context, squarely aligns with the overarching goals of HCI. Carroll et al. [155] posits that HCI aims to decipher users' actions, motivations, and experiences to effectively guide the development of user-friendly computing technology. The knowledge base generated in this process becomes instrumental for system designers. Dourish et al. [156] assert two crucial requirements for a comprehensive account of computer users' practices. Firstly, a deep understanding of these practices within their social and cultural milieu is imperative. Secondly, these practices must be associated with essential concepts such as risk, danger, trust, secrecy, identity, morality, and power to confer them with meaningful significance. The study's linkage of users' practices to these crucial concepts is underscored by real-world instances of privacy breaches within smart homes, resulting in both moral and physical repercussions. These cases illustrate the tangible impact of neglecting privacy concerns within the HCI discipline and

reinforce the critical importance of addressing such issues in the development of smart home technology. The interaction between a user and smart devices would occur within a specific context that can influence the practices and the motivation of the user. Dix et al.[157] argue that this wider context may involve factors which the designers of smart systems cannot control; nonetheless, it is important to be aware of such factors in order to fully understand the problem domain and the users within it.

#### 2.2.2.2 Usability and Privacy

Users often prioritize task performance over concerns about privacy and security in smart systems [158, 159]. Therefore, designers of smart systems need to prioritize user concerns and place them at the core of usability [160]. It is essential to align usability with privacy considerations [161, 162]. On the contrary, Bishop [163] dispels the misconception that a secure system must be complex and difficult to use, emphasizing the importance of prioritizing ease of use for enhanced system usability. Striking a balance between privacy, security, and usability is crucial, prompting designers to implement appropriate security measures with privacy protection in mind. In the realm of user studies, researchers have traditionally viewed users as either experts [163] or employees within specific contexts [164–168]. Inglesant et al. [168] argue that considering smart home users is crucial, as evidenced in specific cases [169, 170]. Schneier [171] asserts that usability is a fundamental factor in addressing security and privacy concerns, as contextual elements influence users' concerns and practices.

We have identified four key research streams in privacy and usability within human-computer interaction (HCI) as outlined by Ackerman [172]: (1) The design and evaluation of system usability, encompassing areas such as usability engineering. (2) The investigation of user-system interactions, including fields like computer-supported cooperative work. (3) The exploration of users' diverse capabilities and preferences in human-computer interaction (HCI) interfaces. (4) The examination of the role of usability in smart technologies, such as ubiquitous and pervasive computing.

While most of the existing research has focused on the intersection of usability and security, there has also been some attention given to the intersection of usability and privacy [173]. One prominent research tool that has been developed is Privacy Bird, which is a usable privacy tool designed to inform online users of the practices of websites [163]. Usable privacy tools typically adhere to four fundamental principles that are essential to their effectiveness [160], which we summarize in: (1) Privacy is not the main task of users. Making privacy a distinct task for users can create usability issues. Privacy tasks should be lightweight or invisible [163]. (2) Privacy should work for all users. As users vary in many aspects, including technical capabilities, disabilities, and skills, privacy design should address these individual differences. (3) Privacy increases the level of risk and reward. If privacy is not designed properly, it can create adoption issues and threaten the privacy of both users and the organization, thereby increasing reputation risk. (4) Privacy must abide by regulations. Privacy laws can be complex, and different jurisdictions have different laws. Meeting regulatory requirements increases the costs and challenges of privacy design, and requires expertise in privacy law.

#### 2.2.2.3 Human Values and Privacy

Research has shown that human values and beliefs can also influence users' practices in addition to usability, emphasizing the need to explore these factors. Prior study [169] discussed that maintaining trust and accountability are crucial for the common good of information infrastructure, as users may be hesitant to utilize it for their daily activities. Trust, in particular, is highlighted as a significant human value for the effectiveness of smart systems. According to Williamson [174], the term "trust" can have various meanings, potentially causing confusion, whereas the concept of "lack of trust" is clearer. This is particularly relevant in situations where information availability is limited [175]. Trust is recognized to be crucial in shaping individuals' willingness to share information within an organization [166]. Additionally, while trust relationships can motivate the breaking of policies and practices, strict adherence to these policies may undermine social relationships

between coworkers [167]. Therefore, privacy designers within organizations must take into account the importance of trust, as ignoring this human value could potentially undermine or subvert the system's security. Singh and Slegers [175] found that users need to feel in control of their information to feel comfortable using smart systems. This control over personal data is related to the human value of privacy[2, 176, 177]. Karat et al. [160] emphasize the critical need for research on the intersection of HCI and privacy. In the context of smart homes, privacy concerns are critical as they can have moral and physical implications for users and bystanders. Bernd and Abu Salma [7, 178] examine how power dynamics and social norms influence domestic workers' perspectives on data collection and usage by smart home devices, focusing on privacy concerns in the workplace, and propose interventions for mitigation.

#### 2.2.2.4 Cross-Cultural Privacy

Li et al. [179] studied cross-cultural differences in privacy management, and presented some recommendations for privacy design in the international context as many technologies have become available around the world and users increasingly share personal information online with people and organizations from different countries and cultures. They further argued that there is a need to investigate cross cultural differences in users' privacy attitudes and behaviors in the use of smart technologies to inform privacy design for technologies that are used globally as many of these technologies still adopt a "one-size-fits-all" privacy design approach [180]. Many cross-cultural studies, not only in privacy but also in other domains, focus on cultural dimensions rather than other measures, such as country and language. This is because cultural dimensions are conceptual constructs that can depict the underlying patterns of how people live in different countries, and offer a way to classify the complex patterns of culture. For example, Li et al. [181] demonstrates that, compared to factors such as country of residence and language, cultural dimensions are better predictors of privacy decisions in terms of both prediction accuracy and explained variance. Other researchers have tried to categorise what

dimensions can describe country level cultural differences, and one of the most influential is Hofstede's six dimensions of culture [182]. Hofstede's model identifies the following six cultural dimensions: (1) Power distance (PDI) is the degree to which the less powerful members of a society accept and expect that power is distributed unequally. A high score of PDI indicates that people accept a hierarchical order. (2) Individualism (IND) is defined as a preference for a loosely knit social framework in which individuals are expected to take care of only themselves and their immediate families. Low individualism is collectivism. (3) Masculinity (MAS) represents a preference in society for achievement, heroism, assertiveness, and material rewards for success. Such a society is more competitive. Its opposite, femininity, stands for a preference for cooperation, modesty, caring for the weak, and quality of life. (4) Long-term orientation (LTO) describes how a society maintains some links with its own past while dealing with the challenges of the present and future. (5) Uncertainty avoidance (UAI) is the degree to which the members of a society feel uncomfortable with uncertainty and ambiguity. (6) Indulgence (IDL) stands for a society that allows relatively free gratification of basic and natural human drives related to enjoying life and having fun. Its opposite is restraint.

Bur et al. [181] argued that support for users' privacy has not been extended equally to all users from around the world, and proposed a framework for evaluating to what extent privacy options are offered and communicated. The proposed framework to be applied in a manner that supports diverse users from around the globe. The framework focuses on cultural issues, legal issues, and user expectations regarding the data-sharing practices and privacy.

#### 2.2.2.5 Privacy in Non-Western and Muslim Contexts

Researchers have argued that privacy concepts vary substantially across cultures, time, and context [177, 183]. 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. [183], 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. [184] highlight the importance of understanding Muslim identity, as Islam is the second-largest global religion [185], and consequently privacy research should address privacy concerns with smart devices in Muslim contexts. While some studies [186, 187] 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. We did not find any research that investigated the role of Islamic norms, practices and values on user privacy in the smart home.

### 2.2.3 Smart Home and Privacy

#### 2.2.3.1 Smart Home Privacy Concerns

Smart devices continue to fuel concerns about users' privacy as risks emerge from data leakage, devices used to facilitate abuse, targeted burglary through device usage information, and many more related threats. Privacy concerns are further exacerbated as many users lack adequate levels of awareness of the threats to privacy posed by smart home devices. In addition, smart devices are susceptible to multiple usability issues that can prevent privacy protection [188, 189]. Researchers [76, 90, 188, 190–197] have identified users' privacy concerns, perceptions, expectations, associated adversarial models with smart home devices, and shed light on some smart home vulnerabilities such as smart TVs recording conversations [198]). Another study [199] found that users disconnected TVs after they became aware of associated privacy threats, and Abdi et al. [194] showed how users regularly avoid such threats by not using the full functionalities of their devices. Prior studies [127, 200] have argued that users lack awareness of privacy threats associated with new technologies such as smart homes, and about how data is processed, and need more clarity and control over their data. These studies emphasized that users' understanding of potential privacy threats and consequences is crucial for managing resulting risks. Gerber et al. [200] discovered that lay users were unable to identify a single privacy risk but instead mentioned general privacy issues (e.g., profiling, data collection) or other non-privacy concerns.

Another study [200] has shown that lay users of smart devices could not identify specific threats from sharing personal data, while other researchers have argued that users need to be aware of privacy threats in order to be driven to use devices according to their privacy preferences [200, 201]. Other studies have found that users prefer to be informed about collected personal data [202–204]. In his taxonomy of privacy types, D. Solove [56] classified privacy into six types, which often overlap with each other. These six types are frequently used in privacy analysis: Right to be let alone [58], limited access, secrecy, control over personal data, personhood, and intimacy. In the same discussion, Karwatzki et al. [205] have distinguished seven types of negative privacy consequences that users perceive when their privacy is breached. The seven proposed privacy consequences are: Physical harm, social status change, resource loss, psychological impact, legal actions, career setbacks, and freedom loss due to personal information access.

#### 2.2.3.2 Bystanders' Privacy Concerns with 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 domestic workers). Such data collection raises concerns about the privacy of bystanders as well as other members of the household. Prior research has focused primarily on household privacy concerns, preferences, and expectations [188, 206–209]. Other researchers in this space have focused on multi-user privacy concerns [206, 210–213]. There is a growing body of literature that explores smart home bystanders [178, 214, 215]; however, more needs to be done to elicit, understand, and relate different privacy preferences—whether they come from users or bystanders [1, 2, 91, 210, 216–225]. We provide definition of smart home bystanders in Section §A.1.3.

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 [226–228]. Bystanders in general may not be aware of smart devices or what they are doing [224, 229, 230], 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 [228, 231, 232]. Additionally, there are concerns that they may lack social or economic power to negotiate and enforce privacy preferences [1, 231–233]. Research studies have largely addressed bystanders primarily in Western contexts [2, 56, 234–239] 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. [232] have argued that smart devices should be designed to provide privacy assurances for everyone in range, and Marky et al. [228] argued that bystanders' limited awareness hinders privacy protection. Finally, in order to enrich knowledge in this space, researchers are working on building a shared knowledge base of smart devices' privacy concerns [188, 240–243].

### 2.2.4 Power Dynamics

#### 2.2.4.1 Smart Home Socio-Economic 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 [7, 244–247]. Kraemer et al. [248] argue that socio-cultural dynamics are linked to control over smart devices, and other studies argue that control over smart devices can result in domestic abuse [249, 250].

Research investigating the privacy concerns of smart home bystanders [207, 251–255] 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 [255]. Other studies [220, 256–259] note that Contextual Integrity [CI], and power dynamics can reveal how populations negotiate conflicting norms in a given context, while other researchers argue that the power dynamics among users lead to reduced privacy control for powerless users [235, 260–265]. Asymmetries in power dynamics and associated privacy vulnerabilities have also been explored in the relationships

between employers and employees in business contexts. These power dynamics can create various trade-offs that also apply to domestic workers in the home, and can negatively affect workers' performance and satisfaction [233, 235, 236, 266–271]. Neville et al. [272] discussed that some users are able to take actions on behalf of the entire family members. Levy and Schneier [273], and Freed et al. [274] discussed how technology can facilitate invasion of privacy in intimate relationships. They observed how authorised users use the functionalities that they have access to in order to track, manipulate and threaten their partners. While, Feltwell et al. [275] explored the collective control of technology in the home and the subsequent power dynamics that develop around ownership and control of the smart devices.

Bernd et al. [178] discussed that domestic workers often expressed privacy concerns and feelings of discomfort about surveillance due to power dynamics. However, many workers said they defer to families' decisions about the deployed smart home devices. They have observed three ways workers framed how power dynamics manifest between workers and their employers (i.e., the families). Workers think home owner have the right to protect their houses, to choose what devices to use, to determine the location of the devices, and how to use them. Lachlan et al. [276] explores interpersonal power dynamics in smart homes. Geeng and Roesner [210] show that users in charge of the smart devices do not consult with cohabitants before installation due to a passivity of co-users or inequality in their relationship [210]. Kraemer and Flechais [220] discussed that the imbalance in control, knowledge, and concerns may change power dynamics in the home and create further tensions between co-users. Van Kleek and Seymour [277] argued that the power dynamics within families and cohabitants are altered by technology in their homes where they do not expect to be surveilled.

Avdic [278] discussed that it would be useful to explore and investigate potential solutions for how bystanders could be conveniently involved into the development of smart homes over time. He argues also that we could investigate the power dynamics between owners and bystanders, and if such dynamics change over time (e.g. children grow up) or if they are strict in some regards (e.g. guests). Sailaja et

al.[279] discussed the need for an efficient management of data to mitigate perceived threats to autonomy and agency, and Geeng et al. [210] suggested some design recommendations to minimize power differences, as smart home technology designs can and should take a role in minimizing the power differences among users in the home. They found differences in power, agency, technical skill, and technical interest among different people living in a smart home. They argued that there is often an active user who takes the initiative to learn about devices, and passive users who adapt to devices and/or rely on the active user to make changes. DeSmet et al. [280] argued that behavior change theories such as the Social Cognitive Theory [281] is well suited for studying power dynamics between different user groups. Bandura. [282] has discussed as well the human agency in his social cognitive theory.

Apthorpe et al. [217] found that smart devices can affect power dynamics among smart home residents, as it pertains to the management of the household environment. However, conflicts can arise among users as the technology can facilitate surveillance, causing distrust and disagreements over device use. Furthermore, the question of exactly who has control over devices in the home may be an indicator of existing interpersonal and/or socio-cultural dynamics [210, 220, 233, 248, 259]. In extreme scenarios, imbalances in device control can enable domestic abuse [233, 274, 283–286], and other studies [114, 287–290] argue that smart devices can turn children into targets of, or bystanders to, data collection. In order to protect the privacy of bystanders in smart homes, various proposals have been made ranging from how to detect hidden cameras [225, 291–294], to methods for signaling that a device is collecting or broadcasting data [188, 227, 228, 232, 295–298]. Others have suggested using objects [299, 300] or contextual cues (i.e., locations, user proximity to others) [91, 120, 210, 219, 232, 301–303] to signal preference to blur or stop recording data. However, these technical approaches are limited, as many users do not trust companies or service providers to apply them [91, 304, 305]. Furthermore, others suggest facilitating transparent and open discussion of device usage inside home between households and bystanders [1, 227, 306].

#### 2.2.4.2 Employer-Employee Dynamics

According to Bangura et al. [307], female domestic workers from Sri Lanka and the Philippines, numbering around 70,000 [50] in Jordan, come from different cultures and religions. They often travel alone and are employed under contractual arrangements that provide them with few rights, no freedom, and limited communication with the outside world. They are essentially kept as virtual prisoners in their employers' households and are unable to form or join unions. Although embassies and consuls in host countries provide some support for their well-being, they are unable to monitor all their nationals due to the large numbers of migrant workers involved. Furthermore, there is an economic interest in maintaining demand for foreign domestic workers, who collectively represent a significant source of foreign earnings for their home countries. As a result of the imbalanced power dynamics, workers tend to compromise their rights and accept their employers' decisions within the home. Rodriguez et al. [308] explored the experiences of working female expatriates, such as maids, nannies, and babysitters, in the Middle East and North Africa (MENA) region, and found that these female domestic workers face unique challenges.

Frantz [309] discussed that over 100,000 Sri Lankan women leave their homes annually to seek employment as domestic workers in the Arab world, with demand rising sharply in Jordan where at least 70,000 foreign domestic workers are currently employed. The study [309] examined the social, economic, and political factors influencing the market for foreign domestic workers in Jordan, highlighting changes in class formation and kinship as key factors. Focusing on Sri Lankan domestic workers in Jordan, the study explored the dynamic relationships between domestic workers and their employers, arguing that the construction of relations of dependency is an essential strategy used by both groups. Additionally, the study [309] showed that at least one in every eleven Jordanian households employs a foreign domestic worker, framing relations between domestic workers and households as relations of dependency rather than patronage. Another study by Caillol et al.[310] focused on Filipino domestic workers in Jordan and their strategies for creating new

opportunities within the Jordanian sponsorship system. Other studies [311, 312] highlight that domestic workers may be subject, in some cases, to exploitation, lack of freedom of movement, and violence against them, including physical attacks ranging from rape to slapping, overworking, lack of food and privacy, and trauma. The article [312] also notes that changing jobs is often impossible, running away from employers can lead to arrest, and continued suffering to finish the contract period.

### 2.2.5 Privacy Protection Regulations

#### 2.2.5.1 Overview of Data Protection Regulations

Several studies [288, 313–326] have discussed data protection with smart home devices. We found that there is quite a variety of legal implementations across Western and non-Western regions (e.g., MAME regions) sampled in our meta review of regulations (cf. Table 2.1). The recent release and implementation of global data privacy laws have significantly impacted organizational behavior and international business. Many, particularly those with a global reach, face pressure to align their policies with the GDPR. This alignment is not only driven by the desire to conduct business in Europe but also because the GDPR has established itself as the *"Golden Standard"* in Data Protection Law globally [327]. The global significance of the GDPR is exemplified by the fine of 150 million Euros that the French National Data Protection Commission (CNIL[34]) imposed for its violation on the global tech giant Google[35]. The CNIL enforcement action focused in particular on the GDPR's transparency and consent requirements, and at the same time, provided useful guidance on how to design privacy policies [328]. Furthermore, in recent years, increasing numbers of countries worldwide have implemented new or amended legislation in data protection and privacy, based on a core set of principles in common with the GDPR as discussed in different studies [179, 329, 330]. These principles include, the recognition of data protection as a fundamental right; the adoption of overarching legislation in the field; the existence of enforceable individual

[34]CNIL-The French Data Protection Agency
[35]CNIL-Fines on Google

privacy rights; and the setting up of an independent supervisory authority[36] of new or modernized laws that overlap up to 80% with the GDPR.

**Table 2.1:** Status of Data Protection Regulation in World Leading Countries

| Country | Data Law | Regulatory Body | Year Enacted | Smart Home Consideration |
|---|---|---|---|---|
| Turkey | DPL[38] | KVKK | 2016 | Not Explicitly |
| Malaysia | PDPA[50] | Malaysia-PDP | 2011 | Not Explicitly |
| Europe | GDPR | EDPS | 2018 | Not Explicitly |
| USA | State Dependent | State Dependent | 2022 | No |
| China | PIPL[48] | CAC | 2021 | No |
| Brazil | LGPD[39] | ANPD | 2021 | Not Explicitly |
| India | DPDP IT Act[49] | India DPA | 2023 | Not Explicitly |
| Canada | PIPEDA Act[37] | OPC | 2000 | Not Explicitly |

Similar to the GDPR, Canada's PIPEDA[37], Turkey's *DPL*[38], and Brazil's LGPD[39] provide a framework for protecting personal data; however, they are not explicitly applicable to personal and household activities (cf. Table 2.1). Various nations struggle to release effective, holistic data protection laws. In the United States, data protection laws vary by state, and there is no comprehensive federal law that uniformly protects personal data. However, certain federal laws regulate specific types of personal data, including health information (HIPAA[40]), financial information (GLBA[41]), and children's online privacy (COPPA[42]). Some states have also enacted their own data protection laws, such as CCPA[43], CPRA[44], and NYPA[45], TCPA[46], and FERPA[47], which provide additional consumer protections and impose obligations on businesses regarding the collection, use, and disclosure of personal data. Overall, USA lacks a comprehensive federal law for data protection. Gilman [331] argues that the USA regulations place greater responsibility on users for protecting their privacy, and allows companies and government entities

[36]UNCTAD-The United Nations Conference on Trade and Development
[37]PIPEDA-Privacy law in Canada
[38]Turkey DPL-Personal Data Protection Law
[39]LGPD-Brazil Data Protection Law
[40]HIPAA-Health Insurance Portability and Accountability Act of 1996
[41]USA - Gramm-Leach-Bliley Act
[42]USA - Children's Privacy
[43]CCPA-California Consumer Privacy Act
[44]CPRA-California Privacy Rights Act
[45]NYPA-New York Power Authority
[46]TCPA-USA-Telephone Consumer Protection Act 47
[47]FERPA-Family Educational Rights and Privacy Act

comparatively more freedom to collect and trade data. Similarly, the China data protetcion law (PIPL[48]), India's DPDP[49], and Malaysia-PDPA[50] contain GDPR-inspired provisions around consent and the right to be forgotten, and do not have explicit considerations for smart home users data protection.

Prior studies [332–336] have explored the impact of GDPR on smart home devices and users, as well as ways to improve GDPR-compliant consent notices. Research has also investigated the effect of GDPR on web interfaces, with Anderson et al. ([337]) arguing that the GDPR aims to protect individuals' privacy by regulating data processing. Additionally, studies have shown that consent decisions can be influenced by factors such as highlighted buttons and the number of options offered ([338]). Other studies have focused on dark patterns that manipulate users into providing consent for data collection. Dark patterns are user interfaces designed to deceive users and have been documented in various sources [339–344]. Examples of dark patterns include hiding privacy-friendly choices and advanced settings, pre-selecting check-boxes, requiring more effort to reject consent, and providing take-it-or-leave-it choices [341, 342]. The negative reputation of dark patterns has led California to prohibit their use under the California Consumer Privacy Act (CCPA[43] [345], and EU data protection officers have cited dark pattern examples in their advisory documents [346]. Nouwens et al. [346] analyzed the 10,000 most visited websites in the UK and found that only 12% of the websites were free of dark patterns.

The modern enterprise landscape is teeming with interconnected devices and services that gather and transmit data to external parties, posing potential risks to privacy and data security [347]. These include copy machines, mobile apps, smart devices (IOT), and more, which may collect sensitive personal information. Enterprises must be cautious in adopting such technologies, understanding their responsibilities as data controllers or processors under data protection laws. While it's commonly assumed that enterprises are always data controllers and third parties are data processors, the reality is more nuanced, with instances where

[48]PIPL-China Data Protection Law
[49]India: Digital Personal Data Protection Act
[50]Malaysia: Data Protection Law

third parties also act as controllers. The distinction between data processors and controllers in GDPR remains significant [51], yet the GDPR introduced substantive provisions directly applicable to processors, blurring this line to some extent. When enterprises engage third-party providers, whether as processors or controllers, there are advantages and drawbacks to each scenario. Opting for a data processor grants more control over data handling, while using a data controller may better protect employee privacy, particularly concerning sensitive information. However, employing a third-party controller might relieve the enterprise of certain compliance responsibilities and potential liabilities compared to a data processor. Enterprises must carefully evaluate these factors, conduct due diligence on providers, understand their obligations based on provider characterization, and take necessary steps to ensure legal compliance

**2.2.5.1.1 The Concepts of Controller and Processor.** The GDPR came into effect in May 2018 [317, 347, 348], ushering in new rights for individuals and imposing fresh compliance duties on organizations handling data within the European Economic Area. The GDPR introduced the potential for significant fines, reaching up to 4% of a company's annual global revenue, for non-compliance. Central to European data protection law, the GDPR maintains the distinction between data controllers, who determine how personal data is processed, and data processors, who handle data on behalf of controllers. However, the line between these roles can be blurry, as demonstrated by cases where entities like employers may act as data controllers despite not owning the data they handle, highlighting the complexity of data management responsibilities under the GDPR.

The distinction between data controllers and processors, as outlined by the GDPR-Article 29 [52] Working Party, revolves around the primary purpose and control over data processing activities. While controllers determine the purposes and means of processing data for their own objectives, processors also have some authority in determining technical and organizational details. However, processors must align

[51] GDPR: Data processors and controllers
[52] GDPR-Article 29

their actions with the controller's authorization and operate within the scope of the contracted services. Despite the delineation, there exists ambiguity, especially concerning what constitutes "providing the service" for processors, encompassing essential business functions, security measures, service improvements, and data analysis for service enhancement. Under the GDPR and other global laws [317, 347], both controllers and processors bear similar obligations, including data security, documentation requirements, and personnel appointments like EU representatives or Data Protection Officers. This parity in obligations underscores the significance of data protection across both roles, diminishing the clear-cut distinction present in prior data protection laws. In practice, scenarios involving data processing can vary widely, from the common roles where a provider acts as a processor for an enterprise to scenarios where both parties are independent controllers or joint controllers, highlighting the complexity and fluidity of data management responsibilities in modern data-driven environments.

Contractual provisions are pivotal in defining data protection commitments between enterprises and third-party providers, whether they act as data processors or controllers under GDPR guidelines [317, 347]. For data processors, GDPR-Article 28 [53] specifies crucial elements that must be included in the contract, such as instructions on data processing, confidentiality obligations, security measures, cooperation in handling data subject requests, data deletion or return, and adherence to the controller's obligations. Conversely, if the provider functions as a data controller, GDPR does not prescribe specific contractual terms, but enterprises benefit from securing binding commitments on data protection and appropriate data usage. In cases of joint controller-ship, contracts should clearly outline roles and responsibilities, particularly concerning data subject notices and rights. Irrespective of the provider's role, enterprises should seek robust contractual assurances regarding data protection, aligning with GDPR principles and potentially supplemented by additional protections through contractual commitments. Although negotiating customized terms may pose challenges with large providers, enterprises can make

[53] GDPR-Article 28

informed decisions by comparing provider terms and selecting those offering strong data protections. These contractual provisions not only ensure legal compliance but also promote transparency, accountability, and responsible data management practices, fostering a secure and trustworthy relationship between enterprises and their third-party providers.

**2.2.5.1.2 Data Protection Regulation within Smart Home Environment.** The GDPR[29] applies to the processing of personal data, which encompasses any information that can directly or indirectly identify an individual. We mention below some provisions within the GDPR that could be applied to data collection and processing within smart homes: (1) Definition of Personal Data: Article 4(1) of the GDPR defines personal data as *"any information relating to an identified or identifiable natural person ('data subject')."* (2) Data Controllers and Data Processors: Articles 4(7) and 4(8) of the GDPR define data controllers as entities that determine the purposes and means of processing personal data, while data processors are entities that process data on behalf of the controller. (3) Principles of Data Processing: Articles 5 and 6 of the GDPR outline principles for processing personal data, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. (4) Lawful Basis for Processing: Article 6 of the GDPR specifies lawful bases for processing personal data, including consent, contractual necessity, legal obligation, vital interests, public task, and legitimate interests. (5) Rights of Data Subjects: Articles 12-23 of the GDPR detail the rights of data subjects, including the right to access, rectify, erase, restrict processing, data portability, object to processing, and not be subject to automated decision-making. (6) Security of Processing: Article 32 of the GDPR mandates that both data controllers and processors implement appropriate technical and organizational measures to ensure the security of personal data. (7) Data Breach Notification: Article 33 of the GDPR requires data controllers to notify supervisory authorities of data breaches without undue delay and, where feasible, within 72 hours of becoming aware of the breach. (8) International

Data Transfers: Articles 44-50 of the GDPR govern the transfer of personal data outside the European Economic Area (EEA) and prescribe mechanisms such as adequacy decisions, standard contractual clauses, binding corporate rules, and certification mechanisms. These articles, among others in the GDPR, form a comprehensive regulatory framework for the protection of personal data within smart homes and similar contexts, ensuring that data collection and processing activities are conducted in a lawful, transparent, and secure manner while respecting the rights of data subjects.

However, examining the GDPR[348–350] and similar regulations, we found that a data controller engaged in personal or household activities for their own purposes is exempt. GDPR and similar regulations typically extend their coverage to the data subject if their data is processed within the home by another data controller. In the case of a householder employing a domestic worker and using a smart home device for surveillance, the householder becomes a data controller, as the context involves an employment contract rather than purely domestic activities. Additionally, consideration should be given to the smart home service provider; if the company is based in the EU, GDPR applies, even if the processing occurs in Jordan. For example, companies like Siemens must adhere to GDPR regulations for their smart home devices sold in Jordan. In situations where the householder acts as a joint controller, the application of GDPR may become a legally gray area. Therefore, GDPR and similar laws are not explicitly applicable to personal and households activities[351, 352]. Vojković et al. [348] examined the regulatory landscape surrounding smart home devices' data processing, and highlighting the responsibilities of data controllers and processors in mitigating potential data breaches. They argued for future efforts to focus on analyzing comparative law and best practices, particularly at the EU member states level, to enhance regulatory frameworks and ensure compliance from data controllers and processors, fostering a safer environment for smart services without compromising user rights.

#### 2.2.5.1.3 Challenges for Data Protection Regulation in Smart Homes.

Enforcing data protection laws in smart home environments poses multifaceted challenges due to the intricate nature of these systems [353–355]. Smart homes comprise various interconnected devices and technologies, making it challenging to effectively monitor and regulate data flows. Furthermore, implementing data protection laws in smart home environments faces several notable technology barriers. The decentralized nature of data processing across devices and platforms complicates comprehensive data protection management. Accurately identifying vulnerable individuals and their legal guardians within these systems presents challenges for GDPR compliance. Balancing robust data security measures with user-friendly design is another challenge, requiring careful consideration. Ensuring interoperability among smart devices while adhering to data protection standards adds complexity to implementation efforts. Furthermore, integrating edge computing for privacy-preserving data processing necessitates navigating technical challenges within existing smart home architectures. Effectively managing data collection and minimization practices is also technically demanding, requiring strategic planning. The dynamic technological landscape requires continuous adaptation to new developments to maintain GDPR compliance and uphold data protection standards effectively.

### 2.2.5.2 Privacy Protection Regulation in Jordan

As of this thesis writing, the Jordan Ministry of Digital Economy and Entrepreneurship[54] has announced the enactment of the new 'Jordan Data Protection Law[55]', slated for enforcement in March 2024[356]. Our meta-review [357–361] of data protection regulations in Jordan (cf. Table 2.2) reveals that the Jordanian constitution protects the right to privacy under *'Article 18*[15] *'*. We believe that the new law in Jordan will be complemented by existing laws in Jordan to address any privacy or data breaches and disputes. These laws include: The Telecommunications Law No.

[54]Jordan-Ministry of digital economy and entrepreneurship
[55]Jordan: Jordan Personal Data Protection Law

**Table 2.2:** Existing Laws in Jordan

| Regulation/Law Name | Articles | Coverage | Personal Data and Smart Home Users |
|---|---|---|---|
| Personal Data Protection Law[55] | All | Personal Data | Depends on Proving Material Damage |
| Cyber-Crime Law[57] | 11, 13 | Mass Surveillance, Online Defamation | Depends on Proving Material Damage |
| Telecommunications Law[56] No. 13/1995 | 56 | Private Communications | No |
| Penal Code[58] | 3, 4, 348, 356 | Penalizes dissemination of Private Data | Depends on Proving Material Damage |
| Labour Law[60] | All | General work terms and conditions | No |
| Access to Information Law[62] | 13 | Correspondence Between Government Entities | No |
| Credit Information Law[61] No.15/2010 | 8, 18 | Credit Status | No |

13/1995: Article 56[56], Cyber-Crime Law[57], Penal Code-Article 348[58], Anti-Terrorism Law No.55/ 2006-Article 4[59], The Labour Law[60] [362, 363], Credit Information Law No.15/2010-Article 8[61], and Access to Information Law-Article 13[62].

The new Jordan data protection law, which is inspired by the EU GDPR [88], aims to establish a legal framework of personal data protection and data processing and storage mandates [364], and to introduce some important concepts to personal data protection, such as: the right to consent to data use, the right to be forgotten, and the right to remain anonymous. While the new law will not address explicitly privacy and data collection in the home, it will state that the ownership of data must be clearly identified, and the owners of the data must be assured that their data will not be used without their consent and awareness. Additionally, Jordan has issued the Government Data Classification and Management Policy 2020[10] to set the base for government entities to classify data according to expected risks. The policy defines four levels: Confidential, Sensitive, Private, and Normal. Our expectations regarding the new Jordanian data law bill [365, 366] did not change after its enforcement, particularly concerning explicit data protection regulations for smart home users, as these were not found in the announced legislation. The new law, along with existing relevant laws, lacks clear definitions regarding rights for users in smart home environments, including ambiguous delineations of data controllers and processors for personal data within these contexts. These laws have different articles that address mass surveillance, penalize online defamation, and

[56]Jordan-Telecommunications Law
[57]Jordan-Cyber Crime Law
[58]Jordan-Penal Code
[59]Jordan-Anti-Terrorism Law No.55/ 2006-Article 4
[60]Jordan-Labour Law
[61]Jordan-Credit Information Law
[62]Jordan-Access to Information Law

allow concerned government authorities to suspend, confiscate, and search personal smart systems and computers, which manifests clear violations of individuals' privacy rights. Moreover, it is worth mentioning that the Jordanian labor law has some articles that prohibit installing smart devices in domestic workers' private locations (bedrooms and bathrooms), but it does not explicitly address workers' data protection, raising questions about whether the homes where workers work qualify as domiciles or workplaces for workers[364].

#### 2.2.5.3 Status of Data Protection Regulation in MAME Region

Exploring data protection regulation in other MAME region countries (cf. Table 2.3) revealed that, while Jordan has just announced the forthcoming enforcement of its data protection law[55], Kuwait [367], and Iraq [368] do not currently have data protection laws. However, the governments of Kuwait [369] and Iraq [368] are considering enacting new data protection laws. Prior study [357] has explored the status of data protection regulation in MENA and argued for urgent adoption of robust and strong data protection legislation in the region's countries that address users' rights, improve their autonomy and freedom of choice over their personal data, and protects users' privacy against surveillance and exploitation for financial profit, as well as unlawful or accidental intrusions, and breaches.

In Saudi Arabia, we found that SDAIA[63] has enacted the Saudi data protection law (PDPL[64]). Saudi-PDPL includes Islamic Shari'ah [186] principles of privacy protection which relates privacy to the dignity of people, guarantees communication privacy, and prohibits monitoring of people. However, Saudi-PDPL is not explicitly applicable to smart home settings. In UAE, the UAE Data Office[65] has enacted the *Federal Decree-Law No. 45* regarding the *Protection of Personal Data* (PDP[66]), which covers the processing of personal data, consent-taking, and promotes several data subject rights, and requirements for controllers and processors, such as mandatory breach notifications, the appointment of data protection officers, and

[63]SDAIA-Saudi Data and Artificial Intelligence Authority
[64]PDPL-Saudi- Data Protection Law
[65]UAE-Data Office of UAE
[66]PDP-Data protection laws

**Table 2.3:** Status of Data Protection Regulation in MAME Countries

| Country | MAME | Data Law | Regulatory Body | Year Enacted | Smart Home Consideration |
|---|---|---|---|---|---|
| Jordan | Yes | PDPL[55] | MODEE | 2024 | No |
| Saudi Arabia | Yes | PDPL[64] | SDAIA[63] | 2021 | No |
| UAE | Yes | Decree No. 41[66] | UAE Data Office[65] | 2021 | No |
| Qatar | Yes | PDPPL[68] Law No. 13 | QFC[67] | 2016 | No |
| Bahrain | Yes | PDPL[72] Law No. 30 | MoJ[71] | 2019 | No |
| Oman | Yes | DP[70] Law No. 06 | MTCIT[69] | 2022 | No |
| Kuwait | Yes | None | None | – | No |
| Egypt | Yes | PDPL[75] Law No. 151 | PDPC[74] | 2020 | No |
| Lebanon | Yes | Law[73] 81 | None | 2018 | No |
| Iraq | Yes | None | None | – | No |
| Syrina | Yes | None | None | – | No |

implementation of technical and organisational measures to support data security. Similar to Saudi-PDPL, the UAE-PDP does not explicitly address smart home data protection. In Qatar, the QFC[67] has presented the *Data Protection Legal Framework (Law No. 13) (PDPPL[68])* in 2016 that addresses *Privacy and Protection of Personal Data*, and similar to other MAME countries, Qatar-PDPPL[68] does not address explicitly smart home data protection.

In Oman, we found that the MTCIT[69] has promulgated the *Data Protection Law* (DP-Law[70]) in 2022. Oman-DP Law addresses data protection principles such as transparency, honesty, respect for human dignity, and data subject rights, as well as obligations on data processing, which bring the country's legislative regime into closer alignment with global data protection laws. However, Oman-DP Law does not explicitly address smart home data protection. In Bahrain, we found that the *Ministry of Justice and Islamic Affairs* (MoJ[71]) has enacted the Bahrain *Data Protection Law No. (30)* PDPL[72] in 2019. Similarly, Bahrain-PDPL does not address smart home data protection explicitly. In Lebanon, we found that the country does not have data protection authority, yet the country has enacted Law No. 81 on *Electronic Transaction and Personal Data*[73]. The Law does not address smart home data protection, and is not a data protection law compared to other

[67]QFC-Qatar Financial Centre
[68]PDPPL-Qatar Data Protection Law
[69]MTCIT-Oman- The Ministry of Transport, Communications and Information Technology
[70]DPL-Oman Data Protection Law 2022
[71]MOJ-Bahrain-Ministry of Justice and Islamic Affairs
[72]PDPL-Bahrain - Personal Data Protection Law
[73]Lebanon-Electronic Transaction and Personal Data

international laws, yet, it does address automatic/non-automatic data processing, and promotes transparency about data retention periods, sensitive personal data, and enforces some security measures to be adopted by data controllers. Finally, we found that Egypt [370] intends to establish its *Personal Data Protection Center* (PDPC[74]) (not yet established at the time of writing this thesis), and we found that the government has enacted *Resolution No. 151 (PDPL*[75]) in 2020. The new Egyptian Law has similarities with the GDPR and addresses data collection and processing; however, similar to neighbouring MAME countries, the law does not explicitly address smart home data protection.

#### 2.2.5.4 Economics of Personal Data

Personal data has been consistently referred to as the "new oil" of the internet [371, 372]. According to Bauer et al. [202], personal data is "one of the world's most valuable commodities". Companies such as Facebook and Google have built their business models around collecting and analyzing user data [373]. While giant companies were profiting from consumer data and privacy concerns, personal data markets, such as PFP (Paying For Privacy) and PDE (Personal Data Economy) [373], were growing. Research into personal data markets and their potential [372, 374, 375] dates back to the 1990s. These markets provide customers with a platform to receive compensation for their use of personal data [376]. Personal data markets are often considered GDPR-compliant because they allow users to prevent their personal data from being used entirely (as opposed to the "right to erasure"). However, since the use of personal data is heavily regulated, existing personal data markets must navigate legal grey areas or operate within regulatory limitations (e.g., enforcement gaps, cross-jurisdiction arbitrage) [377].

Additionally, legislators and researchers have strongly argued for property rights (data ownership) regimes for personal data [378, 379], where data is treated as property. However, some argue that data property rights would not effectively protect user privacy. Data property rights would reduce privacy to a commodity,

[74]PDPC-Egypt's Personal Data Protection Center
[75]PDPL-Egypt's Personal Data Protection Law

rely heavily on consumer choice, and are notoriously difficult to implement [380]. Furthermore, the current notice-and-choice models (e.g., users clicking past privacy notices) are already failing because users are unable to understand the potential uses of data, how it will be used, and the associated privacy risks [75]. Data property rights would face similar challenges to existing consent models since they rely entirely on individual control [381]. Other researchers suggest that data property rights may result in a scarcity of personal data and make business models entirely obsolete [381], which could hinder an economy's potential for innovation (e.g., disruption to businesses, hardware supply chains, and software development) [377].

Moreover, measuring and estimating the monetary value of personal data has been a significant focus of many researchers. Different approaches have been used, including examining market capitalization, assessing revenues or net income per user, evaluating the cost of data breaches, and conducting economic experiments and surveys [382]. However, estimating the value of personal data has been challenging in the past because personal data is highly context-dependent and lacks standardization and measurable impacts over time [75, 382]-[383]. Previous attempts to assign a price tag to personal data [384] were unsuccessful because users' privacy choices were influenced by heuristics and biases (e.g., their own valuations of their personal data) [383, 384].

Finally, the monetary value of personal data cannot fully capture the economic and social benefits [381], and studies examining privacy interactions from the perspectives of users and designers rarely consider the economic interests of product manufacturers or business leaders [338].

#### 2.2.5.5 Privacy Statutes in Islam

As a result of the literature review, we found no research that has specifically examined how Islam affects the privacy of individuals in the context of smart homes. Nonetheless, it is worth noting that Islam recognizes the significance of all human rights for individuals' well-being, personal growth, and existence in a civilized society. According to Norwawi et al.[187], human rights recognized in modern constitutions,

charters, and international treaties are embedded in the Islamic religion. This includes the recognition of fundamental human rights, such as respect for life, privacy, freedom, equality, property, and religious beliefs. Therefore, it can be inferred that privacy is a core human right in Islam that should be protected in all aspects of life, including the use of smart home technology. Further research is required to investigate how Islamic principles can inform the development and implementation of smart home technology while ensuring the protection of privacy rights.

Several studies [186, 187] have highlighted the below about privacy rights in Islam: (1) Islam gives great importance to the fundamental human privacy right. (2) Islamic statute fully acknowledges the sanctity of the privacy of one's home and private life, and there is ample admonition against prying into the affairs of others. (3) The principles of Islam elevate the religious conscience of every Muslim, and protection of the privacy of every Muslim lies at the core of Islamic principles. (4) If someone happens to come across private information, further disclosure of that information is not permitted. Managing the affairs of the private domain is the exclusive right of the owner of that space only. (5) Islam prohibits entering others' homes secretly. (6) Privacy of family members is protected as Islam protects family members from secret intrusion into their privacy. (7) Privacy within the home is protected as Islam puts limitations on people living or existing in the home. (8) Islam educates respect for privacy to the extent that even if someone is invited for meal, he should show up only when expected and should not stay unnecessarily after taking the meal. (9) Islam lays great stress on preserving one's own privacy, and thereby making one aware of guarding one's right of privacy.

Based on the literature review, it can be inferred that Muslim societies generally uphold the value of privacy rights and are expected to exhibit responsible behavior in regards to the privacy of individuals in smart homes. Islamic principles recognize the importance of human rights, including privacy, for personal growth and well-being in civilized societies. Therefore, it can be assumed that Muslim societies prioritize privacy protection in all aspects of life, including in the context of smart home. However, further research is necessary to explore how Islamic principles

can inform the development and use of smart home technology in a way that upholds privacy rights in practice.

## 2.3 Conclusion

This chapter presents several essential elements to contextualize our research studies, including providing information about Jordan as the study context, and a review of the current state-of-the-art privacy research related to smart homes, and data protection regulations. By providing background information on the study context and previous research, this chapter lays the groundwork for the subsequent chapters of this dissertation. The aim is to establish a clear understanding of the research scope and goals, and to situate the study within the broader context of existing literature and research.

From the literature review, several key gaps in existing research on smart home privacy have been identified and detailed in Section §1.1.3. These gaps in the literature highlight the need for further research in the area of smart home privacy, specifically in MAME contexts like Jordan. This need becomes more pronounced due to the lack of explicit data protection regulations for smart home users in Jordan. Further exploration and investigation are essential to bridge these gaps and contribute to the understanding and resolution of privacy concerns in Jordanian smart homes.

# 3 Methodology

Our literature review (cf. Section §3.1) shows the research approaches adopted in smart home security and privacy research studies. These approaches consist of a mix of human-computer interaction (HCI), information security, and usable security and privacy approaches. In Chapter 1, we outline the research problem (cf. Section §1.1), and the identified research gaps (cf. Section §1.1.3). In this chapter, we outline the applied research approach and methodology (cf. Section §3.3), the applied data collection methodology (cf. Section §3.2.3), and the ethical considerations of this research (cf. Section §3.4). In the following sections, we summarize the approaches and methodologies adopted in our research studies.

## 3.1 Privacy and Security Research Approaches

Prior to conducting the research studies reported in this dissertation, we conducted a literature review of the research approaches in the privacy and security field, focusing on those conducted in the smart home environment with an emphasis on users' privacy and protection. In this section, we outline the common privacy and security research approaches adopted in this domain, and we present and discuss the chosen methods and approaches in this dissertation in Section §3.2.

### 3.1.1 Human Computer Interaction Approaches

The research reported in this dissertation are directly related to the field of human-computer interaction (HCI), which aims to use an understanding of user actions, motivations, and experiences to guide technology development. HCI is a multidisciplinary field that overlaps social and behavioral sciences with information technology, employing theories and methods from both areas. Carroll et al. [155] discussed that the key characteristic of HCI is its interdisciplinary nature.

HCI research encompasses the enhancement of work and organizational processes in technology development in general [385]. HCI scholars have developed many different methods for understanding the tasks and work practices of organizations and their members, which can be used to apply technology in new ways in support of human activities [385]. The methods employed by HCI include developing checklists and cognitive walk-thorough, performing field studies and experiments, conducting interviews, focus groups, and surveys, and using a variety of analytic models. Participatory and ethnographically driven designs are both often tested in an HCI context, with users participating in design work and/or having their actual use of new technology studied in order to ensure that real-world use rather than normative description underlies design [386].

Furthermore, the wider physical, social, and cultural context within which HCI occurs can influence users' motives and actions. Dix et al. [157] warn that while designers of interactive systems may have little or no control over elements of this context, they must be aware of them if they are to fully understand the user's behavior within the problem domain. The methodologies and tools used to collect and analyze data from participants have mainly emerged from the social sciences. These methods and tools are detailed in the following sections.

#### 3.1.1.1 User Centered Design

User-centered design (UCD) for smart home devices prioritizes user needs, preferences, and experiences throughout the design and development phases, employing various research methods such as interviews, surveys, and usability testing to gain

insights into user behaviors, motivations, and challenges associated with smart home technologies [387, 388]. This approach involves persona development to create fictional user representations based on research findings, aiding designers in empathizing with diverse user groups and tailoring solutions accordingly. Additionally, user journey mapping visualizes experiences and interactions over time, helping identify optimization points and enhance the overall user journey.

Prototyping and iterative design are integral to UCD, as they enable designers to refine solutions based on continuous feedback, ensuring usability and satisfaction. Usability testing plays a crucial role in evaluating design effectiveness, while accessibility considerations ensure inclusivity for users with disabilities. Co-creation and co-design involve users directly in the design process, fostering collaboration and empowering them to contribute insights. Establishing a continuous feedback loop enables ongoing improvement and alignment with user expectations throughout the product life cycle, ultimately enhancing the usability, effectiveness, and user satisfaction of smart home devices.

#### 3.1.1.2 Survey Research

Survey research entails the collection of information through responses to questions from a carefully chosen sample of individuals [389]. This method is known for its flexibility in participant recruitment, data collection, and instrumentation methods [390]. Surveys are particularly prevalent in descriptive research studies, where the goal is to estimate specific parameters within a population and highlight their associations [391]. Within the domain of usable security and privacy research, surveys have proven invaluable. They serve as a robust tool for delving into the intricate landscape of concerns, behaviors, and needs pertaining to security and privacy [392–394]. Surveys not only provide a quantitative snapshot of opinions and behaviors but also offer a platform for participants to express nuanced perspectives. This dual nature of surveys, combining structured data collection with the opportunity for open-ended insights, enhances their utility in exploring the multifaceted dimensions of security and privacy in the digital landscape.

#### 3.1.1.3 Case Study

Case study research involves a thorough and meticulous exploration of one or more cases within a real-world context, a practice widely embraced in both social and natural sciences [395–397]. These studies examine a phenomenon within its natural setting, employing diverse data collection methods, such as insights from users, groups, or organizations [392, 398], all without experimental control or manipulation. Case study research proves most suitable when study subjects hold significant value, and the contexts of action are pivotal [399]. The goal is to represent specific contexts at a particular moment, capturing and conveying the reality of a particular context during the study period [400].

#### 3.1.1.4 Experimental Design

Experimental design serves as a systematic approach to conducting research, especially within the realm of HCI. Its primary objective is to navigate through the research process in a controlled environment, ensuring precision in data collection. This precision is crucial for extracting conclusions that either support or challenge hypothesis statements [401]. In HCI, experimental design is a versatile tool employed in various settings, both laboratory-based and non-laboratory-based. This includes observations, field studies, interviews, focus groups, and controlled experiments [400, 402]. These studies, however, are intricately tied to the context in which they take place. The complexity arises from factors such as the overarching purpose of the study, time constraints, budget considerations, and the availability of participants. Moreover, experimental studies in HCI come with limitations, including an inability to address weakly-defined issues, a requirement for strict control factors, and a limitation in representing typical interaction behaviors [403].

#### 3.1.1.5 Ethnography

Ethnography, rooted in anthropology, is the systematic and scientific exploration of individual cultures [404]. This method delves into cultural phenomena by adopting the perspective of study subjects [404]. As a form of social research, ethnography

offers comprehensive insights into participants' social interactions, perspectives, interpretations, and behaviors within social situations and natural settings [400, 405]. Typically, ethnography studies involve the meticulous collection of detailed observations and interviews, often spanning extended periods [406].

#### 3.1.1.6 Diary Study

A diary study, also known as experience sampling or ecological momentary assessment (EMA), is a research method focused on collecting qualitative information by prompting users to log entries about their daily lives in a diary, log, or journal, specifically detailing the activities or experiences under examination [403]. These studies are longitudinal in nature, observing participants over an extended period. Diary studies offer the advantage of providing a wealth of contextual information, including scheduled tasks and personal reflections, without incurring the expenses associated with a full-fledged field study [407, 408]. In the field of Human-Computer Interaction (HCI), diaries prove valuable for exploring usage patterns across various technologies, locations, and environments [400, 409].

## 3.2 Adopted Research Approaches

In this research, two methods were chosen for their suitability to the research problem as a whole: Grounded Theory (GT) and Thematic Analysis (TA). GT is well-suited for exploring and generating understanding, while TA is better for synthesizing and evaluating the outcome of an intervention. Since this research involves addressing the research questions detailed in Section §1.1.4, we have chosen GT to address research questions RQ1, RQ2, and RQ3.1 & 3.2, as they are exploratory and well-suited to GT. On the other hand, we have chosen TA for RQ3.3 as it is suitable for making sense of the qualitative data and underlying patterns.

### 3.2.1 Grounded Theory

Grounded theory, introduced by Glaser and Strauss [410, 411], is a research methodology that constructs theories by analyzing collected data iteratively. This

process involves data collection, coding, and analysis to develop an analytic account of qualitative data. According to Saldana et al. [412], coding involves assigning symbolic attributes to portions of language-based or visual data, capturing their essence. Three main coding techniques are utilized: open coding, axial coding, and selective coding. For data collection in this research, semi-structured interviews were chosen, structured using the funnel technique [413]. This technique begins with broad, open-ended questions, gradually narrowing down to more specific ones. It fosters a natural flow of conversation, enabling the interviewer to gather detailed information while building rapport with the interviewee. The funnel technique ensures comprehensive coverage of relevant topics without overwhelming the interviewee with too many detailed questions at once. It is commonly employed in qualitative research, particularly in studies using semi-structured or unstructured interviews.

Grounded Theory (GT) [411] involves the formulation of hypotheses and theories through the collection and analysis of data, often employing inductive reasoning. GT facilitates a thorough examination of topics and situations from various perspectives, leading to comprehensive and profound explanations. This method can uncover beliefs and meanings underlying behaviors and events, exploring both rational and irrational aspects of behaviors. Grounded Theory is particularly well-suited for exploratory work, enabling the development of substantive theories and in-depth explanations of processes [414]. For instance, Adams et al. [415] used grounded theory to study computer users' behavior relating to password systems, while Dourish et al. [156] investigated the everyday security practices of users of ubiquitous and mobile technologies. Inglesant et al. [168] studied the impact of unusable password policies on users' primary tasks. Qualitative research is exploratory, seeking to understand underlying reasons, attitudes, and motivations. In contrast, quantitative research employs statistical analysis to quantify problems [416, 417].

Grounded Theory (GT) was chosen for its suitability to the research objectives, driven by three primary considerations. Firstly, the investigation is exploratory in nature, venturing into a novel domain lacking established theories—specifically, the privacy concerns of bystanders[1] within smart homes in the MAME[14] context

of Jordan. Notably, no existing studies or conceptual frameworks address smart home privacy in the Jordanian context, highlighting the need for an exploratory approach. Secondly, the research entails the collection of empirical, qualitative data encompassing both the practices and beliefs of smart home users, emphasizing the depth and richness of insights sought. Finally, the resulting theory aims to be firmly grounded in the collected data alone, avoiding reliance on external suggestions or preconceived notions, thus ensuring the authenticity and rigor of the emergent findings. We have chosen Grounded Theory (GT) as the methodological approach for our first, second, and third studies, and we provide further details in Sections §4.2, §5.2, §6.2. The subsequent section elaborates on the applied coding techniques, and the validation of findings within grounded theory.

#### 3.2.1.1 Open Coding

During the initial stage of coding, which is called open coding, each segment of data is assigned a code, typically consisting of a few sentences. The coder does not rely on pre-existing categories but instead closely examines the data and identifies actions in each segment. The most significant and frequently assigned codes are then applied to sift through a large data-set [418]. The coder must determine which codes are most effective in thoroughly categorizing the data. Finally, the coder should identify the properties and dimensions of each category. Properties refer to the general or specific characteristics or attributes of a category, while dimensions indicate the extent or importance of a property along a continuum or range [414].

In grounded theory, open coding can be used to identify areas where additional data is needed before deciding where to collect it from. Collecting and analyzing data concurrently can aid in expanding and refining the research as well as in the development of categories [418]. Open coding stops when we reach saturation [414, 419, 420], a point where researchers no longer identify new concepts (codes) in the data. Saturation signals a comprehensive understanding of the initial codes, suggesting that further coding is unlikely to yield substantially new insights (codes). This phenomenon becomes evident when researchers repeatedly encounter the same

codes or when new data points fail to contribute novel information, indicating that the exploration has reached a point of saturation.

#### 3.2.1.2 Axial Coding

Axial coding [410, 418] is a method used in qualitative research to organize and make sense of data by establishing connections between individual codes and relating them to overarching themes and categories. This process involves using a coding paradigm that focuses on three main elements: identifying the conditions that give rise to the phenomenon being studied, understanding the actions or responses of individuals within those conditions, and examining the resulting consequences. Researchers conduct axial coding to analyze how codes relate to one another and to identify the central themes and categories around which they revolve. The ultimate aim is to reconstruct the data in a coherent manner, which enables a deeper understanding of the phenomenon being investigated.

Themes and categories are considered theoretically saturated when no new themes or categories emerge from further analysis [411]. In axial coding, saturation [419] is reached when relationships between codes, themes, and categories are well-established, and the framework becomes stable. Additional data may no longer significantly alter the relationships or contribute to the creation of new axial codes. This indicates that saturation in axial coding reflects a thorough exploration and understanding of the connections between codes, themes, and categories.

#### 3.2.1.3 Selective Coding

Selective coding [410, 418] is the final stage of integrating and refining a theory in qualitative research. In this process, the analyst identifies a core category and then connects all other categories to this core, as well as to each other. While similar to axial coding, which involves developing themes and categories in terms of their properties, dimensions, and relationships, selective coding operates at a more abstract level of analysis. It is important to note that Strauss's use of selective coding differs from Glaser's approach [418]. However, both methods focus on selectively coding around a core variable identified within the data.

### 3.2.2 Thematic Analysis

Thematic analysis [421, 422] is a qualitative research method widely used across various disciplines. It provides researchers with a systematic approach to uncovering patterns and themes within qualitative data, allowing for a nuanced exploration of complex phenomena. By immersing themselves in the data, researchers can identify recurring ideas, concepts, or emotions expressed by participants, offering valuable insights into their experiences, perceptions, and beliefs. Through the process of coding and categorizing these themes, researchers can then analyze the data in a structured manner, revealing underlying patterns and relationships that might not be immediately apparent.

Unlike grounded theory, which focuses on developing theories grounded in data through iterative coding and constant comparison, thematic analysis emphasizes the identification and interpretation of patterns and themes within the dataset. While grounded theory aims to generate new theoretical frameworks, thematic analysis primarily seeks to uncover and understand the underlying meanings present in the data without necessarily aiming to develop new theories. This distinction highlights thematic analysis as a method primarily concerned with identifying and organizing patterns and themes, offering a more focused approach to qualitative data analysis compared to the theory-building emphasis of grounded theory. We have opted for thematic analysis as the methodological approach to help us address RQ3.3 (our fourth study) as it aims to evaluate how privacy protection can be supported, and we provide further details in Section §7.2.

### 3.2.3 Data Collection Methods

For data collection, we have opted to utilize semi-structured interviews and focus groups instead of other methods (e.g., Systems Development [423], Experimentation, and Observations [424]) for several reasons. Firstly, interviews and focus groups offer the opportunity for in-depth exploration of participants' perspectives, experiences, and emotions, yielding valuable insights into their attitudes, beliefs, and behaviors. Secondly, these methods actively engage participants in the research process,

fostering rapport, trust, and candid responses, thereby enhancing the quality of collected data. Additionally, interviews and focus groups provide context, rich narratives, and nuanced understanding that may elude observational and experimental studies alone, enabling researchers to delve deeper into participants' motivations and decision-making processes. Furthermore, the flexibility of direct elicitation methods allows for dynamic probing and adaptation of questions based on participant feedback. Lastly, ethical considerations such as participant consent, privacy, and confidentiality are more effectively managed with interviews and focus groups, ensuring the protection of participants' rights and well-being throughout the research process. In summary, these factors collectively position interviews and focus groups as the preferred approach for obtaining a comprehensive understanding of complex human phenomena and participant experiences. Detailed discussions on semi-structured interviews and focus groups are presented in subsequent sections.

#### 3.2.3.1 Semi-Structured Interviews

Gillham et al. [425] discussed that semi-structured interviews are "the most important way of conducting a research interview" due to the balance between structure and flexibility in the data obtained. Semi-structured interviews are useful for investigating a given topic in depth, eliciting participants' opinions, and understanding the reasons behind those opinions. In this type of interview, questions are open-ended, allowing interviewees to direct the discussion towards the research topic without being guided by the interviewer's expectations. To ensure equivalence among interviews, while it is not necessary in semi-structured interviews to ask the exact same questions to every participant, we made sure to cover the key topics consistently across the interviews to ensure comparability of data [425]. This approach allows for flexibility in exploring participants' responses while still maintaining a level of standardization in data collection.

In-person interviews are often regarded as the optimal method for data collection to mitigate nonresponse and enhance data quality [426]. However, for practical reasons, online interviews were deemed more suitable, offering various benefits

such as higher response rates, enhanced participant accessibility, cost and time savings associated with travel, the option for participants to maintain anonymity if desired, and potential safety advantages for both researchers and participants [427]. Additionally, online interviews were more appropriate for this study, as it started during COVID-19 pandemic.

In all of our research studies, interviews were scheduled at convenient times for all participants, and we were flexible with participants who requested to reschedule the interviews. Interview scripts were structured using the funnel technique [413]. All interviews were conducted via Zoom and Facebook Messenger, audio recorded on a standalone device. While the majority of the interviews were conducted in English, some were carried out in Arabic. The researcher translated the Arabic interviews with utmost caution to preserve the original ideas and avoid alteration. Subsequently, the interviews were transcribed, allowing researchers to identify repeated words and phrases and recover any data that might have been missed in written notes [428, 429].

#### 3.2.3.2 Focus groups

Focus groups prove effective for exploring participants' perceptions and concerns, enabling the generation of new questions and concepts [430, 431]. Typically involving six to twelve participants, these groups foster open dialogue and opinion development within a social context [430, 432]. However, recruiting participants for focus groups can pose challenges [433]. Moderated by researchers, the discussion topic is presented, encouraging participants to express conflicting arguments without judging the participants' opinions [434]. Subsequently, the focus group discussions are transcribed and analyzed [435]. Throughout all the studies of this research, the interview and focus group guidance scripts adhered to the funnel technique [413], transitioning from general to specific inquiries.

### 3.2.4 Validity of Findings

The usefulness of grounded theory and thematic analysis has been debated due to concerns about repeatability, a vital criterion for research methods to ensure

applicability of findings in similar situations [436]. Proponents of these approaches argue that with comprehensive data and conceptually broad analysis, the elicited themes and developed theory can be abstract and applicable to various phenomena in related contexts. Validity of Grounded theory and Thematic analysis stem from their empirical basis and constant connection between emergent theories, themes, and new data [436]. Findings are validated through triangulation [437] incorporating checking with participants, and with inter-rater reliability checks ensuring consistency among coders [438]. Triangulation through participant checking involves validating or modifying generated themes and theories by seeking feedback from participants. After identifying themes and theories from the data, researchers engage participants to confirm whether the interpretations align with their experiences and perspectives. This process enhances the credibility and trustworthiness of the identified themes and grounded theory by incorporating the insights and feedback of those directly involved in the phenomenon being studied. Participant checking serves as a crucial step in ensuring that the emergent themes and theories accurately represent the lived experiences of the participants, contributing to the overall rigor of the adopted approach.

We acknowledge the limitations of Inter-Rater Reliability (IRR) [438, 439] in validating the robustness of our findings. IRR faces constraints as it relies on agreement among coders, yet interpretations can remain subjective, causing variability even with high agreement levels. Additionally, while high agreement in coding indicates surface-level consensus, it may miss the accuracy and depth of interpretations. Furthermore, IRR's emphasis on coding consistency may overlook broader aspects of research validity like theme relevance or contextual understanding. It also lacks direct input from participants and may be influenced by raters' biases, potentially affecting the validity of findings. Despite these limitations, IRR is valuable for assessing consistency and reliability, aiding in the identification of areas of consensus and divergence, quality control, and enhancing the reliability of research findings. Complementing IRR with other validation approaches such as peer debriefing, various triangulation methods [440] (e.g., Methodological, Data,

Investigator, Theory), and other validation methods is essential to overcome these limitations and enhance the credibility and robustness of our research outcomes, especially as interpretations evolve during early-stage themes and theory building.

## 3.3 Research Approach and Methodology

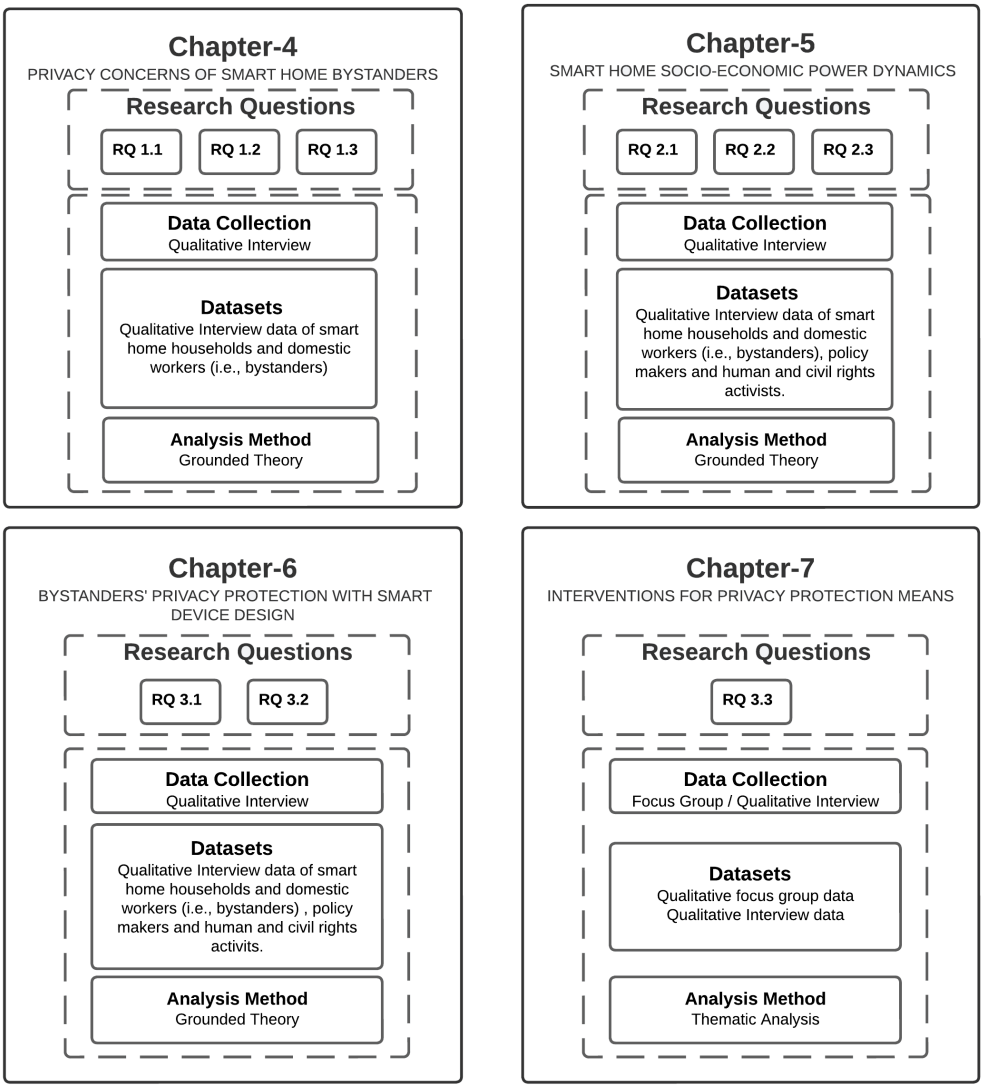
To address the research questions outlined in this thesis (cf. Section §1.1.4), our research methodology aims to achieve the following objectives: (1) Explore users' privacy concerns within smart homes (RQ1), (2) Examine how socioeconomic power dynamics in smart homes affect users' relationship qualities, their privacy concerns, and practices, along with assessing the state of privacy protection regulations in Jordan (RQ2), (3) Investigate challenges in smart device design (RQ3.1, RQ3.2), and (4) Co-design and evaluate a technology probe (mobile application) as an auxiliary tool for enhancing privacy protection (RQ3.3).

Based on our examination of existing research approaches in relevant fields (cf. Sections §3.1 and §3.2), we developed a research approach (cf. Figure 3.1) that systematically and distinctly addressed our research questions. To recruit participants for our qualitative studies, we adhere to qualitative research guidelines [441, 442]. In the subsequent sections, we provide detailed insights into the implementation of our data collection and analysis methods, leading to the acquisition of our datasets. We will also outline the approaches and methodologies employed in conducting the research studies outlined in this dissertation.

### 3.3.1 Smart Home Privacy Concerns (RQ1)

The aim of RQ1 is to understand the privacy concerns, practices, and expectations of households and domestic workers (i.e., bystanders) by exploring and investigating users' privacy concerns and practices in Jordanian smart homes. Our motivation to investigate bystanders' privacy concerns with smart homes in Jordan stems from the outcomes of our exploratory literature review (cf. Chapter 2), which identified a gap where smart home privacy concerns of bystanders in non-Western societies such as MAME contexts like Jordan, have been insufficiently researched. Therefore, our first

**Figure 3.1:** Research Approach and Dissertation Roadmap




study aims to take a step to address this gap. To tackle this research question, we conducted a qualitative user study investigation through semi-structured interviews with 20 participants (12 domestic workers, 8 households) from Jordan (cf. Chapter 4). Our methodology is detailed in Section §4.2, and Figure 4.1.

Participant recruitment involved advertising the study on online social platforms such as specialized Facebook pages, and we also used snowball sampling [443]. We employed purposive and theoretical sampling techniques to recruit participants, enabling the selection of specific eligible individuals, and the sample size was determined by reaching saturation. Demographic details of the participants are

presented in Section §4.2 and Table 4.1. We designed two semi-structured interview guides, one for the domestic workers' group and the other for the households' group, employing the funnel technique [413] to structure our interviews. Prior to initiating our first study, we conducted 4 pilot interviews (2 for each participant group) to assess the clarity of the questions. Adjustments were made based on the feedback from the pilot interviews. The trained researcher conducted the 20 interviews in both English and Arabic, then translated the Arabic interviews into English, ensuring utmost care to faithfully represent the participants' insights without any alterations or changes.

To facilitate theory generation from our research, we employed Grounded Theory to analyze the interview scripts following Strauss and Corbin's data analysis method [410]. The interviews were recorded after taking the participants oral consent, and the researcher transcribed the audio interviews. The coding process of the scripts was facilitated using the NVivo 12 Pro[76] software tool. To verify the reliability of the study codebook, we tested for inter-rater reliability [444]. Additionally, we assessed the reliability and credibility of our findings using grounded theory triangulation [437]. The findings of the first study resulted in five key themes (cf. Table 4.2), detailed in Section §4.3. We discuss the study findings in Section §4.4, and conclude with recommendations to mitigate the impact of smart home devices on bystander privacy in Jordan, along with a discussion of potential future research directions.

### 3.3.2 Power Dynamics, and Data Protection Regulation (RQ2)

The aim of RQ2 is to delve into the complex power dynamics between households and domestic workers within the smart home context in Jordan. This question seeks to uncover how these power dynamics influence and mirror relationship dynamics among users, affect privacy concerns and behaviors, shape perceptions of rights, and potentially foster exploitative practices of smart technologies, which in turn, reinforce these dynamics. Our motivation to investigate power dynamics in smart

[76]NVivo 12 Pro-An application that lets users organize, analyze, and visualize information

homes was inspired by our first study (cf. Chapter 4), which unveiled the influence of asymmetric socioeconomic power dynamics on users' privacy concerns with smart home devices.

Our methodology is detailed in Section §5.2. We initiated a qualitative user study with 30 participants, comprising 8 domestic workers, 7 households, 7 policy makers, 5 human and civil rights activists, and 3 labor law experts from Jordan. Recruitment efforts involved advertising on online platforms like Facebook specialized pages and LinkedIn, along with employing snowball sampling to reach participants who were hard to reach through other approaches. We utilized purposive and theoretical sampling approaches for participant recruitment, allowing the selection of specific eligible individuals, with the sample size determined by reaching saturation. Demographic details of our participants are presented in Table 5.1, Table 5.2, and Table 5.3. We designed three semi-structured interview scripts tailored to each participant group: domestic workers, households, and policy makers and activists (i.e., regulators, human and civil rights activists, and labor law experts). To ensure question clarity and identify potential script errors, we conducted one pilot interview for each script before commencing the study.

We conducted all interviews remotely using Zoom and Facebook Messenger. The interviews were audio-recorded with participants' oral consent. The trained researcher conducted the 30 interviews in both English and Arabic. The researcher translated the Arabic interviews taking utmost care to represent the participants' insights during the translations without any kind of alterations or changes to the participants views and insights. The funnel technique [413] was used to structure the interview scripts. Grounded Theory, following Strauss and Corbin's data analysis method [410], was employed for codebook development and theory generation. The 30 semi-structured interview scripts were transcribed and analyzed facilitated by NVivo 12 Pro software. To ensure codebook reliability and credibility, we tested for inter-rater reliability [444] and used grounded theory triangulation to validate our findings [437]. The findings of the second study are detailed in Section §5.4. Subsequently, we delve into a discussion of these findings in Section §5.5,

providing a thorough examination and offering several recommendations for social, legal, business, and technical interventions aimed at balancing smart home power dynamics and enhancing privacy protection for both bystanders and households.

### 3.3.3 Privacy Protection with Smart Device Design (RQ3.1 and RQ3.2)

The aim of RQ3.1 and RQ3.2 is to explore the smart device design challenges for users' privacy protection in Jordanian smart homes, to consider the privacy of smart home bystanders, to develop solutions that address the privacy needs of all stakeholders, and to take into account non-Western contexts like the MAME context of Jordan. Our motivation to investigate design challenges for privacy protection in smart homes stemmed from our previous studies (cf. Chapters 4 and 5). These studies highlighted a prevalent emphasis on researching privacy protection within smart home devices in Western contexts (Europe and North America). However, there has been limited exploration of the design challenges associated with protecting bystanders, and even fewer studies have addressed these challenges within MAME contexts, such as Jordan.

Our methodology is detailed in Figure 6.1, and Section §6.2. We conducted a qualitative user study, utilizing semi-structured interviews with a total of 44 participants. This participant group comprised six domestic workers, six households, eight local business leaders, 15 designers, and nine international business leaders. Our participant recruitment process involved a two-step approach. The first step aimed to establish an initial understanding of smart home device design, guiding the subsequent step where smart device design processes and designers are discussed and defined (cf. Section §6.4.1.1). To recruit designers and international business leaders, we advertised the study on LinkedIn, while also conducting online searches for potential candidates. Challenges in participant recruitment are detailed in Section §6.2.1, where we addressed these challenges by explaining the ethical and confidentiality measures adopted in the study to potential candidates. Additionally,

we utilized snowball sampling [443], a common technique for engaging with hard-to-reach groups [445–448].

For the recruitment of users (families and domestic workers) in Jordan, we advertised the study on specialized social media groups and reached out to smart device sellers and domestic worker recruitment agencies. To recruit local business leaders, we contacted organizations and companies in Jordan and neighboring MAME countries, identifying and inviting potential candidates. Although designers or manufacturers in Jordan and neighboring MAME countries were not found, we successfully recruited participants working in companies that import and distribute smart devices or assemble pre-designed devices originally designed in Western countries. We employed purposive and theoretical sampling methods in recruiting participants, enabling the selection of specific eligible individuals, and the sample size was determined by reaching saturation. The demographic information of all participants is presented in Table 6.1, Table 6.2, Table 6.3, and Table 6.4.

We designed five distinct semi-structured interview scripts tailored to each participant group: households, domestic workers, local business leaders, designers, and international business leaders. Applying the funnel technique [413], we structured our study scripts. Before initiating the main study, we conducted a pilot interview for each script to ensure question clarity and identify any potential errors in advance. All interviews were conducted remotely via Zoom and Facebook Messenger by the researcher. Participants provided oral consent, and interviews were audio-recorded on a standalone device. The interviews were conducted in both English and Arabic. Arabic interviews were meticulously translated by the researcher to accurately represent participants' insights without alterations.

To facilitate codebook development and theory generation, Grounded Theory, following Strauss and Corbin's data analysis method [410], was employed for the analysis of interview scripts. Similar to previous studies, NVivo 12 Pro software was utilized to facilitate coding process. To verify the reliability and credibility of the identified codebook (cf. Table 6.5), we tested for inter-rater reliability [444] and employed grounded theory triangulation [437]. The findings of the third

study are presented in Section §6.4, followed by a discussion of these findings in Section §6.5. Finally, we conclude by offering recommendations for stakeholders to address the identified challenges.

### 3.3.4 Support Bystanders Privacy Protection in the Smart Home (RQ3.3)

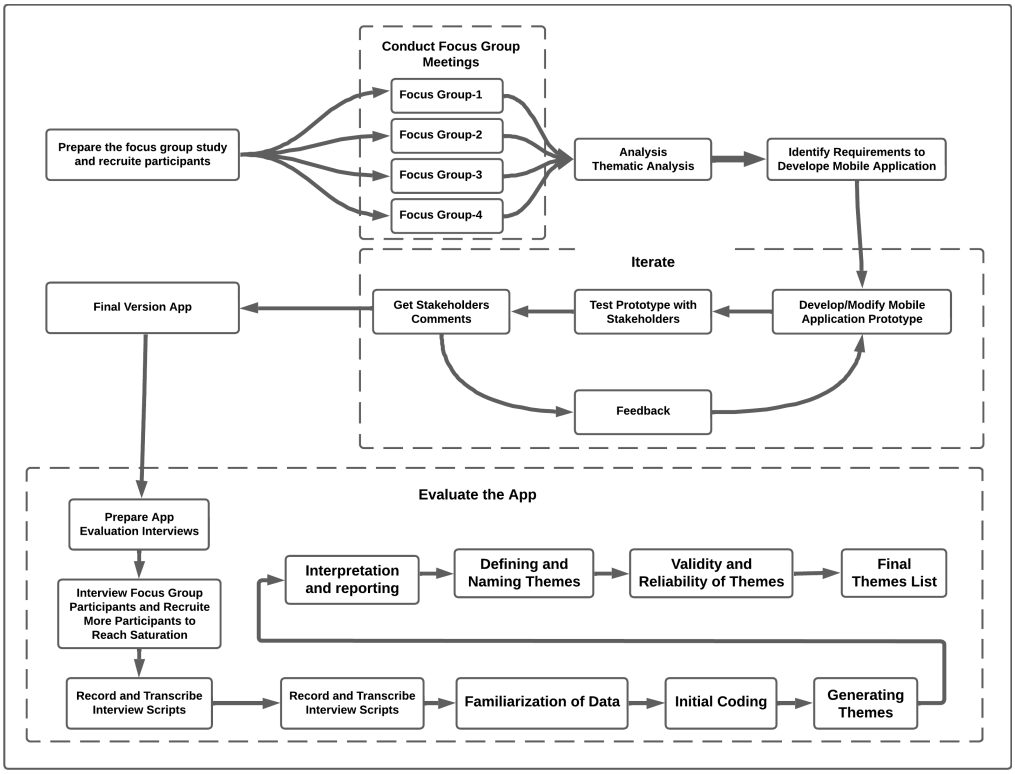
RQ3.3 aims to explore approaches for enhancing privacy protection for bystanders in smart home environments. Building upon findings from our previous studies (cf. Chapters 5 and 6), our fourth study focuses on gaining design insights into bystander privacy, co-designing a mobile application, and evaluating its feasibility as an auxiliary tool for privacy protection.

To address this research question, we conducted a two-phase study. In the first study phase, we adopted a co-design approach (cf. Figure 3.2) grounded in participatory design principles to acquire insights into bystanders' privacy. According to previous research [449, 450], a co-design approach facilitates collaboration between designers and end-users, resulting in user-centered and relevant designs. Our aim was to collaboratively design and prototype a mobile app intended to enhance privacy protection in smart homes. This involved co-designing and prototyping the app with its direct users (domestic workers and households), as well as engaging smart device designers and mobile app developers responsible for smart device design and app development.

We designed a qualitative research study utilizing focus group sessions: a total of 24 participants were involved in four focus groups, each group comprising six participants representing households, domestic workers, designers, and mobile app developers. Drawing on the outcomes of our first phase (cf. Section §7.3), and using Thunkable platform[77], we prototyped a mobile application. The app consists of several screens representing the main functionalities, including demo screens to illustrate the envisioned design and active screens that demonstrate the app's

[77]For more details, see: Thunkable platform

**Figure 3.2:** Fourth Study Approach [Co-Design Approach]




actual functionality in supporting bystanders' privacy protection (cf. Section §7.4, and Figure-7.3 for details of the app's screens).

In the second study phase, our goal was to assess and evaluate the effectiveness of the prototyped app in enhancing privacy protection for domestic workers in Jordanian smart homes. Thus, we expanded our participant pool to include individuals beyond direct users of the app, focusing on key stakeholders crucial for bystander privacy. This extended group comprised labor law and data protection regulators (regulators) and heads of domestic worker recruiting agencies (recruiters). By involving these stakeholders in the evaluation, we aimed to gain a comprehensive understanding of how the app could effectively support privacy protection in the broader context. Through qualitative research conducted via semi-structured interviews, we engaged with 26 participants, including four smart device designers, six households, seven domestic workers, four regulators, and five recruiters. Participants were introduced to the app's functionalities and encouraged to interact with it for three weeks, with an emphasis on understanding its role

in supporting privacy protection. Subsequently, following the funnel technique, semi-structured interviews were conducted to gather participants' perspectives on the app's viability and effectiveness as an auxiliary tool for privacy protection. The participants' feedback and insights informed iterative refinements to the app design, ensuring alignment with user needs and preferences.

In both study phases, we utilized purposive and theoretical sampling techniques to recruit participants, facilitating the selection of specific eligible individuals, with the sample size determined by reaching saturation. Similar to our previous studies, we recruited participants through advertising the study on social media, contacting government entities and domestic worker recruitment agencies, and utilizing snowball sampling. We discuss our research methodology in more detail in Section §7.2, and we present demographic information of all participants in Table 7.1.

Prior to conducting both the focus groups and interviews, we conducted a pilot focus group study to refine the guidance script for clarity and effectiveness. Additionally, we refined the semi-structured interview scripts with experienced researchers. Subsequently, the primary researcher conducted and recorded both the focus groups and interviews online via Zoom and Facebook Messenger, following participants' consent. The recordings were securely stored on a standalone device and professionally transcribed. While all focus groups in the first study phase were conducted in English, some of the interviews in the second study phase were carried out in Arabic. The researcher translated the Arabic interviews with utmost caution to preserve the original ideas and avoid alterations. Both study phases utilized iterative open coding [451] and Braun and Clark's thematic analysis approach [421] for codebook development, facilitated by NVivo 12 Pro. The initial codebooks underwent reliability and credibility testing, consistent with our previous studies. Detailed categories and themes from both study phases are presented in Sections §7.3 and §7.4.2. Finally, the study concludes with a discussion of findings and recommendations for stakeholders, as outlined in Section §7.5.

## 3.4 Ethical Considerations

All of our research studies were subjected to review and approval by the Central University Research Ethics Committee (CUREC) at the University of Oxford (cf. Table 3.1). Before each study, participants received information sheets outlining the study's purposes. An oral consent sheet, containing all necessary information, was presented to participants before obtaining their oral consent. We emphasized the strict confidentiality of collected data to ensure compliance with the UK Data Protection Act 1998 (registration no: Z6364106/2015/08/61). Given the sensitivity of certain interviews, especially regarding privacy, security, and compliance, participants were requested to refrain from naming specific individuals or sites, contributing to a degree of anonymity. For security, all interviews were subjected to AES 256 encryption and were securely stored in a physical safe in our institution. Participants were at liberty to skip any question, and to withdraw from the study at any point (cf. Ethics approval details in Appendix G).

**Table 3.1:** Ethics Approval Numbers

| Chapter | CUREC - Ethics Approval Number |
|---|---|
| 4 | CS-C1A-21-001 |
| 5 | CS_C1A_021_038 |
| 6 | CS_C1A_22_007 |
| 7 | CS_C1A_23_012 |

# 4

# Privacy Concerns

The purpose of this chapter is to explore the privacy concerns with smart homes for both households and domestic workers in Jordan. Specifically, this chapter addresses our first research question (RQ 1): *What are the privacy concerns of households and their domestic workers (i.e., the bystanders[1]) in the smart home in Jordan?* (see RQ1 and its sub-questions in Section §1.1.4). To investigate this research question, we conducted a qualitative study, interviewing households and domestic workers in Jordan. Through semi-structured interviews, we delved into areas such as public awareness of smart devices, worker privacy concerns, expectations, perceptions of privacy rights, and contextual influences. The study resulted in an **exploratory interview study** of how smart home devices impact privacy concerns, practices, and expectations of domestic workers and households in Jordan. Additionally, we explored the influence of contextual factors on users' privacy concerns. We present the study findings in Section §4.3, and we discuss these findings in Section §4.4. The use of the term *'study'* in this chapter refers to our first study reported in this chapter unless stated otherwise.

## 4.1 Motivation

Our motivation to investigate privacy concerns among bystanders in smart homes in Jordan arises from the findings of our exploratory literature review (cf. Chapter 2). The review reveals that smart homes pose potential privacy risks and threats into personal spaces. Previous studies have primarily focused on households and device owners in Europe and North America, acknowledging the significance of bystanders. Our literature review identified a research gap concerning bystanders' privacy concerns in non-Western contexts (e.g., MAME[14]). Therefore, our first study aimed to address this gap by examining the privacy concerns of households and domestic workers (i.e., bystanders) with smart homes in Jordan.

## 4.2 Methodology and Research Question

With approval from the University of Oxford Central University Research Ethics Committee (CUREC) [Approval: CS-C1A-21-001], we conducted semi-structured interviews with 8 families and 12 domestic workers, including nurses, caregivers, nannies, and babysitters. Figure 4.1 illustrates the research process and the applied methodology. Given the limited research on the privacy concerns of domestic workers and their employer families in non-Western contexts, we chose to employ Grounded Theory [411] as our selected data analysis method, and we used the funnel technique [413] to structure the interview scripts. Both Grounded Theory and the funnel technique are outlined further in Section §3.2.1.

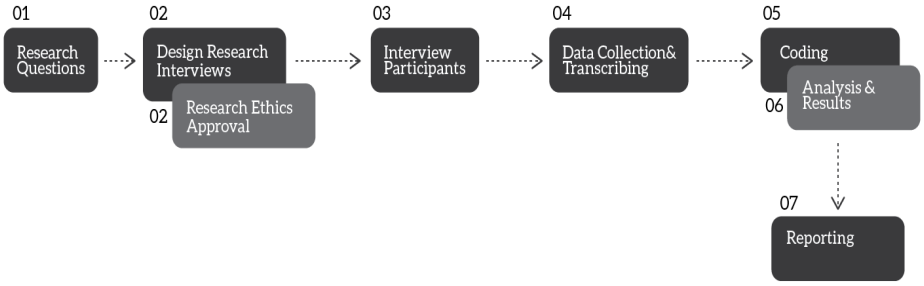
### 4.2.1 Recruitment

Similar to other qualitative research studies, we adhere to guidelines for participant recruitment in qualitative research [441, 442]. We recruited participants through various channels, including posting on specialized social media groups such as 'Babysitters Amman,' 'Babysitting in Jordan,' 'Nurses in Jordan,' and 'Ask Jordan' (cf. Appendix B.1 for sample of the posts). Additionally, we reached out to recruitment agencies, contacted smart device sellers directly, and utilized snowball

sampling[443] after candidates agreed to share their contact details. Volunteers were requested to complete a demographic and basic information survey (cf. Appendix B.2 for details of the screening survey), which included a general study description. Participants who expressed interest provided details such as age, gender, education level, used smart devices, experience with smart homes, employment specifics, marital status, and whether they were employers or domestic workers. Contact details were also collected for future communication with the researchers. 27 candidates filled the survey. After screening the survey results, we identified 20 eligible participants who met our criteria:

- Age should be over 18 years;
- To have a basic knowledge of smart homes devices;
- To be able to communicate either in English or Arabic languages;
- To consent to participating in the interviews and to being audio-recorded;

**Figure 4.1:** First Study Research Process and Methodology




We successfully recruited and interviewed 8 individuals from various employer families and 12 workers from different households. In the interview transcripts, we refer to workers and families as PE and PW, respectively (e.g., PE01 for family number 1 and PW01 for worker number 1). To prevent potential negative effects from socio-economic power dynamics and to encourage open communication, we deliberately avoided including workers and family members from the same

**Table 4.1:** Demographic Information of Participants

| Domestic Workers | | | Families | | |
|---|---|---|---|---|---|
| **Characteristics** | **Number** | **%** | **Characteristics** | **Number** | **%** |
| Workers | 12 | 60% | Families | 8 | 40% |
| Living with the family | 5 | 42% | Living with the family | 5 | 62.50% |
| Not living with the family | 7 | 58% | Not living with the family | 3 | 37.50% |
| **Age** | | | **Age** | | |
| 18-34 Years | 10 | 83% | 18-34 Years | 4 | 50% |
| 35-64 Years | 2 | 17% | 35-64 Years | 4 | 50% |
| **Gender** | | | **Gender** | | |
| Male | 2 | 17% | Male | 5 | 62% |
| Female | 10 | 83% | Female | 3 | 38% |
| **Job Type** | | | **Hired Worker** | | |
| Nanny/Babysitter | 6 | 50% | Nanny/Babysitter | 4 | 50% |
| Nurse | 5 | 42% | Maid | 3 | 37.50% |
| Elderly Care Givers | 1 | 8% | Elderly Care Givers | 1 | 12.50% |
| **Used Smart Devices** | | | **Used Smart Devices** | | |
| Smart Cameras | 12 | 100% | Smart Cameras | 8 | 100% |
| Smart Speakers | 11 | 91% | Smart Speakers | 6 | 75% |
| Smart Lights | 3 | 25% | Smart Lights | 3 | 37% |
| Smart Windows | 2 | 16% | Smart Windows | 1 | 12% |
| Security Systems | 12 | 100% | Security Systems | 6 | 75% |
| Smart Systems | 2 | 16% | Smart Systems | 1 | 12% |
| Smart Home Appliance | 7 | 58% | Smart Home Appliance | 5 | 62% |

households. All eligible participants were contacted to schedule an online interview, which was conducted using Zoom and Facebook Messenger. Standalone recording devices were employed to audio record the interviews.

Prior to conducting interviews with the workers, we explicitly asked them to select locations outside the houses where they work and avoid using the internet infrastructure of their employers' houses. This measure was implemented to ensure that the workers did not feel pressured during the interviews. Table 4.1 provides the individual characteristics of all participants, including job status, technology background, and experience with smart home devices. It is important to note that the workers' reported smart devices may not be entirely accurate, as they may not be aware of all the installed and used smart devices in the home.

### 4.2.2 Interviews

We designed semi-structured interviews using Grounded Theory [411], guided by insights from our literature review (cf. Chapter 2) to identify key topics. Prior to the main interviews, four pilot interviews were conducted to assess question clarity, and adjustments were made accordingly. These pilot interviews were excluded from the

research study analysis. All 20 interviews were transcribed and analyzed using the Grounded Theory procedure [414], complemented by the application of the funnel technique [413] as outlined in Section §3.2.1. This approach ensured a comprehensive exploration of bystanders' privacy concerns in smart homes, providing insights into both rational and irrational aspects of people's behaviors and attitudes [452]. (cf. Appendix B.3, and Appendix B.4 for interview guideline details).

At the beginning of each interview, we described the research topic and sought participants' permission to start and audio record the interview. We assured confidentiality and informed participants that all identifiable information would remain confidential, not shared with any party, and deleted after transcript analysis. Interviews lasted between 30 to 91 minutes, averaging 41 minutes overall, 35 minutes for workers, and 52 minutes for families. Starting with general questions about participants' backgrounds, experiences, perceptions of smart home devices, and relationships between families and workers, we proceeded to more detailed questions, ensuring minimal interruption and avoiding influence on participants or their responses.

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

### 4.2.3 Analysis

After transcribing the interviews, we employed an inductive grounded theory approach to analyze the transcripts. The trained primary researcher conducted, transcribed, and translated the interviews, initiating the initial coding of all transcripts. Subsequently, two researchers grouped the codes into themes (axial coding) and categories (selective coding). Data saturation [419] was observed between the 19th and 20th interviews, where no significant new codes emerged.

After completing our preliminary analysis, we conducted tests on the codes and themes to ensure the reliability and credibility of the generated codebook. We cross-checked the codes with the interview transcripts and reviewed the initial coding, resolving any discrepancies through discussion until a final codebook was established (cf. Table 4.2). Additionally, we calculated the inter-rater reliability, obtaining an average Cohen's kappa coefficient ($\kappa$) of 0.86 for all codes in the data, indicating near perfect agreement [438]. Furthermore, we tested the identified codebook's reliability and credibility using the grounded theory triangulation method. Seven participants (4 workers and 3 families) were randomly selected, and they provided comments on the generated codes and themes, confirming their agreement with the analysis output. While some additional codes emerged during the verification process, they did not introduce new themes and were linked to existing themes.

### 4.2.4 Research Ethics

This study received approval from the University of Oxford Central University Research Ethics Committee (CUREC) [Approval: CSC1A21001]. Participants provided oral consent to be interviewed and audio recorded, and we assured them that their data would be handled with strict confidentiality. Interview scripts were encrypted and stored securely. Participants had the right to withdraw from the study at any point without providing an explanation, and we assured them that their data would not be used if they chose to withdraw. No participants withdrew from the study. Finally, as previously mentioned, to ensure the confidentiality, safety, and freedom of participation for domestic workers, we advised them to schedule and participate in online interviews from locations outside their workplace or refrain from using the internet infrastructure of their workplace (the home). Additionally, we ensured that we did not recruit both workers and family members from the same households simultaneously. For details of the ethics application, refer to Appendix G.1.

### 4.2.5 Limitations

The interviews were conducted in both English and Arabic. While 18 participants (12 in English and 6 in Arabic) were comfortable expressing themselves in either language, two participants faced challenges communicating in both languages, and we made an effort to engage with them primarily in the language they feel more comfortable with, among English and Arabic. Due to the communication difficulties encountered, there is a possibility that we may have missed some insights regarding privacy concerns, power dynamics, user agency, and other related issues from these two participants. Apart from language barriers, our participants lack a strong awareness of smart devices, data handling, data security, and privacy issues in smart homes. Consequently, they were unable to provide detailed answers to several more specific topics. Moreover, despite ensuring the utmost confidentiality for participants in this study, we believe that some workers might not feel secure enough to provide detailed answers about their privacy concerns and the issues they face in the homes they work in. This hesitation could be attributed to imbalanced power dynamics and the fear of creating conflicts with their families in case such information is revealed.

In alignment with other qualitative exploratory studies, our findings represent the perspectives of our 20 participants and cannot be generalized to a broader population. The applicability of these findings to wider populations is a subject for future research.

## 4.3 Findings and Results

The chapter presents the study findings on the privacy concerns of domestic workers and employer families in Jordanian smart homes. Employing the Grounded Theory approach, we identified 220 codes, organized in the codebook outlined in Table 4.2. The study unveiled five key themes: a- Limited public awareness of smart technologies, b- Privacy concerns and expectations, with cameras emerging as the most concerning devices, c- Perceptions of privacy rights and expectations, emphasizing the lack of explicit privacy regulations in Jordan, leaving workers with

limited options and subject to asymmetric power dynamics with their employers (i.e., families), d- Contextual influence on privacy concerns, practices, and rights, and the e- Aspirations for new innovative privacy control features.

As depicted in Figure 4.2, and based on the findings of this study. We identify the following associations between the identified themes: 1- Limited public awareness about smart devices leads to the oversight of associated privacy rights, contributing to blurred privacy concerns about smart technologies; 2- Contextual influences impact privacy concerns, practices, and expectations, fostering a positive perception of privacy protection and rights; 3- Users' aspirations for privacy control introduce new security and privacy concerns, coupled with expectations for enhanced privacy protection features in smart home devices. The following sections provide detailed insights into the identified themes.

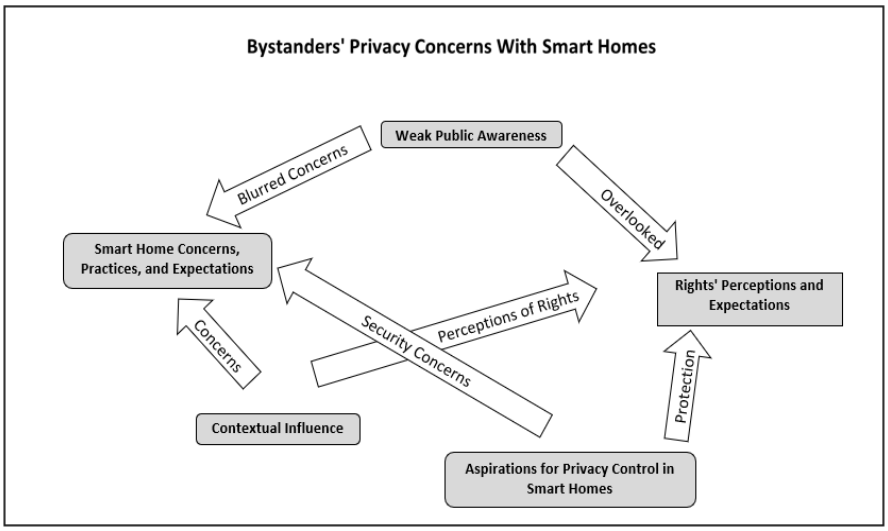
**Table 4.2:** Summary of Themes and Codes

| No | Themes | Sub-Themes |
|---|---|---|
| 1 | limited Public Awareness | limited Public Awareness of Smart Homes |
| | | Weak Competence of Managing Smart Devices |
| | | Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies |
| 2 | Smart Home Privacy Concerns, Practices, and Ex-pectations | People are Mostly Concerned about Audio/Visual Data Collection |
| | | Impact of the Workers on Family's Privacy |
| | | Smart Devices Drive Workers to Adopt Disciplined Practices |
| | | Workers Should Respect the Rules of the Blended Context of the Home |
| | | Family Members or Vendor Staff Manage Smart Devices, and Collected Data |
| | | Families Presume Workers are Aware of Existing Devices |
| | | Perception of Distrusting Workers |
| | | Families Do Not Inform Workers About Devices |
| | | Families Have Concerns with Informing Workers about the Smart Devices |
| 3 | Rights Perceptions and Expectations | Family's Autocracy |
| | | Perception of Disrespecting Workers' Privacy Rights |
| | | Perceptions of Privacy Rights |
| | | Lack of Explicit Privacy Rights and Policies in Jordan |
| | | Power Dynamics and User Agency |
| | | Trust Vendors' Privacy Policies |
| 4 | Contextual Influences | Religious Background and Social Norms Drive Positive Privacy Practices |
| | | Contextual Influences Influence Privacy Concerns, Practices, and Rights |
| | | Religious Background is Presumed to Ensure Privacy Rights |
| 5 | Aspirations for Privacy Control | To Improve and Ensure Awareness of Smart Devices in the Home |
| | | Novel Applications Could Utilize Recognition Technologies |
| | | Concerns With Novel Applications |

### 4.3.1 Limited Public Awareness

We identified limited levels of knowledge, skill, and awareness of smart technologies, further categorized into the following sub-themes.

**Figure 4.2:** Visual Representation of Themes and Codes




#### 4.3.1.1 Limited Public Awareness of Smart Homes

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

When we asked participants about how they understand privacy in the smart home, most of them said that it is mainly about audio and/or video recording them while they are inside the home, and none mentioned other types of data the smart devices might be collecting about them (e.g., attendance patterns, daily activities, personal habits, voice print, etc.) [453].

#### 4.3.1.2 Weak Competence of Managing Smart Devices

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

#### 4.3.1.3 Limited Role of Recruitment Agencies in Raising Awareness About Smart Technologies

We found that participants use recruitment agencies to help them with their recruitment and employment needs, and when we asked participants whether recruitment agencies or public organizations provide any information about smart devices, most said that agencies do not provide any kind of information. Two participants mentioned that agencies had informed them that the homes they are going to work in might have smart devices like cameras and smart speakers without giving them additional details. Some participants mentioned that sometimes the recruitment poster mentioned that the home has smart devices. Additionally, it was interesting to note that some domestic workers share information on specialized social web pages about the homes they have worked for before, thus, new workers could know whether the homes they are going to work in have smart devices or not, and what type of devices are used. PW12 said: *" Not exactly, but they told us that there will be smart devices in the homes that we will be working in, and in some cases when I get my job directly through an advert, some times that advert says*

*clearly that there are cameras or smart devices, and on the other side, we -as a group of care givers- we tell each other about the homes that we have worked in before, and whether they use smart devices or not, so the worker who will be going to that home, will be aware of the smart devices, and will take care and behave in good manner".*

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

### 4.3.2 Smart Home Privacy Concerns, Practices, and Expectations

We identified several privacy concerns, practices, and expectations with the smart home in Jordan.

#### 4.3.2.1 People are Mostly Concerned about Audio/Visual Data Collection

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

about privacy concerns, and it is likely that the question was interpreted as "what kind of privacy concerning devices are most used in the home".

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

#### 4.3.2.2 Impact of the Workers on Family's Privacy

Both families and workers emphasized that the presence of domestic workers in the home has a noticeable impact on family privacy. PE07 said: *"Of course. The presence of domestic workers in the home is squeezing our privacy, and sometimes we do not feel comfortable about that situation."* This highlights the shared acknowledgment of the influence domestic workers can have on the privacy dynamics within households. This sentiment emphasize the complex interplay between domestic work and the perception of privacy, shedding light on the multifaceted dynamics within households.

#### 4.3.2.3 Smart Devices Drive Workers to Adopt Disciplined Practices

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

#### 4.3.2.4 Workers Should Respect the Rules of the Blended Context of the Home

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

#### 4.3.2.5 Family Members or Vendor Staff Manage Smart Devices, and Collected Data

When we asked participants about who controlled the smart devices and managed the collected data, families said one or more of the family members do. Workers said they do not know exactly who does that, but they think that one of the family members does. PW06 said: *"The family do".* Some participants said the device vendor's employees might do as well. PE01: *"According to amazon privacy rights, it is only us and amazon developers after we grant them our permission to do so."*

#### 4.3.2.6 Families Presume Workers are Aware of Existing Devices

When inquiring about families informing workers about smart devices, some families expressed an assumption that workers are already aware of these devices within the household. PE03 expressed this perspective, stating, *"No, she has to know because everything is in the house."* This response reflects a common expectation among families regarding the workers' familiarity with the smart technology present in their homes.

#### 4.3.2.7 Perception of Distrusting Workers

Some workers shared the perspective that the lack of disclosure regarding smart devices is a clear sign that families distrust them. PW12 said: *"Because they do not trust us as a stranger in the house, as they do not know us, they want to be*

*more careful about their families and homes."* This insight shows the connection between transparency about smart devices and the perception of trust within the employer-worker relationship.

#### 4.3.2.8 Families Do Not Inform Workers About Devices

The analysis reveals a pattern where certain families do not inform their domestic workers about smart devices. PE03 said: *"We did not inform her."* This finding shows the variations in communication practices among families, adding nuance to the dynamics of smart technology disclosure within domestic environments.

#### 4.3.2.9 Families Have Concerns with Informing Workers about the Smart Devices

When we asked families about the reasons that prevent them from informing the workers about the smart devices, some families expressed concerns about potential consequences, citing fears of job resignation or creating conflicts when workers become aware of the devices. PE03 said: *"Yes, maybe she will break some of them or create a problem; she may misuse them."* This insight sheds light on the perceived risks that influence families' decisions regarding disclosure, providing a nuanced understanding of their reservations.

### 4.3.3 Rights Perceptions and Expectations

The following theme describes how privacy rights in Jordan are perceived by our participants.

#### 4.3.3.1 Family's Autocracy

The analysis has shown that some families have an autocratic attitude concerning what should happen inside their homes, as these families think that their home is their own territory where they can do whatever they wish. Those families think that they do not have to inform workers about smart devices that are collecting data about them, nor do they need to request workers permissions to monitor and record them. PE05 said: *"It is my home, my territory, and the worker is coming*

*to live with me or to visit me, she has to adapt to my rules. Her privacy should not affect my desire to feel secure in my home".*

#### 4.3.3.2 Perception of Disrespecting Workers' Privacy Rights

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

#### 4.3.3.3 Perceptions of Privacy Rights

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

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

unclear whether and under what circumstances an employee could gain access to a recording on an employers' device.

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

#### 4.3.3.4 Lack of Explicit Privacy Rights and Policies in Jordan

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

#### 4.3.3.5 Power Dynamics and User Agency

The analysis has shown the power dynamics between employers and workers are such that workers frequently give up their privacy rights in favor of other perceived benefits, such as safety, security, convenience, and to retain their jobs. PW09 said: *"Sometimes, I agree with families on not using the cams, and sometimes they do not accept. In the end I have to adapt as this is my job".* This is consistent with what Flechais and Kraemer [248] have discussed in their work on smart home families, where power dynamics and user agency [454] strongly influence awareness of how devices work, competence levels, and gaining permission to access the devices. Our finding also aligns with the work of Geen et al. [210], who found that power imbalances among smart home users reduce user agency.

#### 4.3.3.6 Trust Vendors' Privacy Policies

When we asked participants about whether they trust vendors' privacy policies, they expressed a broad sense of trust. PE01 said: *"As per Amazon, privacy is protected. But Alexa is turned on 24/7, and I have my doubts that Alexa can listen to us without our knowledge"*. This response highlights a nuanced perspective, revealing underlying uncertainties that coexist with the overall trust in vendor policies.

### 4.3.4 Contextual Influences

Jordan's Moderate Religious background, social norms, and customs have influenced privacy concerns, practices and rights.

#### 4.3.4.1 Religious Background and Social Norms Drive Positive Privacy Practices

We found that the religious background, social norms, and customs of Jordan were raised as motivating some positive privacy practices such as urging families to treat workers well. PE05 said: *"Yes. I am religious person, I believe, I must inform her and respect her privacy"*. When we asked participants about the differences between visitors and domestic workers in their homes, and whether they would inform them about the installed smart devices. Some participants demonstrated a clear difference in the standing of workers and guests, saying that they would not inform workers, but they would inform visitors. This was because they felt that the social dynamics involved with having visitors would drive them to inform visitors about smart devices and also to respect visitors' privacy rights. PE04 said: *"The visitor may become upset if we do not tell him, but the worker is paid to do his job and he must accept that we are protecting our home"*.

#### 4.3.4.2 Contextual Influences Influence Privacy Concerns, Practices, and Rights

We found that some privacy concerns are influenced by the religious background of the person, like for example, some female workers mentioned that they do not accept to be monitored, or video recorded without their hijab[22]. PW01 said: *"It does not*

*feel good that they [the family] may see me when I change my clothes, or take off my hijab so I need to be careful."*. This insight emphasizes the intersection of privacy considerations with cultural and religious values, adding a layer of complexity to the understanding of privacy dynamics in smart homes.

#### 4.3.4.3 Religious Background is Presumed to Ensure Privacy Rights

We have found that many participants believe that Islam ensures privacy rights, that a committed Muslim person will adhere to Islam's statutes and will respect privacy of others, and that Islam also urges people to build good relationships with others and to trust each others. PW03 said: *"The family always tells me, they are religious people, and will not hurt me"*, and PE07 said: *"We can not hide devices from her, it is forbidden in our religion"*. These statements highlight the connection of religious values with privacy considerations, reinforcing the role of religion in shaping perspectives within smart home environments.

### 4.3.5 Aspirations for Privacy Control

We found that participants had a number of hopes and aspirations for more innovative privacy control features.

#### 4.3.5.1 To Improve and Ensure Awareness of Smart Devices in the Home

When asked about the potential of novel technology to enhance the design of smart devices and raise awareness of existing ones to protect bystanders' privacy in smart homes, participants articulated a wish-list of privacy control features aimed at protecting individuals' privacy. PE02 said: *"Maybe we can use a secret word or something like that and maybe a mechanism to ask the device owner whether to record the new user or not, or through facial gestures, I mean through a certain mechanism"*.

#### 4.3.5.2 Novel Applications Could Utilize Recognition Technologies

Some participants mentioned that recognition technologies could be used to improve the design of smart devices to help people enjoy the smart devices benefits, and to protect privacy at the same time by excluding identified bystanders from data

collection or use. PE01 said: *"I think by using voice recognition, and facial recognition"*. This perspective emphasizes the belief in the positive impact of innovative technologies in addressing privacy concerns through selective data collection and usage exclusions for identified individuals.

#### 4.3.5.3 Concerns With Novel Applications

Some participants mentioned that new privacy protections could jeopardize the safety, security, and privacy of people in the smart home. PE01 said: *"No, they may hide themselves from the devices, and conduct crimes, and they should not be given any ability to hide themselves from the devices. I think this may jeopardize the home security"*. This perspective highlights the delicate balance between privacy protections and maintaining a secure environment within smart homes, adding a nuanced dimension to the issue.

## 4.4 Discussion and Recommendations

### 4.4.1 Summary of Findings

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

The findings and recommendations of this study resonate with the outcomes of prior research studies [2, 178, 184, 187, 192, 455], which have shown limited public awareness of smart technologies and the implications on people's privacy, the exigent demand for privacy research to address non-Western contexts—specifically Muslim contexts, and the roles of policymakers and public awareness entities in improving the privacy protection of smart home bystanders. Despite the fact that this study

focuses on Jordan, we believe that the elicited outcomes and recommendations could be applicable to some extent to other contexts in the MAME region where they share similar social norms, customs, and religious background. However, future research addressing other MAME contexts is needed to either confirm the outcomes of this study and/or present new findings and recommendations.

### 4.4.2 Recommendations for Public Awareness

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

We believe that improving awareness of smart technologies among the population would help individuals mitigate privacy threats and enhance privacy protection. It would also facilitate privacy-related discussions between employers and workers to resolve conflicts and mitigate the impacts of family autocracy. By explicitly raising awareness of the privacy rights of domestic workers, this approach may help address the asymmetric power dynamics between these different groups.

### 4.4.3 Recommendations for Policymakers

It is important to note that, at the time of conducting this study, the new data protection law[55] in Jordan had not been officially announced. However, as discussed in Section §2.2.5.2, the newly announced data protection law in Jordan lacks explicit privacy regulations for smart home users. This regulatory gap exposes smart homes to asymmetric power dynamics between families and workers and also limits user

agency, given the lack of clarity around what is deemed acceptable. We recommend that policymakers and concerned entities specifically address bystander privacy concerns in regulations in Jordan and consider leveraging social norms during the development and update of future regulations.

Another pertinent legislation is the Jordanian labor law [456], which lacks specific articles addressing work in smart spaces and the privacy rights of workers in such environments. It only mentions the unacceptable practices of installing cameras or audio devices in sensitive locations such as bedrooms and toilets, providing no clear guidance on whether smart homes are considered domiciles or workplaces. Finally, while the role of religion in setting policy goals is debated, it is important to note that the religion of Islam [186, 187] is being used to justify certain privacy attitudes and practices. Islam places a strong emphasis on the importance of human rights in supporting the well-being and personal growth of every individual in civilized societies. Norwawi et al. [187] argued that the human rights recognized in modern constitutions[15], charters, and international treaties are embedded in the religion of Islam, as respect for life, privacy, freedom, equality, property, and religious belief are essential features of Islam. Based on the above discussion, Muslim societies, in general, are expected to respect privacy rights.

### 4.4.4 Recommendations for Smart Device Designers

Our participants expressed a desire for more innovative privacy controls and features, including the adoption of visual and/or audio recognition technologies (such as facial gestures and hand movements), different privacy modes, smart privacy settings, visual and/or audio alerts, and the incorporation of new features based on Artificial Intelligence technologies (AI). These advancements aim to reduce associated risks to the privacy of different user groups and enhance user agency in smart homes. They propose making smart devices discoverable, notifying users of their actions, and requesting permissions wherever applicable.

These aspirations highlight the need for greater innovation and contextual awareness in designing smart devices. The specific desires of workers and families

in Jordanian smart homes serve as valuable inspiration for innovations that could be applicable to a wider Middle Eastern context.

## 4.5 Conclusion

In this chapter, we explore the impact of smart devices on the privacy of domestic workers (bystanders) in smart homes within the non-Western context of Jordan. To achieve our research objective, we conducted a semi-structured interview-based study involving 20 participants (households and workers) in Jordan. Our study provides an exploratory analysis of how smart home devices influence the privacy concerns, practices, and expectations of domestic workers and households in Jordan. Additionally, we investigate the influence of contextual factors on users' privacy concerns within the realm of smart homes in Jordan. Finally, we present the key findings derived from our study and discuss their implications.

# 5

# Smart Home Power Dynamics

The purpose of this chapter is to examine the impact of socio-economic power dynamics on privacy concerns and practices within Jordanian smart homes, addressing our second research question, RQ.2: *"How do socio-economic power dynamics affect the privacy of households and domestic workers (i.e., bystanders[1]) in Jordanian smart homes?"* (see RQ2 and its sub-questions in Section §1.1.4). To tackle this research question, we conducted qualitative semi-structured interviews with key stakeholders, exploring how these power dynamics influence privacy concerns and practices among households and domestic workers. Our investigation extends to understanding the impact of smart devices on household-worker relationships and exploring the current state of data protection regulations in Jordan

In Section §5.2, we outline our research approach, involving semi-structured interviews with 30 participants. Moving to Section §5.4, we present the study's findings. This study resulted in an **examination study** of the socioeconomic power dynamics between households and their domestic workers in smart homes in Jordan, and how these dynamics, shaped and influenced by contextual factors such as norms, customs, religious backgrounds, and economic status, affect the quality of relationships (e.g., trust and respect) between households and their workers. It also investigates how smart technologies impact and reinforce these power dynamics, as well as how these dynamics and contextual influences influence

users' privacy concerns in Jordanian smart homes. Detailed findings are discussed in Section §5.5. The use of the term *'study'* in this chapter refers to our second study reported in this chapter unless stated otherwise.

## 5.1 Motivation

Our interest in exploring power dynamics in smart homes is rooted in the insights gained from our literature review (cf. Chapter 2) and the findings of the first study (cf. Chapter 4). The first study revealed concerns about privacy protection for both households and bystanders, who navigate complex power dynamics within smart homes and may become susceptible to exploitative practices facilitated by smart technology. These power dynamics are shaped by intricate social norms, customs, religious beliefs, and economic factors. As previously mentioned, there has been limited exploration in non-Western contexts, such as MAME[14] contexts like Jordan, and this chapter aims to contribute to filling this gap.

## 5.2 Methodology

This chapter presents the outcomes of a qualitative study that addresses our second research question outlined in Section §1.1.4. Following established approaches in previous qualitative research [7, 144], we conducted a user study utilizing semi-structured interviews. The aim was to explore how smart devices affect, reinforce, and reflect power dynamics between households and their domestic workers in Jordan, as well as the potential role of regulation in mitigating any adverse implications of smart home devices on affected populations. To gain insights into these topics, we interviewed households and domestic workers, and participants involved in policy making: ICT regulators, labor law experts, and human and civil rights activists. Through these interviews, we sought to understand how smart devices could either reinforce or alleviate power dynamics within smart homes, as well as how regulation could address any adversarial effects of smart home devices on households and bystanders in Jordan.

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

### 5.2.1 Recruitment

Similar to our first study, we adhere to guidelines for recruiting participants in qualitative research studies [441, 442]. We developed a screening questionnaire to identify potential candidates meeting our criteria, which encompassed a minimum age of 18 years, a minimum of two years of experience in their role, a basic understanding of smart devices, and a willingness to engage in interviews and audio recording. The structure of our screening questionnaire survey is detailed below (For details of screening questionnaire, refer to Appendix C.2):

- For all participants, it is required to be above 18 years old.
- For Households. Minimum of two years experience with smart home device.
- For Domestic Workers: Minimum of two years of experience working in smart homes.
- For Regulators. Minimum of two years experience with data protection regulation.
- For Labour Law Experts. Minimum of two years experience with labour law.
- For Activists. Minimum of two years of being active in this domain.
- For all candidates, to consent to participating in the interviews and being audio recorded.

As part of our recruitment strategy, similar to our previous study (cf. Chapter 4), we advertised the study to recruit households and domestic workers in Jordan through social media groups (cf. study posters in Appendix C.1), reached out to smart device sellers and domestic worker recruitment agencies, and used snowball sampling. We established connections with 12 candidate households and 12 candidate domestic workers. The competence of households and workers in using smart devices was assessed based on Dreyfus' model of skill acquisition [457], which categorizes competence levels as Novice, Competent, Proficient, and Expert. To recruit regulators (i.e., ICT and labor) and human and civil rights activists, we contacted entities from both the private and public sectors in Jordan, including ICT companies and mobile operators, The Ministry of Digital Economy and Entrepreneurship (MODEE[54]), Jordan Telecom Regulator Commission (TRC[78]), Intaj[79], and JOSA[80]. Recruiting regulators and activists posed challenges due to the sensitivities associated with data protection regulation [458]. Data protection can be considered a taboo topic in many private and public entities [459]. To overcome these challenges, we briefed participants about our ethical, security, and privacy measures, and we employed snowball sampling [443], a method commonly used to recruit participants from hard-to-reach groups [445]. This approach allowed us to reach 11 ICT regulators, six labor law experts, and nine activists. In total, we established connections with 50 candidates, including 12 households, 12 domestic workers, 11 ICT regulators, six labor law experts, and nine activists.

We initiated contact with all 50 candidates through email and phone to request and coordinate interviews. Out of these, 38 individuals expressed interest and completed our screening questionnaire. Subsequently, we successfully recruited a diverse group of 30 participants, including seven household heads, eight domestic workers, seven ICT policymakers, three labor law experts, and five human and civil rights activists. Together, they collectively represents 15 households, two ICT companies, three government entities, two civil rights organizations, and

[78]TRC: Jordan Telecom Regulator Commission
[79]INTAJ: The Information and Communications Technology Association
[80]JOSA: Jordan Open Source Association

two independent activists. (For participant demographics, refer to Table 5.1, Table 5.2, and Table 5.3).

To prevent potential harm or ethical concerns and ensure the freedom of participation for domestic workers, we took measures to avoid recruiting workers and family heads from the same households. For other participants, such as policy makers and activists, we did not exclude individuals who might be connected.

**Table 5.1:** Demographic Information of Domestic Workers

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

**Table 5.2:** Demographic Information of Households

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

**Table 5.3:** Demographic Information of Policy Makers & Activists

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

### 5.2.2 Methodology and Interviews

To address the research question, we conducted semi-structured interviews with 30 participants from July 2022 to November 2022. The study scripts were structured using the funnel technique [413] (cf. Section §3.2.1). By initially asking broad questions and progressively delving into specifics, the interviewer ensures comprehensive coverage of relevant topics without overwhelming the interviewee with excessive details at the beginning.

Grounded Theory [410, 414] was selected as the primary research methodology due to its suitability for investigating domains with limited prior exploration as explained in Section §3.2.1. We conducted all interviews remotely using Zoom and Facebook Messenger, which we audio-recorded with the participants' oral consent. The primary researcher conducted the interviews in English and Arabic – 23 interviews in English, and seven interviews in Arabic. The recruitment advertisement (cf. Appendix C.1) clearly requested volunteers to assist with this study, and our participants were happy to volunteer without compensation.

#### 5.2.2.1 Pilot Study

Pilot interviews were conducted for all semi-structured interview scripts (households, domestic workers, activists, and regulators). These interviews aimed to ensure the clarity of the questions and identify any issues in the interview scripts in advance. No significant alterations were made to the interview scripts following the pilot interviews.

#### 5.2.2.2 Interviews

The study included interviews with households, domestic workers, regulators, and activists about the use of smart home devices, their impact on privacy, privacy concerns, and data protection regulation in Jordan. The households were asked about the type and use of smart devices, their relation with domestic workers, and their understanding of data protection laws. Domestic workers were asked about their relation with households, their understanding of data protection rights,

their use of smart devices, their privacy concerns and practices, and whether they can enforce their privacy preferences and why. Both regulators and activists were asked about the impact of smart devices on privacy, data protection regulations in Jordan, and how to mitigate the adversarial implications of smart devices. To avoid response bias[460], we started the interviews with general questions, and gradually narrowing the focus to ensure coverage of all relevant topics without influencing the responses of the interviewees. (cf. Appendix C.3, C.4, C.5, and C.6 for the interview question guidelines).

#### 5.2.2.3 Data Analysis

Similar to our approach in the first study, and following Strauss and Corbin's Grounded Theory [410, 411], we transcribed and analyzed the 30 semi-structured interview scripts using NVivo 12 Pro[76]. The primary researcher translated the Arabic interviews, taking utmost care to represent the participants' insights during the translations without any kind of alterations or changes to the participants views and insights.

We conducted the initial coding of the interview scripts. Throughout the coding process, we engaged in discussions, seeking clarifications, insights, and additional data. We also annotated the study scripts to provide further context and information. A total of 187 codes emerged from the initial coding. These codes were then applied to the remaining interviews through regular comparisons, and new codes were added where necessary. Subsequently, we grouped the codes into themes (axial coding) and categories (selective coding) based on the dimensions and properties of each theme. Data saturation (where new data no longer provides significant additional insights) was separately observed for all three participant groups [414, 419].

To verify the credibility of the codebook, we cross-checked the codes against the interview transcripts. We tested for inter-rater reliability and found that the average Cohen's kappa coefficient ($\kappa$) for all codes was 0.88, indicating near perfect agreement[438]. We also tested the findings for reliability and credibility using triangulation [437] by randomly selecting seven participants (two households, two

workers, one regulator, one labour law expert, and one activist) and asked them to comment on the codes and themes. All participants agreed with the identified categories and themes, and their comments enabled us to identify some additional insights but did not generate new themes. In total, we identified 211 codes which we organised into the categories and themes presented in Section §5.4.

#### 5.2.2.4 Research Position and Ethics

Our research focuses on power relationships and their impact on technology use. We consider our positionality [461] and its potential influence on participants and research outcomes. Our overarching research question explores the implications of power dynamics on technology use, particularly regarding ethical values such as freedom, fairness, and accountability. However, we took precautions to ensure that our views did not bias the research process. These precautions included framing our interview guide to avoid leading questions, positioning the study as an exploration of privacy and interpersonal implications of smart technology, and employing two coders to analyze and cross-check the data. We also prioritized preserving the anonymity and privacy of our respondents, while remaining vigilant for any evidence of illegal treatment (which we did not find). As our research is exploratory, we maintained a neutral standpoint and focused on reporting rather than intervening when evidence of potential unfair technology use arose. This research area poses challenges, and future studies may uncover additional instances of exploitation or unethical situations, necessitating standardized research strategies and protocols to identify, assess, and address such issues. We acknowledge the limitations of our study, including the potential influence of our own biases on the results. Despite these limitations, we have confidence in the validity of our findings. To ensure ethical considerations, our study received approval from the University of Oxford Central University Research Ethics Committee (CUREC) [Approval: CS_C1A_021_038]. Participants provided oral consent, and we assured them that their data would be handled with strict confidentiality. Interview scripts were encrypted and stored securely. Finally, participants had the right to withdraw from the study at any

point without providing an explanation, and we assured them that their data would not be used if they chose to withdraw. No participants withdrew from the study. For details of the ethics application, refer to Appendix G.2.

## 5.3 Limitations

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

1) We conducted all interviews in English, except for seven interviews that were conducted in Arabic with participants who were unable to communicate in English. Those interviews were translated carefully, but it is possible that some nuances were lost as a result of the language barriers.

2) Qualitative research depends on researchers' skills, and can be influenced by their personal biases [462]. To address this limitation, the primary researcher is a trained researcher on designing and conducting interviews to avoid influencing interviewees, and we outlined our positionality in Section §5.2.2.4.

3) Self-reporting bias is common in interview research studies [463]. Qualitative research commonly faces Self-Reporting Bias [463], causing participants to forget details or provide inaccurate responses. Participants might adjust answers based on their perception of researchers' viewpoints, introducing bias [464]. To enhance validity and minimize self-reporting bias, open-ended questions were employed, avoiding leading ones to encourage comprehensive answers. Concise responses prompted follow-up inquiries for additional information.

4) This qualitative research study is limited by the size and diversity of recruited sample.

5) Due to sensitivity of the study topic, participants might have biased their answers due to different concerns they might have. To mitigate this, we explained to the participants about our security and privacy measures, focusing on how we will encrypt collected data and process it.

6) Similar to other qualitative studies, our findings reflect the understanding of our 30 participants and are not generalisable to a wider population. Instead, the focus of such explorations is in gaining a greater understanding of the deeper

issues and concerns, and how they relate to one another. Exploring how these findings are generalisable is the subject of future work.

## 5.4 Results and Findings

This section presents the findings of our study into smart home power dynamics in Jordan. We present and discuss the findings under two main categories: 1- Smart Home Power Dynamics (cf. Section §5.4.1), and 2- Perspectives on Mitigating Smart Home Power Dynamics (cf. Section §5.4.2). Some of the findings in this study affirm and complement some of the findings from our first study (cf. Chapter 4), particularly pertaining to bystanders' privacy concerns, the absence of explicit privacy regulations, and contextual influences on privacy concerns and practices. The alignment of some of the results in this study with the findings from our first study strengthens the reliability, robustness, and credibility of our research outcomes. It also emphasizes the significance and authenticity of our research within the investigated context.

This study's findings show the impact of smart home devices on the power dynamics within household-worker relationships in smart homes in Jordan. In Section §5.4.1, we explore the contextual and economic power dynamics in these smart homes, shedding light on how households utilize smart devices to monitor and control their domestic workers. This practice can be perceived by workers as a new form of modern slavery[81][465]. Additionally, we examine how these exploitative technologies shape the privacy concerns and practices of both households and their domestic workers. In Section §5.4.2, we delve into participants' perceptions of privacy rights and data protection in Jordan. We then present participants' aspirations for mitigating and balancing the socio-economic power dynamics in Jordanian smart homes. Furthermore, we discuss how smart technologies could be leveraged to enhance user and bystander agency, rather than serving as tools for exploitation.

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

Figure 5.1 depicts the identified associations between the identified themes based on the insights gained from this study's findings. For a general overview of the codebook, refer to Table 5.4.

**Figure 5.1:** Visual Representation of Categories and Themes

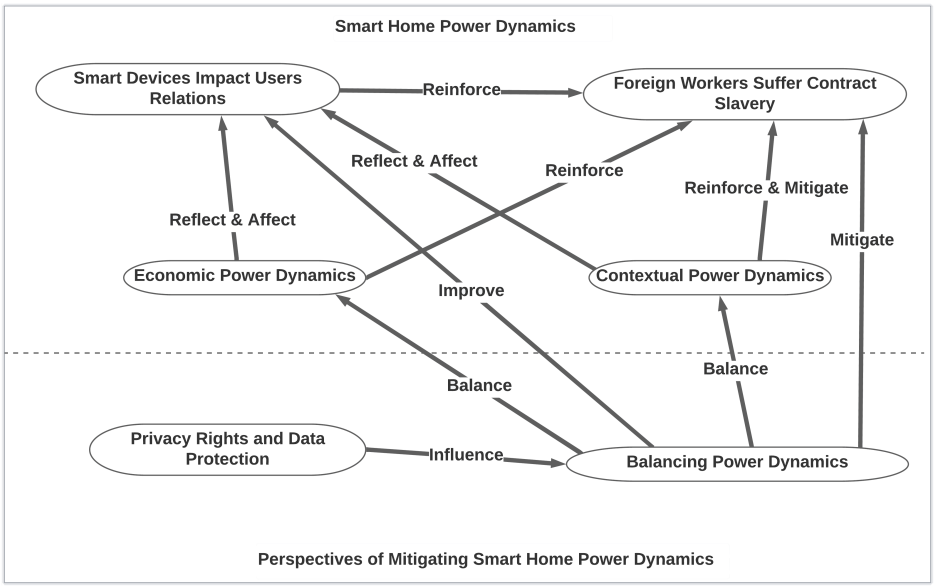



**Table 5.4:** Summary of Categories and Themes

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

### 5.4.1 Smart Home Power Dynamics

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

#### 5.4.1.1 Contextual Power Dynamics

**5.4.1.1.1 Smart Home Social Power Map.** Previous studies [466–468] discuss power-control theory and the relative power fathers have in patriarchal households, and how these inequalities are reduced in egalitarian households. Supporting these studies, our findings identified different levels of social power within households in Jordan; the highest *'first social power level'* is attributed to the family-head (usually the father). Our households argued that the family-head has the ultimate power in the home, and the final say in terms of home activities: particularly decisions related to smart devices and hiring domestic workers [H01]. However, they added that –in some cases – the head of the household could be the mother or the elder son [H01]. Moreover, our findings uncover that in many cases the family-head is neither the administrator of the smart devices, nor the direct recruiter of the domestic worker [H05].

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

**5.4.1.1.2 Household Privileges.** Complementing our previous findings (cf. Section §4.3.3.1), this section shows that households perceive themselves as having authority over data collection decisions within their smart homes. We observe that the privacy concerns and practices of users are influenced by contextual social norms and their past experiences with data collection through smart technologies.

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

**5.4.1.1.3 Contextual Norms and Religious Background Influence Users' Relations and Privacy Considerations.** To complement the findings from our first study (cf. Section §4.3.4), this section presents how social norms and religious backgrounds influence users' relations, privacy concerns, practices, and considerations with smart devices in Jordan. Regulators argued that contextual norms and religion both influence user relationships and privacy practices. [R04] said: *"some households treat their workers well, and in good ways. As Muslims, [households] have to be good with their workers. They are employees not slaves"*. Moreover, regulators discussed that households assume Muslim workers are trustworthy [R02]; however, another regulator argued that households assume non-Muslim workers are more professional and disciplined [R03]. Regulators also mentioned that social norms and religious beliefs influence positive privacy practices [R02], and households argued that religiously committed households will inform workers about the devices they use [H06]. From their side, workers believe that Muslim households will treat them well, and will respect their privacy [W03]. Moreover, regulators and

households affirmed the household *'Autocratic Practices'* (cf. Section §4.3.3.1), explaining that households believe they are free to do whatever they see fit inside their home [H03]. Regulators added that household autocracy is part of Jordanian culture [R02]. Despite displaying autocratic practices against workers, activists noted that households do not deny workers' basic rights (i.e., shelter, salary, and food). Activists affirmed that this is a cultural issue, and limiting household power inside the home will require cultural transformation [A05].

**5.4.1.1.4 Women Experience Reduced Power and Rights.** Regulators and activists argued that women are a marginalized group in MAME region [A02,R01], and activists explained that because of this, foreign female workers experience reduced rights and freedom in the home [A02], and also have to compromise privacy rights *"to survive"* the contract period [A02]. One female foreign worker said that she was not allowed to express herself, to go out of the home on her own, or to talk to outsiders, and she was required to wear loose clothes, and hijab[22] [W06]. Activists argued that many people in MAME region consider women a symbol of honor[19], and some households consider female workers' honor part of their own honor. [W04] said: *"my employer does not allow his wife to sit with visiting men, and he asked me not to talk to men"*. Regulators also argued that women are protected through social norms, and religious beliefs in Jordan [R01].

### 5.4.1.2 Economic Power Dynamics

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

**5.4.1.2.1 Imbalanced Economic Power Dynamics.** Activists argued that domestic workers come from low economic societies, thus they accept hard working conditions [A03], and noted that worker-household relations are shaped by these economic imbalances [A04]. Workers confirmed this [W02], and households emphasized that workers have to accept and respect the rules of the home [H06].

Adding more details, regulators highlighted that wealthy households tend to be more autocratic and stringent with their workers due to the economic disparity between the two groups [R07], *"I believe rich families put a big load on their maids, and they do not talk with them about anything other than the jobs they do"*. Supporting this, workers argued that it is more comfortable to work for average income households compared to higher income ones [W03]. Activists also thought that the financial gap between households and workers is huge, and results in households undervaluing workers' rights and freedom [A05].

**5.4.1.2.2 Workers Compromise Privacy Rights.** Adding to our previous discussion (cf. Section §4.3.3.5), we found that workers compromise their privacy rights with smart devices and tend to normalize co-living with them [W07]. One of our participant workers argued that she accepts devices to avoid conflicts, and to maintain good relations with the household: *"I find it easier to accept that and to avoid conflicts with [the household]"* [W05]. Moreover, workers highlighted *"Difficulty in Finding Jobs"*, and explained that they trade-off privacy rights and hard work conditions to maintain jobs [W05]. From their side, labour law experts discussed that jobs are becoming scarce, and not easy to find, which results in workers making trade-offs to maintain jobs [LE03], adding that workers tend to be less concerned about privacy when salaries are good [LE03]. A foreign domestic worker [W04] said: *"there are no jobs in my country, I will not lose my job because of cameras"*. Moreover, workers explained that the socio-economic power dynamics are not on their side, and they are unable to discuss or enforce any preferences on households [W05].

### 5.4.1.3 Smart Devices Impact Users Relations

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

**5.4.1.3.1 Privacy Concerns.** Complementing our previous findings (cf. Section §4.3.2), smart home devices are increasingly used to collect, store and share different types of data about populations in range. Whether these devices are used intentionally or incidentally, they impact the dynamics of household-worker relation from different angles. Worker [W03] said: *"they installed the cameras last year, and I feel that my relation with [the household] is not like before"*. Households expressed that smart devices are becoming an integral part of their daily life [H05], and argued that smart devices could be helpful in mitigating safety and security threats [H06]. Both households and workers highlighted that they are mostly concerned about audio-visual data collection [H01,W07]. Households, and workers mentioned that they are not fully aware of what different types of smart devices might be collecting about them, and where the collected data stored [H02,W02]. Some also expressed uncertainty about potential threats on privacy arising from non audio-visual smart devices: [W02] said *"I do not know how smart heating system, or smart lights could affect me. I am not saying they are not, but I really do not know how"*.

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

**5.4.1.3.2 Strained Relationships.** Our findings indicate that workers have perceptions of distrust, disrespect, and lack of transparency in smart homes [W06]. Workers perceive household use of smart devices inside the home as a sign of distrust [W04], which is influenced by the purpose and location of devices [W07]. Conversely, workers expressed their own distrust towards households due to uncertainty about how collected data is used, particularly when households conceal or refrain from

informing them about devices [W01]. Both households and workers acknowledge that smart devices can serve as tools to demonstrate worker trustworthiness and foster trust within households. This can strengthen trust between workers and households, lead to a gradual decrease in monitoring, and blur the boundaries between home and workplace [H06, H07, W05]. On the other hand, households claim they use devices to monitor their homes, rather than intentionally monitoring workers [H02]. Furthermore, while workers feel uncomfortable with smart devices [W04], households argue that they cannot simply turn off the devices to make workers more comfortable [H04]. Workers clarify that they do not expect households to switch off the devices entirely, but rather seek agreement on when, where, and how households use the devices to create a comfortable work setting [W01].

**5.4.1.3.3 Smart Home Devices Reinforce Asymmetrical Power Dynamics.** Similar to what Bernd and Abu Salma [7] discussed, we found that smart devices reinforce power dynamics between households and domestic workers as they provide households with tools to monitor and control workers. Workers argued that households can use collected data against them in many ways (e.g., terminate their contracts, exploit, or defame them) [W04]. However, regulators said that smart devices can be good for the security of both households and workers, and can provide evidence in case of any dispute [R04]. Workers also argued that smart devices could be good as they provide evidence of workers' good attitudes and performance [W04].

#### 5.4.1.4 Foreign Workers Suffer Contract Slavery

Findings demonstrate the strict practices imposed on workers, with households considering the worker's living quarters as their workplace and disregarding their privacy rights within the home [H03]. Some workers recounted instances where households would use devices to record them without seeking their consent [W01]. Workers argued that these actions constituted intrusive monitoring and made them feel constantly surveilled and controlled [W05]. They cited examples of households using smart devices to monitor them extensively, leading to discomfort and violations of privacy [W05]. Furthermore, one worker expressed concerns that they could

be observed during private moments such as changing clothes or removing their hijab [W05]. Another worker described how the household remotely monitored her activities through smart devices [W04]. These practices are indicative of the limited rights of foreign domestic workers in Jordan, and could be seen as signs of contract slavery. Expanding on this, activists argued that foreign domestic workers in Jordan face marginalization, reduced agency, and a lack of privacy rights in their employers' homes [A04]. Some workers said they felt like slaves—particularly female workers [W06]. Labor law experts gave examples of wider mistreatment: some households confiscate workers' passports and Identity Cards, deny vacations, restrict smartphone and internet access, and confine them to the home for most of their contracts' periods [LE03]. Furthermore, activists highlighted the inability of foreign domestic workers to terminate their contracts without paying back the cost of recruitment to their employers [A02]. This practice sustains a cycle of contract slavery as workers cannot afford these costs [W06]. Consequently, activists explained that workers are forced to endure harsh working conditions and limited rights [A03]. Workers also reported that recruitment agencies in their home countries fail to clarify the financial obligations related to contract termination before their arrival in Jordan [W08].

### 5.4.2 Perspectives on Mitigating Smart Home Power Dynamics

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

#### 5.4.2.1 Privacy Rights and Data Protection

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

**5.4.2.1.1 Lack of Data Protection Regulation in Jordan.** As discussed in Section §2.2.5.2, and in conformity with our findings in Section §4.3.3.4, we found that Jordan lacks explicit data protection laws that address data protection of households, and bystanders in smart homes. At the time of conducting this study, regulators, labour law experts, and activists confirmed that Jordan lacks explicit data protection regulation and policies [A05, LE02, R04]. Moreover, regulators argued that existing laws are outdated [R02], and activists argued that *"privacy is overlooked in existing laws"* [A04]. Regulators mentioned that Jordan applies its cybercrime law[57], and the penal code-Article 348[58] [R04]. They added that privacy – as a general concept – is expressed in the Jordanian constitution[15] [R06]; however, regulators noted that how this relates to data protection is not explicitly addressed in the constitution [R03]. Regulators mentioned that Jordan is about to issue a new data protection law [R07] (this study was conducted before the announcement of the new data law[55] in Jordan), and argued that the new law is inspired by the EU GDPR[29], and will be tailored to fit Jordanian context [R03]. It is worth mentioning that the new law in Jordan is announced to be enacted in March 2024, and we found that the new law, as expected, does not explicitly address smart home users' data protection.

**5.4.2.1.2 Economic-Contextual Influences on Privacy Rights.** As discussed in Sections §5.4.1.1, and §5.4.1.2 of this chapter, activists mentioned some economic, contextual and religious influences on privacy rights, and highlighted how contextual norms in Jordan ensure the inviolability of home [A01]. Regulators argued that religious background and cultural norms encourage households to inform bystanders (e.g., visitors, and domestic workers) about smart devices, and do not allow households to monitor their workers. [R05] said: *"In my social culture and in Islam it is not allowed"*. In contrast to this, other regulators said the existing culture tends towards an autocratic model, a patriarchal power structure, women being dis-empowered, and individuals in lower social and economic order being disadvantaged [R06].

#### 5.4.2.2 Balancing Power Dynamics

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

**5.4.2.2.1 Awareness is Important For Protection.** This section affirms and complements our previous discussions (cf. Section §4.3.1). Findings of this study emphasize the importance of awareness, as we found that raising awareness is crucial to mitigating the negative effects of smart home asymmetrical power dynamics. Activists mentioned the importance of awareness of different types of smart devices, and of privacy concerns [A04]. They argued that improving awareness can mitigate imbalanced socio-economic power dynamics [A03]. Regulators argued that awareness is crucial to protection as it enables informed attitudes and perspectives, and also emphasized that regulations alone are not enough [R05]. Labour law experts argued that providing social security coverage and health insurance to workers, and educating them could empower them and help mitigate unequal power dynamics [LE02]. When we asked activists, labour law experts, and regulators about how to improve awareness of smart devices and privacy protection, they suggested a variety of channels: social media, mass communications advertisements, informing the education system, and running awareness campaigns [LE02]. Regulators emphasized the need for both private and public sectors to collaborate to improve public awareness [R04]. Additionally, activists, labour law experts, and regulators emphasized the importance of awareness guidelines to be available and accessible [A03, LE02, R04].

**5.4.2.2.2 Consider Household-Workers Needs.** Labour law experts argued that using smart devices to monitor domestic workers should be regulated as it is difficult to protect workers' privacy without proper regulations that consider and balance the needs of households and workers [LE02]. In contrast, regulators argued that no law could be adopted that undermined a household's freedom [R03]. Our

participants overall felt that balancing the needs of both parties is fundamental to ensure the safety and security of the home, to protect workers' rights and privacy, and to encourage healthy relationships between them [R03, LE02, A02].

**5.4.2.2.3 Regulation Modernization to Consider Smart Home Power Dynamics in Jordan.** As discussed in Sections §5.4.2.1, Jordan currently lacks explicit regulations for data and privacy protection, despite the growing need due to the growing adoption of smart devices[7]. As this study was conducted before the announcement of the new data law[55] in Jordan, regulators expressed optimism about the new law [R01], sharply contrasting with concerns raised by activists regarding its effectiveness in addressing users' privacy concerns [A01].

Regulators acknowledged the global socio-economic context in shaping legislation in this field [R06]. They recognized that Jordan's influence may not be significant enough to drive modifications in smart device designs by vendors [R04]. Activists and regulators emphasized the potential of international cooperation to exert influence on large technology companies. Domestic regulations alone may not suffice in overcoming their power [A05, R04]. One avenue discussed was the introduction of legal liabilities to encourage manufacturers to enhance smart device design [R05], or the establishment of a global agreement that sets guidelines for manufacturers to improve their designs [R02]. Regulators stressed the global nature of privacy protection as an overarching goal [R05]. However, they noted that various parties hold different views on the direction and extent of privacy discussions and data laws in Jordan [R02]. Pushing back against the notion of privacy being negotiable, activists emphasized that data protection is a fundamental human right [A04].

At the time of conducting this study, and before the announcement of the new law's enactment, regulators clarified that the new law would be distinct from existing cybercrime legislation[57], while complementing the existing legal framework in Jordan [R04, R06]. Additionally, both activists and regulators argued that social norms and religious principles play a vital role in regulating data protection and maintaining a balance in smart home dynamics [A05].

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

## 5.5 Discussion and Recommendations

Our findings reveal the influence of power dynamics on household-worker relationships, intertwined with contextual norms, customs, religious background, and economic status. In response, we propose interventions aimed at balancing power dynamics, protecting bystanders' privacy, and enhancing their agency.

### 5.5.1 Summary of Findings

The findings were presented under two main categories. The first category is *Smart Home Power Dynamics* (cf. Section §5.4.1), where we found that smart home power dynamics relate to the Jordanian contextual norms, customs, religious background of individuals, and their economic status, and how these affect and reflect dynamics of household-worker relationships. We found that domestic workers tend to compromise their privacy rights for received benefits and to avoid conflicts. Consistent with prior study [312], we also found that foreign domestic workers can

suffer from contract slavery and are a marginalized group in Jordan. Additionally, we found that female workers experience reduced rights, yet they have some social standing. Moreover, we found that households, and workers are primarily concerned about audio-visual data collection and about the purpose of using devices (e.g., spying and/or controlling of workers). We also found that they are concerned about the potential data gathering activities of other smart devices (e.g., smart lights, smart door locks, smart heating), however, they are not well-informed about the specific categories of data that are being collected by these devices, nor are they aware of the possible consequences of these data gathering activities on their privacy.

The second category is *Perspectives on Mitigating Smart Home Power Dynamics* (cf. Section §5.4.2), where we found that Jordan lacks explicit data protection laws, and we discuss participants' aspirations for mitigating and balancing asymmetrical smart home power dynamics. As a result, we discuss and propose a set of recommendations for interventions to mitigate imbalanced power dynamics in Jordanian smart homes, protect privacy, empower domestic workers, and prevent technology exploitation.

### 5.5.2 Contextual Interventions

We highlight in Sections §5.4.1.1 and §5.4.1.2 the negative impacts of smart home power dynamics on workers' agency and privacy. Given that households are both employers and owners of the home and devices, they possess the greatest power to determine how, where, and when to use these devices. Drawing on the findings from Section §5.4.2.2, we explore contextual considerations and propose interventions for mitigating smart home power dynamics.

#### 5.5.2.1 Consider Jordanian Context

Prior studies have highlighted contextual variations in privacy concepts across diverse cultures and contexts, underscoring the limitations of extrapolating Western research findings to non-Western settings like Jordan [177, 183]. These variations manifest in various aspects, such as the centralization of decision-making and power,

diminished women's rights, and the collective nature of MAME societies, in contrast to the individualistic tendencies prevalent in Western societies [469, 470].

Nevertheless, in alignment with prior Western studies [178, 188], our study in Jordan emphasized diverse privacy concerns (such as invasive monitoring). Participants emphasized the impact of socio-economic power dynamics on relationship qualities, including trust, respect, and comfort between households and workers. Notably, Jordanian households were observed to adopt autocratic practices, restricting workers' agency and limiting their freedom of choice. This led workers to compromise their privacy rights in exchange for benefits like jobs, salary, and shelter. Given these findings, addressing contextual privacy concerns in Jordan becomes imperative, considering the influence of social, religious, and cultural factors. This approach aims to mitigate power imbalances and minimize the risk of privacy violations against vulnerable domestic workers. As a response, we propose a set of recommendations directed at policymakers, social entities, and manufacturers to better account for this context.

**5.5.2.1.1 Policy Makers to Consider Jordanian Context.** At the time of conducting this study, the findings (cf. Section §5.4.2.1), and in consistency with our literature review (cf. Section §2.2.5.2), show that Jordan lacks explicit data protection and privacy regulations that address conflicts among smart home users. Similarly, existing data protection laws in other countries (e.g., EU-GDPR, USA-CCPA[43], Brazil-LGPD[39]) primarily focus on regulating data protection with companies and service providers like Google, rather than explicitly addressing the data protection of smart home users. To address this, we propose that the new data protection law in Jordan, and its successive updates, leverage social norms and religious backgrounds within Jordanian society in future revisions and reviews. Furthermore, we argue for a more international approach to data protection regulation, considering the increasing adoption[7] of smart technologies worldwide. Achieving this global consensus requires collaborative efforts between governments

and international and regional entities such as ITU[82], GSMA[8], TMForum[83], Accessnow[84], and AADR[85].

In addition to international efforts, we propose the new data protection law in Jordan and its updates to mandate privacy certifications for smart devices entering local markets. Recognizing the dual nature of the smart home as both a workplace for domestic workers and a residence, it is crucial for Jordanian regulators and policymakers to address the specific needs of marginalized user groups, with a particular focus on women. To address this, we suggest the establishment of a dedicated *'privacy advice channel'* through relevant authorities and societal entities in Jordan. This channel would serve as a platform for workers and household members to seek guidance on privacy matters, propose good practices, and report autocratic practices and privacy violations.

Furthermore, we argue for future updates of data law in Jordan to hold households accountable for their use of user data and to establish guidelines for obtaining informed consent, essential for lawful data processing. Emphasizing the importance of innovative regulations that cater to users' needs and concerns, we also highlight the necessity for manufacturers to receive design guidelines. Finally, we emphasize the importance of collaboration among all stakeholders, including policymakers, manufacturers, and societal entities. Addressing these challenges necessitates not only regulatory measures, awareness campaigns, and technological advancements but also a fundamental cultural shift towards more responsible data practices.

**5.5.2.1.2 Manufacturers to Consider Jordanian Context.** Outside of the requirements imposed by regulation, it is also important for manufacturers to actively engage with socio-economic power dynamics and privacy concerns of the Jordanian context. Companies should engage more deeply with the principles of privacy by design (PbD[33]) [471] and actively seek feedback from users in Jordan (we discuss PbD

[82]ITU-The United Nations specialized agency for ICT
[83]TMForum-The global industry association for ICT service providers
[84]Accessnow-Organization defends the digital rights of communities at risk.
[85]AADR-The Arab Alliance for Digital Rights.

in detail in Section §6.5.3.3). Building on previous studies [228, 472], we recommend international manufacturers collaborate with local policy makers to establish design guidelines that align with the needs and expectations of users in Jordan, ensuring the inclusion of vulnerable user groups. This approach will help manufacturers strike a balance between business interests, user expectations and contextual privacy needs. Furthermore, companies can deepen their ability to develop context-friendly devices [473] by enhancing their designers' understanding of the contextual concerns in Jordan, and to meet the expectations of domestic workers while enhancing their agency. We argue that there are substantial business opportunities for manufacturers who can tailor their offerings to different markets, including Jordan and wider MAME areas, given the rapid growth of smart technologies[7].

#### 5.5.2.2 Balance Household-Worker Needs

Ensuring that households in Jordan will prioritize the privacy needs of domestic workers and create an environment that encourages open communication is a significant challenge. In achieving this, it is important for good practices to be developed for how households can be more respectful of workers' privacy in the context of smart homes.

To promote privacy-respecting practices, targeted awareness campaigns should be conducted for households. These campaigns should educate households about privacy risks associated with smart devices and emphasize the importance of understanding and respecting workers' privacy preferences. This will need to be tempered with guidance to navigate the delicate balance between workers' privacy and the safety and security needs of the home, together with accessing support from government authorities and society organizations. Building on previous studies [210, 211], we suggest the leveraging of Jordan's unique social and religious norms – including the customs and obligations relating to good hospitality or Muslim traditions of morality (e.g., kindness, honesty, justice) – to shape how household should engage in proactive communication with workers regarding privacy. By promoting awareness and education, these campaigns should aim to foster an

environment of mutual respect and trust, leading to healthier and more equitable relationships within smart homes.

#### 5.5.2.3 Domestic Workers' Recruitment Agencies to Inform Workers

The agencies that facilitate the recruitment of domestic workers should also be encouraged to inform and educate workers about privacy risks with smart homes. This can be achieved through tailored booklets and guidelines for workers from different linguistic backgrounds (e.g., Philippines[86], Indonesia[87], Ethiopia[88], Ghana[89], and Bangladesh[90]). Recruitment agencies should also provide comprehensive information about Jordanian culture, social norms, religious background, work conditions, and workers' privacy rights. Collaboration between recruitment agencies, local policymakers, and concerned organizations is recommended to develop simple guidelines that achieve a fair balance between privacy of workers and the needs of households. Agencies should also obtain workers' consent through job contracts, provide tailored information to households, and facilitate negotiations between workers and households to mitigate power imbalances and promote healthy relations.

### 5.5.3 Technical Considerations and Interventions

Drawing upon the recommendations outlined in Section §5.5.2.1.2 and the findings presented in Section §5.4.2.2.4, this section discusses some technical considerations and interventions aimed at rebalancing power dynamics.

#### 5.5.3.1 Innovative Technologies and Multi-User Consent

We propose leveraging the outcomes of innovative technologies, such as Artificial Intelligence (AI) and Machine Learning (ML), to develop algorithms and statistical models that enable smart devices to learn from data collected in specific applications. This would facilitate the identification of bystanders, decision-making, and actions

[86]Languages spoken in Philippines include: Tagalog, Cebuano, Ilocano
[87]Indonesian is the official and national language of Indonesia
[88]Spoken languages in Ethiopia include Oromo, Amharic, Somali
[89]Spoken languages in Ghana include English, Akan, Ghanaian Pidgin
[90]Bengali is the language spoken by workers from Bangladesh

to support privacy protection and enhance user agency. AI-enabled smart devices can learn to improve privacy over time, understand contextual power dynamics and usage patterns, integrate data protection with user recognition technologies (e.g., user identification and profiling), and either hide or delete bystanders' data. Furthermore, we argue for empowering workers by providing control over collected data. However, achieving this relies on either obtaining consent from the family or implementing novel regulations in Jordan to enforce it.

As highlighted in other studies [474, 475], our findings (cf. Section §5.4.2.2.4) underscore concerns arising from single-user consent impacting passive users, potentially subjecting unaware individuals to data collection. We argue for further research to develop and contextualize multi-user consent mechanisms tailored to Jordanian expectations and values. Additionally, devices should be designed to prioritize data management across privacy settings, addressing challenges outlined in previous studies [476, 477], including granularity, complexity, user awareness, interoperability, managing changes in privacy settings, and transparency. One promising approach to achieve this is adopting and tailoring Information Flow Control techniques to monitor the use of bystander data and enforce regulations [478, 479].

#### 5.5.3.2 Semiotics of Privacy

To enhance the protection of users' privacy through effective user-device communication, we propose leveraging Semiotics[32]—utilizing consistent signs and symbols suitable for Jordanian users and comprehensible for foreign domestic workers. Given the complexities of accommodating diverse languages, education levels, religious and cultural norms, and the potential of AI, ML, and natural language processing, Semiotics can significantly contribute to this domain. For instance, smart devices can employ various communication channels (e.g., audio, visual) to convey their presence or data collection capabilities to people nearby. Additionally, we suggest that smart devices could notify the mobile apps of bystanders, possibly through

discovery protocols like UPnP[91], SSDP[92], or BLE[93]. However, it is crucial to consider the security implications of revealing such information.

#### 5.5.3.3 Data Minimization and Perturbation Techniques

To support privacy protection, we argue for the implementation of data minimization techniques [480], ensuring that data is collected only for specific purposes. This reduction in data collection mitigates the risks associated with misuse, exploitation, and exposure of sensitive information. It is imperative, however, to strike a balance, ensuring that this decrease in data collection does not compromise the performance or functionality of smart systems. Coupling data minimization with giving bystanders control over the collection and use of their personal data empowers workers to make informed decisions and mitigates exploitation. This approach facilitates a balance between the amount of data collected and the extent to which bystanders are authorized to access and control it [480].

Prior research has discussed the effectiveness of data perturbation techniques and differential privacy in protecting datasets [247, 481]. Building upon these techniques, we propose the application of perturbation methods to bystander data by intentionally introducing noise or modifying the data to protect users' privacy and prevent exploitation. For instance, smart devices can collect various types of data from the home, such as temperature, humidity, light levels, or audio-visual data, which can be used to infer the presence and activities of users, including bystanders. However, perturbing bystanders' data makes it more challenging to accurately infer information about them. Balancing data perturbation with household security and safety requirements poses challenges, and perturbation techniques may not be universally effective against all types of internal and external privacy breaches. Consequently, combining them with other privacy protection techniques is necessary to ensure robust privacy protection [247, 481].

[91]UPnP- Universal Plug and Play
[92]SSDP- Simple Service Discovery Protocol
[93]BLE- Bluetooth Low Energy

## 5.6 Conclusion

This chapter explores smart home power dynamics between households and domestic workers in Jordan, providing recommendations to balance power dynamics, prevent the misuse of smart technologies for exploitation, enhance domestic workers' agency, and protect their privacy. The findings expose power differentials and household privileges, demonstrating how socio-economic dynamics impact relationship qualities. It uncovers issues such as contract slavery and marginalization, emphasizing the lack of explicit data protection regulations for smart home users in Jordan. The study concludes with an examination analysis of the socioeconomic power dynamics between households and their domestic workers and how these dynamics impact relationship qualities. We summarized the study findings and discussed the implications.

# 6

# Privacy Protection With Smart Device Design

This chapter explores smart device design challenges associated with privacy protection for domestic workers in Jordanian smart homes. Therefore, this chapter tackles our third research question, RQ.3: *"How can we support privacy protection for domestic workers (i.e., bystanders[1]) in the smart home in Jordan?"* To address this question, we break it down into two sub-questions: a) *"How can design of smart home devices support privacy protection for domestic workers in the smart home?"*, and b) *"What are the design challenges of privacy protection for domestic workers in the smart home?"*

To address these research questions, we conducted a qualitative research study with 44 key stakeholders. Section §6.2 outlines our research approach, involving semi-structured interviews. The study findings (cf. Section §6.4) resulted in an **investigation analysis** of smart device design challenges with bystander privacy protection in Jordanian smart homes. We discuss these findings in Section §6.5. The use of the term *'study'* in this chapter refers to our third study reported in this chapter unless stated otherwise.

## 6.1 Motivation

Our motivation to explore the design challenges of privacy protection with smart home devices stemmed from insights gained in our first and second studies (cf. Chapters 4, and 5), which revealed that the growing adoption of smart home devices [10] has led to increasing privacy concerns, especially for smart home bystanders. While most research has focused on households in Western contexts (i.e., Europe and North America), very few studies have explored design challenges for domestic workers' privacy protection, particularly in MAME[14] contexts like Jordan. This study takes a step to fill this gap.

## 6.2 Methodology and Research Question

As explained in Chapter 3, and following similar approaches used in previous qualitative research studies [7, 144, 482], we designed and conducted a qualitative user research study with participants concerned with smart home device design (i.e., designers, business leaders). We focused on understanding their concerns with data protection design of smart home devices such as smart cameras, smart speakers, smart lights, and smart door locks. Additionally, we engaged with local users (i.e., households and domestic workers) of smart home devices in Jordan, as well as local manufacturers and importers of such devices in Jordan and some neighboring MAME countries. This engagement aimed to explore their perspectives on privacy protection through smart device design.

In this chapter, 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 U (e.g., [U01] being household number 1), and to Domestic Workers (i.e., bystanders) as W (e.g., [W01] being domestic worker number 1).

### 6.2.1 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 §6.4.1.1, where we discuss smart device design processes and designers in more detail. Based on this initial understanding, and adhering to guidelines for recruiting participants in qualitative research studies [441, 442], we developed our screening questionnaire survey as below (cf. screening questions in Appendix D.4):

- 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 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;

- For all participants, it is required to be above 18 years old.

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 [458, 483], and to some extent a taboo topic [459] in many organizations. Therefore, many candidates chose not to participate, citing non-disclosure agreements (NDA) and business confidentiality obligations. To address this challenge, participants were briefed on our ethical, security, and privacy measures, with a focus on data encryption and compliance with the General Data Protection Regulation (GDPR[29]). Additionally, we employed snowball sampling [443], a method commonly used to engage with hard-to-reach groups [445–448]. 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. (cf. study poster for designers and international business leaders in Appendix D.3).

To recruit users (families and domestic workers) from Jordan, similar to our approach in Chapters 4 and 5, 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 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[79], JODDB[94], Jordan's RSS[95]; JCC[96]; UAE's ATRC[97]; and Egypt's ASRT[98]) to advertise the study and to identify and invite potential candidates from Jordan and some neighboring 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 (cf. study posters for households, workers, and local business leaders in Appendix D.1, and Appendix D.2).

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 [484].

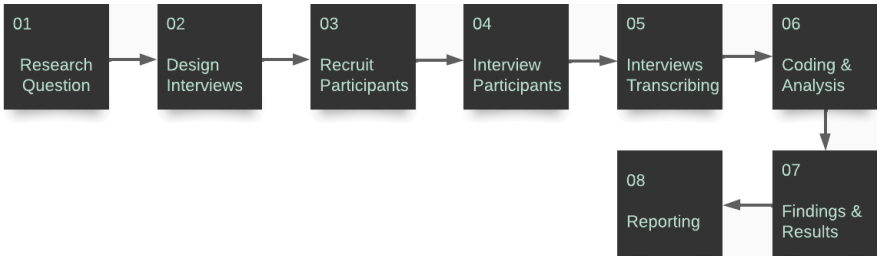
Despite not being able to recruit designers and local business leaders from Jordan and MAME countries, we engaged with smart device local agents and assemblers from Jordan and other MAME countries to identify the reasons behind lack of local manufacturers and designers, and whether they consider privacy 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.

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

[94]JODDB: Jordan Design and Development Bureau
[95]RSS: Jordan Royal Scientific Society
[96]JCC: Jordan Chamber of Commerce
[97]UAE Advanced Technology Research Council
[98]Egypt Academy of Scientific Research and Technology

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[99]), and the 12 users (i.e., families and domestics workers) were from 12 different households. Similar to our approach in Chapters 4 and 5, and to prevent potential harm or ethical concerns and ensure the freedom of participation for domestic workers, we adhered to ethical considerations and took measures to avoid recruiting family heads and workers from the same households. However, this exclusion measure was not applied to other participants, such as designers, business leaders, and local business leaders. For this research study, and as explained in Section §3.2.1, we chose Grounded Theory [410, 411, 414] as it is a well-established methodology for studying areas that have not been widely researched (cf. Figure 6.1 for the research process and the applied methodology).

**Figure 6.1:** Research Process and Methodology




#### 6.2.1.1 Participant Demographics

The demographics of our 12 users (i.e., families and domestics workers) (cf. Table 6.1) 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. 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 [457]: Novice, Competent, Proficient, and Expert.

[99]Small and medium-sized enterprises

The demographics of our eight local business leaders (cf. Table 6.2) 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 (cf. Table 6.3), consisted of three female participants and twelve male participants across 13 companies. Seven worked as UX[100] designers, one as GUI[101] 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 (cf. Table 6.4), 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[102], CTO[103], CPO[104], PDO[105], and Team Business Leaders).

**Table 6.1:** Demographic Information of Users (Families and Domestic Workers)

| P# | Gender | Nationality | Age Group | Degree | Field | Occupation | Competence | Used 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, Samsung Smart TV |
| U03 | Male | Jordan | 40-49 | B.Sc. | Finance | Procurement Mananger | 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 | Domestic Worker - Home Nurse | Competence | Amazon Echo Dot, LIFEX Smart Light LG Smart TV, Hikvision Smart Camera |
| W02 | Female | Philippines | 20-29 | High School | Home Care | Domestic Worker-Baby Sitter | Competence | Google Home, Samsung Smart TV Hikvision Smart Camera |
| W03 | Female | Philippines | 20-29 | Diploma | Home Care | Domestic Worker-Baby Sitter | Competence | Google Home, LG Smart TV REOLINK Smart Camera |
| W04 | Male | Jordan | 30-39 | B.Sc. | Medical | Domestic Worker-Home Nurse | Expert | Amazon Echo Dot, Sony Smart TV |
| W05 | Female | Ethiopia | 20-29 | High School | Home Care | Domestic Worker- Maid | Basic | Google Home, Smart Camera |
| W06 | Female | Bangladish | 20-29 | High School | Home Care | Domestic Worker- Maid | Basic | Smart Camera |

### 6.2.2 Methodology and Interviews

We conducted semi-structured interviews with 15 designers, nine international business leaders, eight local business leaders, six user families, and six domestic

[100]UX: User Experience Design
[101]GUI: Graphical User Interface Design
[102]CEO: Chief Executive Officer
[103]CTO: Chief Technology Officer
[104]CPO: Chief Product Officer
[105]PDO: Product Development Officer

**Table 6.2:** Demographic Information of Local Business Leaders

| P# | Gender | Age Group | Education | Role | Experience (Year) | 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 Heating systems |
| 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 6.3:** Demographic Information of Designers

| P# | Gender | Age Group | Education | Role | Experience (Year) | Company Size (Type) | Company Location | Products |
|---|---|---|---|---|---|---|---|---|
| D01 | Male | 20-29 | BSc | UX Designer | 4 | 250-500 (SME) | UK | Smart Activity Tracker |
| D02 | Male | 20-29 | BSc | Solution Architect | 5 | 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 | 5 | 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 | 4 | 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 | MSc | UX Designer | 3 | >1000 (LE) | USA | Smart Speaker, Smart Home Hub |
| D10 | Male | 20-29 | BSc | UX Designer | 4 | >1000 (LE) | Holland | Smart Inddor/Outdoor Camera Smart Light |
| D11 | Male | 30-39 | BSc | Localization Officer | 7 | 10-100 (SME) | UK | Smart Thermometer |
| D12 | Male | 40-49 | BSc | Firmware Designer | 11 | >1000 (LE) | UK (Chinese Company) | Smart Indoor/Outdoor Camera |
| D13 | Male | 30-39 | 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 |

**Table 6.4:** 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 |

workers. Interview scripts were structured using the funnel technique [413], which involves a gradual progression from general to specific questions. We have explained the funnel technique in Section §3.2.1. 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 [460, 485], 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.

The primary 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 reason. No participants withdrew.

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

**6.2.2.0.2 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 (cf. families' interview guidelines in Appendix D.5)

**6.2.2.0.3 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 (cf. workers' interview guidelines in Appendix D.6).

**6.2.2.0.4 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 (cf. local leaders' interview guidelines in Appendix D.7).

**6.2.2.0.5 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 (cf. designers' interview guidelines in Appendix D.8).

**6.2.2.0.6 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, CCPA[43]), 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 (cf. international business leaders' interview guidelines in Appendix D.9).

### 6.2.2.1 Data Analysis

Following Strauss and Corbin's Grounded Theory method [410, 411], we transcribed the audio recordings. We analyzed a total of 44 semi-structured interviews, and using NVivo 12 Pro[76] software, we conducted the initial coding of all interview scripts. Throughout the coding process, we engaged in discussions with another researcher (the researcher's academic advisor), who asked and requested some clarifications and insights. The primary researcher also annotated the study scripts to provide additional data and context. 356 codes emerged forming the study codebook from the initial coding. 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 we 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 [414, 419, 420] separately for all our participant groups. We observed data saturation 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. 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 ($\kappa$) for all codes in our data was 0.84, indicating near perfect agreement [438]. Moreover, we tested the identified codebook for reliability and credibility using grounded theory triangulation [437] 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 Table 6.5 in Section §6.4.

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 primary 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.

#### 6.2.2.2 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 encrypted and stored securely 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. For details of the ethics application, refer to Appendix G.3.

## 6.3 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 [462, 486]. To mitigate this, the primary researcher conducting all 44 interviews is trained in how to design and conduct interviews carefully, asking questions in a neutral and open manner to avoid influencing interviewees.

*Bias:* In interview studies, self-reporting bias is frequently encountered [463]. Participants, influenced by their perception of researchers' viewpoints, may unintentionally forget details, provide inaccurate responses, or adjust their answers, thus

introducing bias [464]. To mitigate self-reporting bias, proactive strategies were employed, such as utilizing open-ended questions and encouraging participants to provide detailed responses. Additionally, when participants offered brief answers, the researcher prompted for further elaboration to ensure clarity.

*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.

*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.

## 6.4 Findings and Outcomes

This section presents the findings of our study into smart home device design challenges for data and privacy protection in Jordan (cf. Table 6.5). We present and discuss these under two key categories: 1- Privacy Protection Through Smart Device Design (cf. Section §6.4.1), and 2- Perspectives and Challenges of Privacy Protection With Smart Home Device Design (cf. Section §6.4.2). Some of the

findings in this study align with and complement some of our previous studies' findings (cf. Chapters 4, and 5), particularly in the realms of privacy concerns, regulations, and power dynamics. The recurrent identification of these themes strengthens the reliability, robustness, and credibility of our research outcomes, and underscores the enduring significance and authenticity of our research within the explored context. Figure 6.2 depicts the identified categories and themes.

**Table 6.5:** 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 |

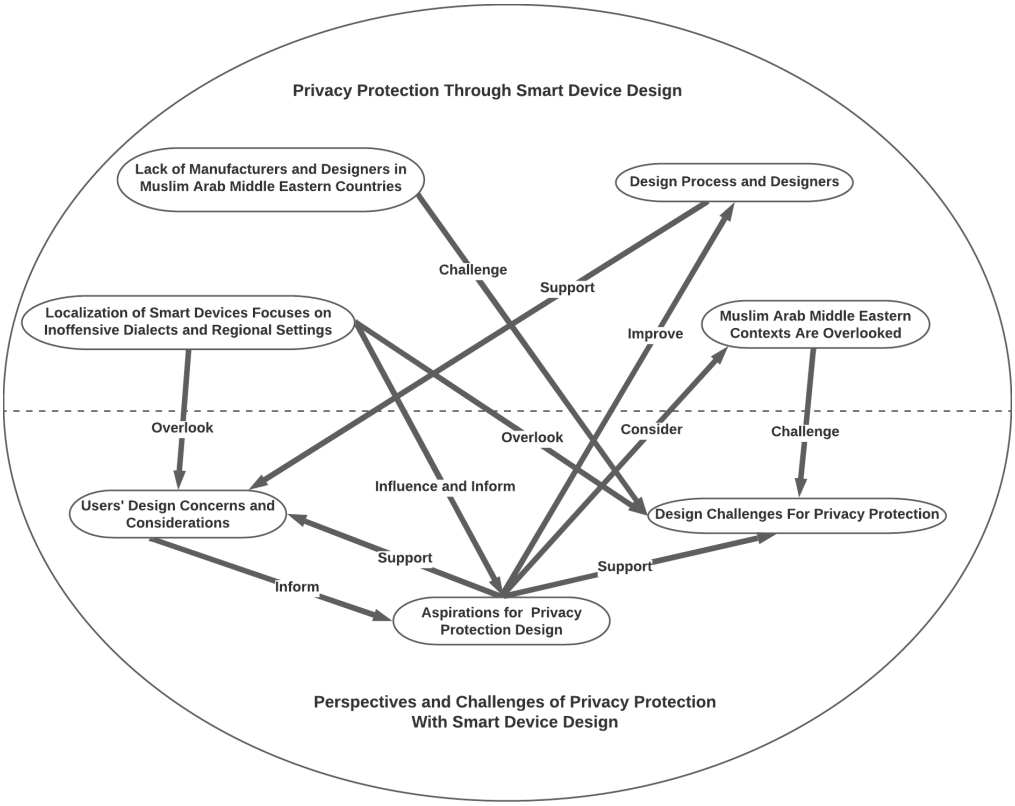
## 6.4.1 Privacy Protection Through Smart Device Design

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.

### 6.4.1.1 Design Process and Designers

As discussed in Section §6.2.1, to recruit the right sample of participants for this study, we conducted preliminary research on the design profession and processes of

**Figure 6.2:** Visual Presentation of Categories and Themes




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 [487–489], 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*[100]*/UI*[106] *Designers, Software and Firmware Designers, Localization Officers, and Solution Architects)"*.

For the definition of smart device design process, we found that there is no agreement on a specific definition. However, Luchs et al. [490] defines product design as: *"the set of properties of an artifact, consisting of the discrete properties*

[106]UI: User Interface Design

*of the form (i.e., the aesthetics of the tangible good and/or service) and the function (i.e., its capabilities) together with the holistic properties of the integrated form and function"*. The design process can be summarized in five key steps (cf. Figure 6.3):

1. *Concept Generation*: Marketing team and creativity team collaborate to agree on the concept and functions of the device. They may discuss with the technical team about required hardware, firmware, and software design.

2. *User Modeling*: Marketing team and creativity team work together to identify the target audience and sort users into groups (i.e., age, gender, socio-economic status, education).

3. *Visualization Sketch*: Imagination of the device and how users will use it.

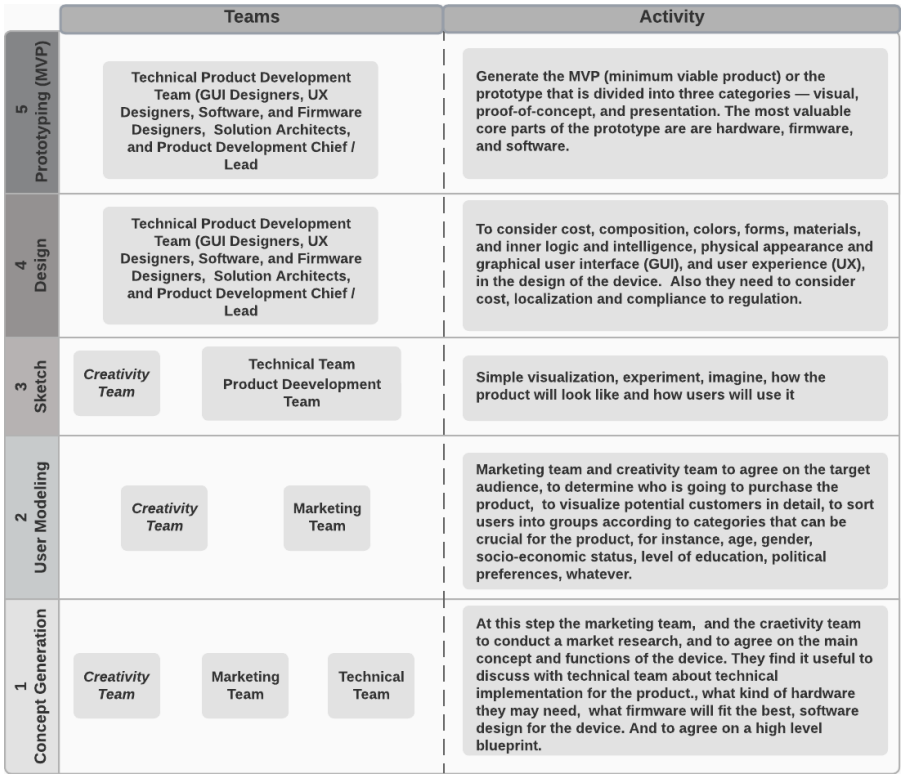
4. *Design*: Technical Product Development Team (i.e., GUI Designers, UX Designers, Software and Firmware Designers, Solution Architects, and Product Development Chief/Lead) collaborate to agree on cost, inner logic, physical appearance, graphical user interface (GUI), user experience (UX), user interface (UI), localization, and compliance with regulations

5. *Prototyping*: The Technical Product Development Team develops the MVP (minimum viable product) or the prototype, which is divided into three categories — visual, proof-of-concept, and presentation models

#### 6.4.1.2 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.

**Figure 6.3:** Smart Device Design Process




Local business leaders pointed to Research and Development costs, the limited size of nascent MAME markets[107], and economies of scale[108] as impediments to the 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*

[107] Report-Smart Homes Devices Market in the Middle East, Turkey, and Africa
[108] Economies of scale relate the cost of production to production volume and market size

*[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.

#### 6.4.1.3 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 were unable to participate due to being bound by NDA 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 address specific contexts.

#### 6.4.1.4 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 primarily prioritize device functions, price, and ease of use. Designers also highlighted the importance of *Inclusive*[109], *Accessible*[110], *Non-Offensive*[111], *Ethical*[112], and *Relevant*[113] 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,

[109]Inclusive design considers the full range of human diversity with respect to ability, language, culture, gender, age, and other forms of human difference.

[110]Accessible design aims to make sure that people with disabilities can access and use smart products effectively.

[111]Non-Offensive design avoid causing someone to feel resentful, upset, or annoyed.

[112]Ethical design refers to design that resists manipulative patterns, respects data privacy, encourages co-design, and is accessible and human-centered.

[113]Relevant design is connected with its context in ways that satisfy users and societal needs and concerns.

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 [491]'* that automatically tuned to users' context (i.e., location) .

### 6.4.2 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, designers, 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.

#### 6.4.2.1 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.

**6.4.2.1.1 Privacy and Security Concerns with Smart Device Design.** Affirming and complementing our previous findings (cf. Sections §4.3.1 and §5.4.1.3.1), users in this study (both families and domestic workers) (N=12) confirmed that they are primarily concerned about audio-visual smart devices. They expressed interest in understanding the potential impact of other types of smart devices on them [U03, U04, W05, W06] and added that they were unsure 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]. Moreover, 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, U02]. To address these threats, they emphasized the importance of designing privacy protection measures that address both types of threats.

#### 6.4.2.1.2 Concerns of Smart Home Bystanders and Power Dynamics.

Expanding on, and affirming the insights gained from our previous findings (cf. Sections §4.3.3.5 and §5.5.2.1). 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[23] 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*[22] *"*. 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 marginalized 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. 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.

**6.4.2.1.3 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[114]), 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].

[114]GDPR- Art. 15: Right of access by the data subject

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.

**6.4.2.1.4 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.

#### 6.4.2.2 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.

**6.4.2.2.1 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*[115] *is fining companies like Amazon*[116] *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].

**6.4.2.2.2 Feasible Solutions For Privacy Protection Design.** Designers (N=11) mentioned that they used different approaches 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"*.

[115] ICO: The United Kingdom, Information Commissioner's Office
[116] For more details, see: GDPR fines against Amazon

**6.4.2.2.3 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].

**6.4.2.2.4 Limited Awareness Constrains Design Freedom.** Adding to our findings in the first and second studies (cf. Sections §4.3.1 and §5.4.2.2.1). 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"*.

**6.4.2.2.5 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), the USA, and other countries (such as Brazil-LGPD[39], Turkey-DPL[38], Malaysia-PDPA[50]), this study's findings further highlight the lack of explicit smart home privacy protection regulations in Jordan and at the international level, as noted in our previous studies (cf. Sections §4.3.3.4 and §5.4.2.1.1), particularly for bystanders as a user group [L06, LB01]. This lack results in unclear obligations for smart device manufacturers and uncertainty around the legal consequences of non-compliance with applicable laws [L03]. 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 [365], although its specifics remain uncertain. It is worth mentioning that this study was conducted before the announcement of the new data law[55] in Jordan. However, as

discussed previously, the newly announced law does not explicitly address smart home users' privacy concerns.

In addition to arguing 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 and laws in the USA (e.g., CCPA[43], CPRA[44], NYPA[45], HIPAA[40], TCPA[46], and FERPA[47]). 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, CCPA, CPRA) 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 business leaders, designers, and regulators [D08].

**6.4.2.2.6 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.

#### 6.4.2.3 Aspirations for Privacy Protection Design

Complementing our second study findings (cf. Section §5.4.2.2.4) around aspirations for privacy protection, this study's 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[33]). 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[32] 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. Moreover, designers emphasized that it is 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 provide services and protect their data [D09].

## 6.5 Discussion and Recommendations

This 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 on privacy protection design. While some of our findings complement some of our previous studies' findings (cf. Chapters 4, and 5), this chapter introduces new insights, and proposals to smart device design for privacy protection in the Jordanian context.

### 6.5.1 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 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 the privacy protection design of smart home devices does not effectively 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.

### 6.5.2 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.

#### 6.5.2.1 Increase Data Literacy and Educate Stakeholders

As presented in Section §6.4.2.2.4, stakeholders' limited awareness constrains design freedom and hinders privacy protection design capabilities. Prior studies [492–494] 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 §6.4.2.3, and emphasizing our previous discussion and recommendations for improving privacy protection in Sections §4.4, and §5.5, we argue that awareness needs to be improved among all

stakeholder groups to enhance 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 [371, 495], 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 [496, 497] 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 that 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.

#### 6.5.2.2 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 [498]. Similarly to smart home device users in Western contexts [178, 188, 249, 250, 499–501], users in Jordan also showed security and privacy design concerns as presented in Section §6.4.2.1 (e.g., design flaws, inability to recognize bystanders, concerns about privacy policies and consent). Our previous studies (cf. Chapters 4, and 5), and prior research [224, 283] have noted these concerns and presented broad recommendations to facilitate privacy protection.

As presented in Sections §6.4.2.1.1 and §6.4.2.1.2, 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 drawing on the suggestions of Bernd et al. [7], 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.

#### 6.5.2.3 Empower Women Workers

In line with our second study findings (cf. Section §5.4.1.1.4) and consistent with prior studies [502–504], users highlighted that female foreign domestic workers from poor countries are considered a marginalized group in Jordan. They called for collaboration among governments, social organizations, and companies to protect their rights. To empower this user group, we emphasize our previous recommendations (cf. Section §5.5.2.3) and propose several actions for governmental entities and recruitment agencies: Firstly, they should prioritize raising awareness

among 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[90], Filipino[86], and Ethiopian[88]), 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 families should be encouraged to discuss privacy requirements openly. Furthermore, families should be encouraged to contemplate the ethical implications of undermining workers' rights, while societal entities argue 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 §6.5.3.

### 6.5.3 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. In addition to our discussion and recommendations in Section §5.5.3, we believe that a significant part of these proposed technical interventions can be beneficial not only in the local context of Jordan but also on a global level

#### 6.5.3.1 Utilize Innovative Technologies

Emphasizing and building upon our recommendation in Section §5.5.3.1, we argue for designers to leverage emerging technologies, such as Artificial Intelligence (AI), to enhance data protection in smart home devices. This entails implementing features like profiling bystanders (e.g., domestic workers), user recognition, erasing or protecting their data, and devising innovative AI strategies for evaluating and managing bystanders' privacy. Companies should adopt differential privacy

algorithms [95] and data partitioning techniques [505] to minimize unnecessary data collection and store user data locally on edge devices rather than centralized cloud storage. Moreover, we argue for the use of mobile applications to improve the protection of workers' privacy, alongside the adoption of perturbation methods and differential privacy, which have demonstrated effectiveness in privacy protection [247, 481]. Nevertheless, striking a balance between privacy protection and household security requirements remains challenging.

#### 6.5.3.2 Semiotics For Smart Devices

We reiterate our previous recommendation regarding semiotics (cf. Section §5.5.3.2), urging designers to delve deeper into semiotics to assist them in designing culturally sensitive and appropriate signals for smart devices, including both verbal and non-verbal communication. Smart devices introduce novel and more sophisticated interaction methods compared to previous technologies, leading to diverse interactions with various stakeholders, including children, adults, the elderly, disabled users, and bystanders such as neighbors, guests, or domestic workers. To ensure effective communication regarding privacy concerns with smart devices, it is imperative for these devices to utilize consistent signals that resonate with the target audience. Thus, we assert that exploring the field of semiotics holds substantial potential for advancing the state of the art in the design of smart devices [9, 98]. However, as discussed previously, 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, presents significant challenges.

#### 6.5.3.3 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) [498, 506, 507]. 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. [508] 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.

#### 6.5.3.4 Responsible Innovation

We note that many of the issues we have uncovered are strongly aligned with the principles of responsible innovation (RI) [92, 93]. 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[30] framework [509], which encourages innovators to foresee unintended consequences, reflect on the goals and motivations driving innovation, involve affected communities through open dialogue, and take action to shape the course of innovation is crucial. We also argue for the implementation of a certification system that can identify those who adhere to ethical and responsible practices in data protection and integrate data protection seamlessly into their design processes. This certification system, we believe, would align with global efforts aimed at fostering more ethical design practices [510–512].

### 6.5.4 Business Considerations and Interventions

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

#### 6.5.4.1 Address Cost Challenges in Privacy Protection Design

As presented in Sections §6.4.2.2.1, §6.4.2.2.2, and §6.4.2.2.3, findings showed that cost represents a challenge for considering non-Western (MAME) contextual privacy concerns 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 [513, 514]. To overcome these financial challenges, and informed by outcomes of prior studies and the discount usability engineering movement [144, 515–517], 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 [518]), workarounds, common sense, and 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.

#### 6.5.4.2 Consider Jordanian Context

As discussed in Sections §6.4.1.2, and §6.4.1.3, 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. This, combined with various business barriers and challenges in the Jordanian and MAME region, such as limited market size and smart devices penetration rates[7], lack of local manufacturers, high localization costs, and regulatory limitations, contributes to the overlooking of the Jordanian context. Prior studies [519, 520] have highlighted the influence of unknown and hard-to-manage elements on design processes, including designers' contextual values, norms, and concerns. Other research [521, 522] 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. [523], 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[117] 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 [524, 525] 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[526] compared to larger companies (cf. Section §6.4.1.3). 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).

#### 6.5.4.3 Adopt Ethical and Transparent Design Practices

Sections §6.4.2.1.3 and §6.4.2.1.4 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 [527–534]. These deceptive and unethical design practices, also known as dark patterns, have been variously criticized as bad design, illegal, dishonest, deceptive, and manipulative [527–534]. This 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

[117] IDC-Report about the demand for smart home devices across the Middle East

and family members [474, 475]. Implementing multi-user consent mechanisms in smart home devices is essential to support user agency and free choice [474, 475]. 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 [478, 535–538].

To establish a sustainable and healthy smart device market, companies must delve into ethical business models that prioritize user data, particularly in the context of Jordan and the MAME region. Understanding and utilizing contextual values (social, religious, geopolitical) can guide businesses in shaping practices that align more closely with users' needs. It is crucial to examine how business values and practices impact privacy protection. Therefore, we propose the development and adoption of an *'Ethical Design Framework'* by both regulators and companies. This framework signifies a commitment to honest, respectful, and ethical processes in designing smart devices for various contexts [478, 535–538].

#### 6.5.4.4 Expand Localization to Consider Privacy Concerns

As presented in Section §6.4.1.4, 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 [539–541]. 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 [539–541] involve translating content, considering colloquialisms, dialects, geopolitical sensitivities, regulations, regional settings (currency, measurement units), and avoiding offensive signs and phrases [542, 543]. However, these practices

often overlook privacy concerns [539]. 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.

### 6.5.5 Legal Considerations and Interventions

In previous sections of this dissertation (cf. Sections §6.4.2.2.5, §5.5.2.1.1, and §4.4.3), 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, USA data protection laws –CCPA[43], CPRA[44], Brazil-LGPD[39], India's DPDP[49], Turkey-DPL[38], Malaysia PDPA[50]), 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 emphasize and expand upon our recommendations in Section §5.5.2.1.1, proposing 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[82], Broadband Commission[118], and some industry non-profit organizations such as GSMA[8], and TMForum[83].

[118]Broad Band Commission: The ITU/UNESCO Commission for Sustainable Development

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 highlight the significance of global initiatives [544, 545] in promoting privacy protection design guidelines for smart devices. One example is 'Project Connected Home over IP (CHIP)' [546], 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, we emphasize that 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.

## 6.6 Conclusion

In this chapter, we explored design challenges for privacy protection of domestic workers in smart homes in Jordan. This chapter contributes to a growing body of work on how smart device design can address various privacy concerns of smart home users, including families and domestic workers. To achieve our research goal, we conducted a semi-structured interview-based study with 44 participants, including designers, business leaders, households, and workers. This resulted in a qualitative investigation and a Grounded Theory of smart device design challenges

with privacy protection in Jordan. We summarized the key findings of our study and discussed their implications.

# 7

# CO-DESIGN AND TECHNOLOGY PROBE

This chapter explores design insights on bystanders'[1] privacy concerns in Jordanian smart homes and strategies for protection, with the goal of co-designing a mobile application as a technology probe to gain insights for privacy protection. It addresses the third part of our third research question, RQ 3.3: *"How can we support privacy protection for domestic workers in the smart home in Jordan?"* Employing a mixed-methods approach, Section §7.2 outlines our research approach, incorporating focus groups and semi-structured interviews. We begin by collecting insights to co-design and develop a privacy-focused app (the probe) through four focus groups involving 24 stakeholders. Subsequently, we qualitatively evaluate the app's feasibility and effectiveness with 26 representative stakeholders.

Section §7.3 presents our focus group outcomes, which informed the development of the privacy-focused mobile application as detailed in Section §7.4. The second phase of our study evaluates the feasibility of the app, and we present the findings in Section §7.4.2. The study resulted in a **technology probe study** of a privacy-focused mobile app, to explore design insights into bystander privacy, and to assess how the app as an auxiliary tool can enhance the privacy protection of domestic workers in Jordanian smart homes. We discuss the study findings in Section §7.5.

In this thesis, we use the terms the *'mobile application'*, the *'app'*, and the *'probe'* to refer to the privacy enhancing app, and we use the term *'study'* in this chapter, to refer to our fourth study reported in this chapter unless stated otherwise.

## 7.1 Motivation

Our motivation to conduct a design investigation into bystander privacy concerns and protection means stemmed from insights gained from our prior studies (c.f. Chapters 5, and 6), which revealed users' aspirations to utilize a mobile app to support the privacy protection of bystanders in Jordanian smart homes. Our goal is to gain design insights to co-design a mobile application tailored to domestic workers in these homes and to assess the feasibility and effectiveness of such an intervention.

## 7.2 Methodology and Research Approach

This research study is aimed at addressing the third part of our third research question outlined above. To achieve this goal, and drawing on the insights from our prior studies and other research. [7, 9, 10, 211], we conducted a two-phase study to gain design insights into privacy concerns and protection strategies for bystanders in Jordanian smart homes, aiming to co-design a mobile app as a proposal to address the intricate privacy landscape in this context. It is essential to note that while this initiative represents progress, it is not intended as a comprehensive solution to the multifaceted challenges inherent in the broader privacy context. The first phase focused on understanding users' privacy concerns associated with smart homes in Jordan, and to collect requirements for co-designing a mobile application to support privacy protection of domestic workers in these homes. We designed a qualitative research study utilizing focus group sessions. A total of 24 participants were involved in four focus groups, each group comprise six participants representing households, domestic workers, designers, and mobile app developers. Our focus centered on prevalent smart home devices such as cameras, speakers, lights, and door locks, considering the growing privacy concerns with the increasing adoption of smart

devices in Jordan[10] [10, 11, 547]. Drawing on the outcomes from the first study phase (cf. Section §7.3), and using Thunkable platform[77], the primary researcher prototyped a mobile app in collaboration with another researcher (the researcher's academic advisor). The app consists of various screens, incorporating mock screens to illustrate the envisioned design and active screens that demonstrate the app's actual functionality in supporting bystanders' privacy protection (cf. Section §7.4, and Figure-7.3 for details of the app's screens).

The second phase of the study aimed to assess the viability and effectiveness of the prototype mobile application in enhancing privacy protection for domestic workers in Jordanian smart homes. Conducting qualitative research through semi-structured interviews, we engaged with 26 participants, including four smart device designers, six households, seven domestic workers, four regulators, and five recruiters. Participants were introduced to the app's functionalities and encouraged to interact with it for three weeks. Our focus was on ensuring participants' understanding of the app's primary features and its main purpose in supporting privacy protection, rather than eliciting feedback about its practical use in real-world contexts. Following this, we conducted semi-structured interviews to gather participants' perspectives on the viability and effectiveness of the app as an auxiliary tool for supporting privacy protection of domestic workers in smart homes.

In both study phases, similar to our approach in Chapters 4, 5, 6, and to prevent potential harm or ethical concerns while ensuring the freedom and unbiased participation of domestic workers, we took measures to avoid recruiting workers and households from the same homes. However, for other participants like designers, developers, recruiters, and regulators, we did not rule out those who might be connected. Consequently, we recruited households and workers from a diverse pool of 14 different households.

In this chapter, specific terms are used to categorize participants: *"Designers"* for those involved in smart device design, *"Household Users"* for local users of smart home devices, *"Domestic Workers"* for passive bystanders in smart homes, *"App developers"* for mobile app developers, *"Recruiters"* for heads of recruiting agencies,

*"Regulators"* for labor law and data regulators. Throughout the transcripts of both study phases, we employ an abbreviation system to identify participants. The system consists of a letter followed by two numbers, where the letter represents the participant type (i.e., [D] for designers, [H] for household users, [W] for domestic workers, [M] for mobile app developers, [A] for recruiters, and [R] for regulators), The first number indicates the focus group number, and the second number represents the participant's identifier within that specific focus group. For the identifier that denotes focus group number, we assigned zero to indicate that the participant did not participate in the focus group phase of the study. For example, [D1_1] refers to designer one in focus group one, [H2_1] signifies household one in focus group two, [W3_1] denotes domestic worker one in focus group three, [M4_1] represents mobile app developer one in focus group four, A0___2 signifies recruiter two, and R0___3 denotes regulator three. [G2] denotes focus group two.

### 7.2.1 Recruitment

We developed a screening questionnaire to identify potential candidates who met our criteria (cf. Appendix E.3 for details of the screening survey). This criteria is :

- For designers, mobile app developers, regulators, and recruiters to have a minimum of two years of experience in their respective fields;
- For household heads, to have an active role in decisions regarding smart devices and domestic workers;
- For domestic workers, to have access to the internet and smartphones within homes they are employed in;
- For all candidates, to have basic knowledge of smart home devices and privacy;
- For all candidates, to have general knowledge of MAME[14] 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 be audio recorded.
- For all candidates, it is required to be above 18 years old.

In the first phase of the study, the objective was to gather design insights on privacy from direct users (domestic workers and households) to co-design the app. Additionally, we included designers of smart devices that the app aims to support privacy protection with, and mobile app developers who will ultimately develop the co-designed app. Therefore, we recruited users (workers and households), along with designers of smart devices and mobile app developers, for the first study phase to gather their insights about privacy and power dynamics, and to co-design the proposed app. For the second study phase, which aims to assess and evaluate the viability and effectiveness of the app, in addition to including participants from the first study phase, we included participants who are not direct users of the app but play a significant role in the privacy protection of bystanders in the smart home and might have indirect interaction with the app implementation rather than directly using the app. These newly added participants include labor law and data protection regulators in Jordan (regulators) and heads of the recruiting agency for domestic workers (recruiters). Introducing new participants during the evaluation phase helped us gain comprehensive design insights into bystanders' privacy concerns, the power dynamics of smart homes in the Jordanian context, and how we could co-design the app to effectively support privacy protection.

To recruit households, and domestic workers from Jordan, similar to our approach in Chapters 4, 5, 6, we advertised the study on social media groups, reached out to smart device sellers and domestic worker recruitment agencies, and used snowball sampling. We established connections with nine candidate households and 10 candidate domestic workers. To recruit smart device designers and mobile app developers, similar to our approach in Chapter 6, we advertised the study on Linkedin specialized groups. Additionally, we searched the internet (i.e., Google, and Linkedin) to identify and reach out to potential candidates according to their

professional profiles. We encountered similar challenges as those faced in Chapter 6 when recruiting designers willing to share their views and experiences with privacy and data protection. Therefore, many candidates chose not to participate, citing non-disclosure agreements (NDA) and business confidentiality obligations. To address this challenge, participants were briefed on our ethical, and security measures, with a focus on data encryption and compliance with GDPR[29]. Additionally, we employed snowball sampling [443, 445, 446]. In the beginning, we recruited two smart device designers, and utilizing snowball sampling, we were introduced to another seven designers. To recruit mobile application developers we advertise the study on some Linkedin specialized groups and we managed to make connections with seven developers. For the first phase of the study, we established connections with 35 candidates, including nine households, 10 domestic workers, nine smart device designers, and seven mobile app developers. We initiated contact with all 35 candidates using email and phone calls to request and schedule interviews. Out of this pool, 29 candidates showed interest and completed a screening questionnaire. Ultimately, 24 participants from diverse backgrounds were successfully recruited, comprising seven household heads, seven domestic workers, six designers, and four mobile app developers. These participants formed the basis for creating four focus groups, each with six members representing their respective categories.

In the second phase, we included recruiters and regulators in the app evaluation. Utilizing snowball sampling [443], we reached out to domestic worker recruitment agencies and public-private entities in Jordan, such as MODEE[54], ICT companies, and Mobile Operators. We established connections with 12 candidates: five regulators and seven recruiters. Ten candidates completed the screening questionnaire, resulting in the recruitment of four regulators and five recruiters. In addition to the newly recruited participants (regulators and recruiters), we extended invitations for the second phase to 12 participants from the focus groups, excluding app developers, prioritizing input from workers, households and designers. As the study progressed, we invited a further 5 new participants from the focus groups to ensure sufficient

saturation [419], concluding the second phase with a total of 26 participants (17 from the focus groups and 9 new stakeholders).

#### 7.2.1.1 Participant Demographics

The demographic information of the 33 participants in both phases is presented in Table 7.1. Among the participants, there were four female workers and three male workers. In terms of household heads, there were three female and four male household heads. All the designers, mobile app developers, recruiters and regulators were male. While this represents a limitation, we discuss its impact in Section §7.2.5. Regarding the occupational backgrounds of our households, two participants work in education sector, one in ICT, one was an HR manager, one was a lawyer, one was a marketing manager, and one was a housewife. Among the seven domestic workers, three were from Jordan, one was from the Philippines, one was from Ghana, one was from Bangladesh, and one was from Ethiopia. Three domestic workers were home nurses, three were maids, and one was a babysitter. All designers and mobile app developers were affiliated with international companies, except for two mobile app developers from Jordan. Similar to our approach in all studies, to assess users' competence with smart devices, we adopted the widely recognized Dreyfus' model of skill acquisition [457], which categorizes individuals into different stages of skill development: Novice (Basic), Competent, Proficient, and Expert.

### 7.2.2 Methodology

#### 7.2.2.1 Focus Groups and Interviews

Focus groups, a valuable research tool for discussing perceptions and generating concepts [430, 431], typically involve six to twelve participants, promoting open dialogue and opinion development in a social context [430, 432]. Challenges in recruiting participants may arise [433]. Moderators, like the primary researcher in this study, guide discussions, encouraging diverse viewpoints while maintaining impartiality [434]. Discussions are recorded, transcribed, and analyzed thematically [435]. From January to April 2023, four focus group sessions with six

**Table 7.1:** Demographic Information of Participants

| P# | Focus Group# | Phase | Gender | Nationality | Age | Education | Role | Experience (Years) | Company Size | Competence | Used Smart Devices |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **H1_1** | | 1 & 2 | Male | Jordan | 40-49 | B.Sc. | Teacher | 10 | | Basic | Smart Camera, Sony Smart TV |
| **W1_1** | | 1 & 2 | Male | Jordan | 30-39 | B.Sc. | In Home Nurse | 5 | | Basic | Google Home, Smart Camera |
| **W1_2** | **G1** | 1 & 2 | Female | Ethiopia | 20-29 | High School | Maid | 2 | | Basic | Smart Security, Smart Camera |
| **D1_1** | | 1 & 2 | Male | England | 50-59 | B.Sc. | UX Designer | 12 (SME) | SME | Proficient | Smart Thermostat, Smart Door Lock |
| **D1_2** | | 1 | Male | England | 30-39 | B.Sc. | UX Designer | 4 (SME) | SME | Proficient | Smart Thermostat, Smart Door Lock |
| **M1_1** | | 1 | Male | India | 20-29 | B.Sc. | App Developer | 4 | SME | Expert | Google Nest Audio, Smart Cameras |
| **H2_1** | | 1 & 2 | Male | Jordan | 30-39 | M.Sc. | ICT Manager | 6 | | Expert | Smart Camera, Smart Light |
| **H2_2** | | 1 & 2 | Male | Jordan | 40-49 | B.Sc. | Marketing Manager | 11 | | Basic | Smart TV, Smart Camera |
| **W2_1** | **G2** | 1 & 2 | Male | Jordan | 30-39 | B.Sc. | In Home Nurse | 7 | | Basic | Amazon Echo Dot, Smart Cameras |
| **W2_2** | | 1 & 2 | Female | Ghana | 20-29 | High School | Maid | 4 | | Basic | Smart Cameras, Smart TV |
| **D2_1** | | 1 & 2 | Male | German | 40-49 | M.Sc. | Solution Architect | 9 (SME) | SME | Expert | Smart Light, Smart TV |
| **M2_1** | | 1 | Male | Jordan | 30-39 | B.Sc. | App Developer | 8 | SME | Expert | Smart Speakers, Smart Plugs |
| **H3_1** | | 1 & 2 | Female | Jordan | 30-39 | PhD | University Professor | 7 | | Competent | Google Home, LG Smart TV |
| **H3_2** | | 1 | Female | Jordan | 30-39 | B.Sc. | Lawyer | 8 | | Basic | Smart TV, Smart Camera |
| **W3_1** | **G3** | 1 & 2 | Female | Philippines | 30-39 | High School | Babysitter | 6 | | Basic | Smart Camera , Smart Lights |
| **D3_1** | | 1 & 2 | Male | USA | 20-28 | B.Sc. | Firmware Designer | 5 (Large) | Large | Expert | Google Home, Smart Camera |
| **D3_2** | | 1 | Male | USA | 30-39 | B.Sc. | UX Designer | 9 (SME) | SME | Expert | Smart Security System, Smart Lights |
| **M3_1** | | 1 | Male | Jordan | 30-39 | B.Sc. | App Developer | 7 | SME | Expert | Amazon Echo Dot, Smart TV |
| **H4_1** | | 1 & 2 | Male | Jordan | 30-39 | M.Sc. | HR Manager | 6 | | Competent | Smart Camera |
| **H4_2** | | 1 & 2 | Female | Jordan | 40-49 | B.Sc. | Housewife | 5 | | Basic | Smart Camera |
| **W4_1** | **G4** | 1 & 2 | Female | Bangladesh | 20-29 | High School | Maid | 4 | | Basic | Smart Camera, Smart Door Bell |
| **W4_2** | | 1 & 2 | Male | Jordan | 30-39 | Diploma | In Home Nurse | 7 | | Basic | Smart TV, Samrt Camera |
| **D4_1** | | 1 & 2 | Male | USA | 20-29 | M.Sc. | Firmware Designer | 5 (Large) | Large | Expert | Google Home, Smart Camera |
| **M4_1** | | 1 | Male | India | 20-29 | B.Sc. | App Developer | 4 | SME | Expert | Smart Camera, Amazon Echo Dot |
| **A0_1** | | 2 | Male | Jordan | 30-39 | B.Sc. | GM Recruiting Agency | 4 | | Basic | Smart Camera |
| **A0_2** | | 2 | Male | Jordan | 50-59 | B.Sc. | GM Recruiting Agency | 9 | | Competent | Smart Camera, Smart TV |
| **A0_3** | | 2 | Male | Jordan | 40-49 | B.Sc. | Director Recruiting Agency | 7 | | Competent | Smart Camera, Smart TV |
| **A0_4** | | 2 | Male | Jordan | 50-59 | M.Sc. | Director Recruiting Agency | 12 | | Basic | Smart Camera |
| **A0_5** | | 2 | Male | Jordan | 30-39 | B.Sc. | GM Recruiting Agency | 6 | | Basic | Smart Camera, Smart TV |
| **R0_1** | | 2 | Male | Jordan | 40-49 | B.Sc. | Labour Law Expert | 8 | | Competent | Amazon Echo Dot, Smart Camera |
| **R0_2** | | 2 | Male | Jordan | 40-49 | B.Sc. | Regulatory Team Leader | 9 | | Competent | Smart Camera, Smart Heating System |
| **R0_3** | | 2 | Male | Jordan | 40-49 | B.Sc. | Regulatory Expert | 11 | | Expert | Smart Camera, Smart Door Lock |
| **R0_4** | | 2 | Male | Jordan | 40-49 | B.Sc. | ICT Regulation Manager | 9 | | Competent | Smart Lights, Smart Camera |

participants each were conducted, followed by 26 semi-structured interviews in June, July, and November 2023. Our methodology in both phases adhered to the funnel technique [413], transitioning from general to specific inquiries. We have explained the funnel technique in Section §3.2.1. Remote sessions and interviews were conducted via Zoom, with audio recordings. Participants were given the opportunity to express thoughts, share insights, and seek clarifications. While a prepared question set was followed, adaptability was maintained by incorporating follow-ups and excluding redundancies. (cf. Appendix E.4, and Appendix E.5 for focus group, and interview guideline details).

During the focus group phase, participants provided insights into smart devices, usage patterns, and their understanding of data protection rights [460, 485]. We delved into their perspectives on data collection practices, trust levels concerning smart devices, and strategies for enhancing data protection. Specifically, we inquired about their opinions regarding the potential adoption of a mobile app as a supplementary tool to protect domestic workers' privacy in smart home environments. This approach primarily aimed to gather participants' thoughts on the viability and effectiveness of such an app, desired key features, as well as potential challenges and associated concerns. In the second phase, participants provided views on the

potential for the probe (the app) for supporting privacy protection with smart home devices. They discussed how such an intervention can educate users about privacy risks, balance power dynamics, facilitate privacy discussions among households and workers, scan for smart devices and notify users, and perform other functions like collecting user feedback to improve privacy features. This approach uses the app as a technology probe to actively engage users, gather insights, and enhance privacy practices within smart home environments.

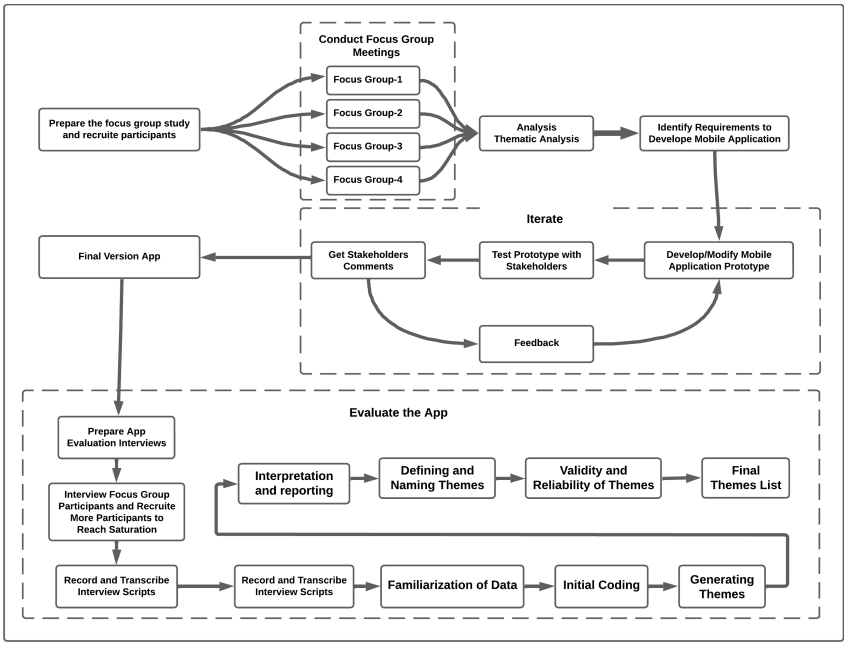
All participants, including the newly added regulators and recruiters, offered valuable insights to enhance the app's design and features. We refined the app based on their suggestions through an iterative feedback process. To mitigate response bias [460, 485], we started with general inquiries about privacy concerns and the app's concept, and avoided leading questions. Both the focus groups and interviews were conducted in English and Arabic by the primary researcher. All focus groups were in English, while interviews were bilingual, with nine in Arabic. The information sheet and advertisements for the study explicitly invited volunteers, who willingly contributed their time without compensation.

#### 7.2.2.2 Co-Design Approach

Informed by insights from prior research on co-design promoting collaboration between designers and end-users [450], we employed a participatory design process to investigate bystanders' privacy concerns and protection strategies in Jordanian smart homes, with the goal of co-designing and developing a mobile app to enhance the privacy of this vulnerable user group (cf. Fig-7.1). Given the prevalent use of smartphones in Jordan[119] and the streamlined development and adoption of mobile apps [548], developing a mobile app emerged as a practical solution. This decision was further substantiated by our previous studies' findings (cf. Chapters 5, and 6). Based on insights from the first phase, we developed a mobile app prototype, iteratively refining it with feedback gathered during the second phase for comprehensive evaluation.

[119]Jordan: Digital Report-2021

**Figure 7.1:** Research Process and Applied Methodology [Co-Design Approach]




#### 7.2.2.3 Pilot Study

A pilot focus group study was conducted to ensure the clarity of focus group questions and to address any issues with the discussion scripts. For this, a convenience sample of four experienced researchers from our institution, with pertinent backgrounds, was selected [549]. This pilot study included one focus group session. Feedback indicated that the focus group scripts required no significant modifications, mainly focusing on phrasing of discussion topics, sequencing, and clarity enhancement. Similarly, the same four researchers who participated in the pilot focus group were consulted for refining the semi-structured interview scripts. Their input was sought to assess question clarity, depth, and comprehensiveness. Similar to the focus group scripts, no major adjustments were suggested for the interview scripts. The pilot study feedback primarily aimed at enhancing question phrasing, sequencing, and overall comprehensibility.

### 7.2.3 Data Analysis

Thematic analysis [421] was chosen as the methodology for both phases of our study. We have explained thematic analysis in Section §3.2.2. The research process and

methodology applied are illustrated in Figure 7.1. The focus group data underwent systematic thematic analysis to explore privacy concerns related to smart home devices. The dataset, consisting of professionally transcribed audio recordings, was also analyzed using NVivo 12 Pro[76] software similar to our approach in the previous studies. The analysis, guided by iterative open coding [451] and Braun and Clark's thematic analysis approach [421], involved two researchers. The other researcher (the researcher's academic advisor) sought clarifications and insights during coding, while the primary researcher added contextual notes. The initial codebook was collaboratively developed, and for credibility, we cross-referenced codes with focus group transcripts. Discrepancies in initial codes were addressed through joint review, resulting in the final codebook. Inter-rater reliability was assessed, yielding a Cohen's kappa coefficient ($\kappa$) of 0.85, indicating near perfect agreement [438]. A total of 138 codes were identified and organized into categories and themes discussed in Section §7.3.

In the second phase, we systematically applied thematic analysis to the data, recording and transcribing interviews. Following a similar approach to the focus group, we used iterative open coding [451] and Braun and Clark's thematic analysis method [421]. NVivo 12 Pro software facilitated the coding process. A collaborative initial codebook was created, cross-validated against interview transcripts for validation. Reviewing initial codes and supporting quotes, any discrepancies were resolved through discussion, resulting in the final codebook. Inter-rater reliability remained near perfect [438] (Cohen's kappa coefficient, $\kappa = 0.82$). Additionally, we tested the codebook's reliability and credibility using triangulation [437] by randomly selecting eight participants (two workers, two households, one designer, two recruiters, and one regulator) to comment on the identified codes and themes. Clear consensus emerged, with feedback adding details without generating new themes. In total, we identified 87 codes, organized into categories and themes in Section §7.4.2. Data saturation [414, 419] was observed separately for each study phase, occurring between the 3rd and 4th focus group in the first phase and between the 24th and 25th interviews in the evaluation phase.

### 7.2.4 Research Position and Ethics

We acknowledge our positionality [461] and its potential influence on both participants and research outcomes, prioritizing ethical values such as fairness, freedom, and accountability. Our objective in this study is to investigate bystander privacy concerns and protection means in Jordanian smart homes through a co-design approach, aiming to understand the impact of smart technologies on privacy and power dynamics. Framing our study as an examination of privacy and power dynamics within Jordanian smart homes to address concerns, empower users, and enhance privacy protection, we aim to develop a mobile app as a supporting tool for bystanders' privacy protection.

We took precautions to ensure that our views did not bias the research process. These precautions included designing our focus group and interview guides to avoid leading questions, positioning the study as an exploration of privacy and interpersonal implications of smart technology, and employing two coders to ensure the reliability of data analysis. We prioritized participant anonymity and privacy, actively searching for evidence of any illegal treatment (which was not found). Aiming for neutrality, we focused on reporting rather than intervening in potential instances of unfair technology use. Challenges persist in this research domain, and future studies may necessitate standardized research strategies and protocols for identifying, assessing, and resolving such instances. Despite acknowledging study limitations, including potential biases, we maintain confidence in the validity of our findings. Ethical considerations were paramount, with approval obtained from the University of Oxford - Central University Research Ethics Committee (CUREC) [Approval: CS_C1A_23_012]. Participants provided oral consent, assured of strict confidentiality and the right to withdraw without explanation. No participants opted to withdraw from the study, and focus group and interview scripts were securely encrypted and stored. For details of the ethics application, refer to Appendix G.4.

### 7.2.5 Limitations

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

a) Language: While the focus group sessions were conducted in English, the choice of English or Arabic interviews was provided in the second phase, for those who can speak Arabic. Translated Arabic interviews were precisely managed to preserve original perspectives. Challenges in coherence were faced by some non-native English speakers due to language nuances. Nevertheless, minimal impact on analysis was found during validation of results.

b) Qualitative research quality depends on researchers' skills and potential biases. Novice researchers may encounter difficulties in conducting effective focus groups, interviews, posing probing questions, and exploring critical subjects, potentially leading to overlooking of relevant data [462]. The depth of data collection significantly relies on moderators' and interviewers' expertise, as well as question quality [486]. To address this, a skilled researcher moderated the four focus groups and conducted the 26 interviews, utilizing neutral and open questioning techniques to prevent influencing participants' responses.

c) Self-Reporting Bias is a common challenge in qualitative research [463], leading participants to forget details or provide inaccurate responses. Additionally, participants may adjust their answers based on their perception of researchers' viewpoints, introducing bias [464]. To improve validity and reduce self-reporting bias, proactive measures were taken, which involved employing open-ended questions to elicit comprehensive responses. Additionally, concise answers prompted further inquiries to gather additional information, ensuring a thorough understanding of the participants' perspectives.

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

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

f) We acknowledge a limitation in gender diversity among our participants, as we were only able to recruit male designers, mobile app developers, recruiters, and regulators. While this limitation may have influenced their perspectives, we believe it did not significantly impact the effectiveness of the study outcomes. Our focus was primarily on gathering professional perspectives rather than personal experiences.

g) The qualitative nature of the study means its findings are not intended for generalization, but rather for a deep understanding of participants' perspectives. The study's focus is on exploring complex issues, not creating broadly applicable conclusions. Thus, hypotheses arising from this study would need confirmation in further research for broader relevance and applicability.

## 7.3 Findings of the Focus Groups Study

The section outlines the findings from our focus groups, emphasizing design insights for co-designing a mobile app for privacy protection tailored to domestic workers in Jordanian smart homes. The identified two categories: "Privacy Protection with the App" and "Considerations and Challenges," shed light on how users navigate privacy threats with smart devices and the intricate tensions between households and workers. The findings further explore potential privacy protection strategies, offering participants' perspectives on a privacy-focused mobile app and emphasizing expected features and functionalities. The section also addresses challenges, including the adoption strategy of the app within asymmetric power dynamics that favor households in Jordan. Additionally, it highlights legal considerations and technical requirements. The findings in this study converge with, and complement some of our previous studies' findings (cf. Chapters 5, and 6), with a specific focus on themes related to privacy concerns, regulatory considerations, and power dynamics. We

emphasize that the repeated occurrence of these patterns strengthens the reliability, robustness, and credibility of our research findings, underscoring the significance and authenticity of our research within the examined context (cf. Table 7.2 for the identified Categories and Themes).

**Table 7.2:** Focus Groups - Categories and Themes

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

## 7.3.1 Privacy Protection with the App

This section presents privacy concerns and power dynamics, explores the potential for protection with the app, details the app's proposed features, and outlines privacy protection strategies. Further details are provided in the following sections

### 7.3.1.1 Privacy Concerns and Power Dynamics

**7.3.1.1.1 Privacy Concerns.** Adding more details to our previous studies' insights (cf. Sections §4.3.1 and §5.4.1.3.1), our findings in this chapter highlight unanimous appreciation for the value of smart home devices among participants, acknowledging their benefits in enhancing productivity, simplifying tasks, and improving overall comfort. For instance, [H2_1] noted the convenience and efficiency of remotely controlling the temperature through a smart thermostat. Similarly, [D2_1] emphasized how these devices assist in managing household chores, focusing on time-saving and enhanced manageability. Additionally, [W2_2] acknowledged their value for individuals such as children, the elderly, or those with mobility challenges. Despite these positive views, participants raised significant privacy concerns associated with smart devices, including issues like data collection, potential misuse, unauthorized access, low awareness [H1_1,W1_1], and challenges related

to dark patterns [341] and complex privacy policies [H1_1,D3_1,W1_1,D2_1]. Notably, [H2_2] emphasized the importance of protecting personal data, stating, *"We want to ensure that our data remains private and is not exploited by companies or individuals"*. Concerns specific to workers included privacy breaches through smart devices used for monitoring workers [W2_1], with [W2_2] highlighting challenges reflecting constraints on workers' agency and trust issues.

In line with our previous studies (cf. Chapters 4, 5, and 6), this study uncovered weak awareness and a lack of transparency regarding smart devices and data collection [H1_2,W3_1], limited understanding of data protection rights and regulations [W2_1,H1_1], and challenges related to user consent [W2_1,W2_2], as well as a call for collective responsibility for privacy protection [H3_2,W3_1]. However, participants often argued that the benefits of smart devices outweigh the associated risks [H1_1,H3_1].

**7.3.1.1.2 Autocratic Dynamics and Marginalization Within Domestic Settings.** In conformity with the findings in our previous studies (cf. Sections §4.3.3.5 and §5.5.2.1), findings unveil dynamics within Jordanian smart homes, exposing tensions between workers and households [H4_1,D2_1]. Participants express concerns about privacy, highlighting the delicate balance between convenience and protecting user privacy [H1_1,W2_1,W4_1]. Some households discuss privacy concerns with workers [H3_1], while others avoid such discussions due to trust issues and imbalanced power dynamics [H4_2,W2_1,W3_1]. Both households and workers report concerns around marginalization of workers and contract slavery[81] in Jordanian smart homes. Female foreign workers, often marginalized, express worries about privacy breaches through smart devices [W2_1,W3_1], emphasizing the need for inclusive privacy protection measures to address vulnerabilities in specific user groups and prevent further marginalization [H3_1].

Participants share knowledge of restrictive practices, such as confiscating passports and IDs, limiting movement, and restricting internet and smartphone access [W1_2]. Workers express a desire to discuss privacy needs but refrain due to

potential consequences on their job [W1_1,W1_2]. Participants suggest the app could facilitate such discussions without jeopardizing jobs or relationships with households [D1_1,W2_1,M1_1]. Some households justify restricting workers' access, citing concerns for family security [H4_2]. This situation raises concerns about contract slavery and autocratic household practices. However, some workers report having access to smartphones, internet, and a weekly day off [W4_1]. A growing number of households permit workers access to the internet and smartphones, highlighting diverse practices in managing relationships with domestic workers in Jordanian smart homes [W1_1,H2_2,H3_1].

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

#### 7.3.1.2 Potential for Protection with the App

During the focus groups, participants shared their views on smart devices, privacy concerns, and associated power dynamics. We then engaged in discussions with them regarding their thoughts on the feasibility of the app as an intervention to support privacy protection. We explored how they envisioned such an app, the features they wished to see, and the functions they believed would be useful for privacy protection. These discussions aimed to gather input on proposed features and the associated challenges and concerns. In this section, we present the proposed features for the app, which include educating users, facilitating structured privacy discussions, and implementing essential technical features and functions. These are complemented by privacy protection strategies, such as improving awareness and alleviating power dynamics while fostering trust-building. Further details are provided in the following sections.

**7.3.1.2.1 Proposed Features for the App.** Participants highlighted key app features for effective privacy protection. The proposed features include:

1- Participants emphasized the importance of structured privacy discussions and empowering workers to transparently communicate their privacy preferences, encompassing aspects like data collection, audio/video restrictions, and data storage limits. These discussions were highlighted as crucial for fostering effective and friendly communication with households, as suggested in Section §7.3.1.1.2. To address this, participants[H3_1,W1_2, W2_2, W4_1), proposed leveraging the app to structure and guide simple privacy discussions. The envisioned app would provide households with insights into workers' preferences regarding various privacy aspects, including data types, storage duration and location, sharing protocols for user identification and profiling data, and other privacy preferences demonstrated within the app's interface [D2_1,H3_1]. Moreover, discussions revolved around the potential involvement of recruiting agencies (H3_1, W1_2, W3_1) to oversee communication between households and workers, ensuring continuous updates on workers' status as supported by worker representatives (W2_2, W4_1). However, households raised concerns, prompting designers (H2_2, D2_1) to argue for careful regulatory measures.

2- Information sharing about smart devices and privacy risks. Participants [H4_1,W4_2,H2_1,D1_1] suggested that the app could be utilized to provide information about smart devices, data collection processes, privacy threats, the applicable data protection regulations, privacy protection best practices, and to promote respect for home safety. This would raise user awareness and enable them to make informed decisions.

3- Scanning for nearby devices and providing privacy threat alerts. Participants [D1_2,D2_1,W3_1,W1_1] highlighted the importance of users knowing about existing devices and the types of collected data, and empowering informed actions. [D3_2] emphasized the importance of notifications: *"Notifications... keep users informed and alerted"*. To address this, they proposed that smart home devices should be designed to broadcast information about their type and the collected

data. The app could then receive these information and notify users around the devices accordingly.

4- Inquiries with a privacy advisor via dedicated hotline/chat agents. Workers [W2_1,W3_1] expressed a desire for the usefulness of chatting or discussing with a privacy advisor through a chat channel or hotline. This would assist them in obtaining information about smart devices, privacy threats, and guidance on how to respond in case of privacy breaches.

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

6- Supporting user profiling by sharing identification data with smart devices. Participants argued for the importance of profiling users around smart devices to enable data segregation and facilitate hiding or deleting bystanders' data subject to household permissions. Workers expressed concerns about bystanders' recognition [W2_1]. Designers endorsed the idea of smart devices recognizing multiple users for a multi-user consent mechanism, suggesting that the app support this by collecting users' identification data and sharing it with smart devices [D2_1].

7- Participants [D2_1,M2_1,M4_1] discussed general requirements for the app, such as language accessibility, ease of use, user-Friendly, intuitive design, and inclusivity, ensuring effective use by diverse users, including domestic workers [M2_1,W3_1]. [W3_1] emphasized: *"The app should be available in our language [Filipino] and designed for everyone to understand and use"*. Furthermore, participants argued for separate User Account Management versions for households and workers [M1_1,D2_1,W3_1], available in relevant languages to facilitate the creation of two tailored versions of the app, one for households and another for workers. They also highlighted the need for a comprehensive help and support function [D2_1,M2_1,M4_1].

**7.3.1.2.2 Privacy Protection Strategies.** Adding to the insights we gained from our previous studies (cf. Sections §5.4.2.2, and §6.4.2.1.2), participants in this study suggested recommendations aimed at mitigating power dynamics and ensuring the protection of workers' privacy. They emphasized enhancing awareness of smart devices, data collection, and privacy threats [H2_1,D3_2]. Households emphasized knowledge about surrounding devices, exercising caution in sharing sensitive information, and the significance of staying well-informed about privacy features and risks. [H2_1] said: *"We need to know about devices around us... we take great care when we share data with devices. We don't share our credit card details, and we avoid sensitive conversations or changing clothes close to devices"*. [W2_1] highlighted the pivotal role of user education in addressing smart device privacy threats. [D3_1] argued for devices that empower users with privacy controls and provide clear information about data collection and privacy settings. Workers emphasized open communication and trust-building with households to address power dynamics [W4_2].

Mobile app developers highlighted shared ethical responsibilities [M1_1], and designers emphasized prioritizing privacy, user autonomy, and multi-consent as fundamental ethical principles [D1_2]. Designers and households explored using the app to access multiple smart devices, subject to household permission. Participants acknowledged the app alone cannot fully protect workers' privacy [D1_1,H2_1,W1_1,H3_1], but recognized its value as an auxiliary tool, complementing other actions from various stakeholders. Diverse views emerged: [D3_1] emphasized companies implementing robust privacy measures, [D1_1] highlighted manufacturers' responsibility to inform and empower users, and [H3_2] believed in shared user-company responsibility. [H2_1] acknowledged the role of regulation, [M2_1] emphasized understanding user privacy concerns, and designers emphasized cultural shifts and regulations to empower vulnerable user groups [D3_1], endorsed by workers [W1_1].

### 7.3.2 Considerations and Challenges

This section presents participants' perspectives on developing the proposed mobile app and the associated concerns, including app feasibility, adoption barriers, and legal considerations. Further details are provided in the following sections.

#### 7.3.2.1 Concerns with the App

**7.3.2.1.1 Feasibility and Adoption.** When discussing the feasibility of a mobile app co-designed to support privacy protection, participants highlighted that its success depends on well-designed features and functionalities [D2_1], users' capabilities to use the app appropriately [D1_1], and permitting workers to utilize it [D4_1,W2_1]. [W3_1] endorsed this view, and households affirmed this, stating a preference for restricting device access to only family members due to potential risks [H1_1,H3_2,H4_1,H4_2,H2_1]. Furthermore, participants argue that the importance of the app features and functions lies in their positive impact, which could be summarized by educating and informing users [D2_1], promoting respect for privacy among users (households and workers) [H1_2], encouraging workers to respect home safety, privacy and security [D2_1,D1_1], in addition to the app's ability to structure a privacy discussion between workers and households [W1_1], which is vital for effective and useful communication [H1_1].

In response to users' proposal for the app to facilitate privacy discussions with households (cf. Section §7.3.1.1.2), we questioned the necessity of the app, considering that workers could directly engage in conversations with their employing households. In response to this discussion, some participants acknowledged the possibility of talking directly to households [H1_1,W2_1], while others argued that direct communication with households would not be feasible due to existing power dynamics, autocratic household practices [H2_1], considerations related to empowerment and agency of workers [W1_2,D1_2,W2_2], in addition to weak awareness among workers [W1_2,H2_1]. One worker expressed the view that trust, care for her privacy, and comfort need to be established before discussing privacy needs with the family [W2_2]. Another worker added that discussing

privacy preferences is a sensitive topic with households, as they might become cautious about the worker's intentions, suspecting possible wrongdoings [W1_1], illegal activities [W3_1], unethical behavior [W4_2], or even a crime [W2_2]. This caution could lead to households terminating workers, especially for new workers who are still in the early stages of their work agreement and lack sufficient trust with families [W2_2,H3_1].

To avoid potential consequences of direct communication with families, participants suggest initiating a general discussion about utilizing the app to protect users' privacy, starting from recruitment agencies [D2_1,W2_1]. Other participants endorse the idea, arguing that this could trigger a wider discussion about privacy preferences [W2_2,W3_1,H3_1,H3_2,D4_1], leading to detailed conversations about workers' privacy needs, and might encourage families to agree to app adoption, allowing workers to use it even for short periods during the day or week [D2_1,M2_1,H1_2,W1_2]. In another discussion, when asked about the preference between a mobile application and a website, participants acknowledged the potential of websites but argued for mobile apps as being more user-friendly and convenient [H2_1,D1_1,W2_1].

The adoption of such an app would contribute to improving trust and respect [D2_1], ultimately leading to better relations with households and improved performance of workers [W1_1,H1_2]. Leveraging these advantages and highlighting the positive impact of the app in discussions with households would help encourage them to adopt it and permit its usage among workers [H1_2,W3_1,D4_1,M2_1]. However, households emphasize that families retain the right to evaluate workers and impose restrictions or take disciplinary actions, including termination, in response to negative actions [H1_1,H3_2].

**7.3.2.1.2 Legal and Ethical Considerations.** Participants engaged in discussions concerning the legal considerations associated with developing a privacy-focused mobile app for smart homes in Jordan. Designers emphasized adherence to data protection laws in Jordan and relevant regulations, ensuring respect for

users' privacy rights [D3_1]. Households expressed the same [H3_1] and indicated curiosity to further explore the applicable regulations in Jordan. Workers emphasized informed consent, wanting clear and transparent data collection information, purpose, and access details [W1_1], and households and developers emphasized that the app should support explicit consent and user-controlled data sharing options [H2_1,M4_1]. Moreover, developers underlined the need to define liability and responsibility for privacy protection and highlighted transparent data collection practices through clear, concise privacy policies and disclosures about third-party integration [M1_1].

#### 7.3.2.2 Development of the App

This section presents participants' perspectives on the app development requirements, and the associated challenges.

**7.3.2.2.1 Technical Requirements.** Participants highlighted the technical requirements for the proposed app. Designers highlighted seamless integration with various smart devices. [D4_1] said: *"The mobile app should be compatible with various smart devices"*. Developers emphasized robust security measures, including encryption and secure data storage [M2_1]. Requirements like audio-video recording, location sharing, chat agent, and messaging were discussed [W2_2,H2_2,H3_2,M2_1,M4_1]. Designers emphasized an intuitive UI[106]\UX[100] design catering to diverse users [D3_2]. Continuous technical support and updates were deemed crucial [M2_1].

**7.3.2.2.2 Challenges with the App Development.** Participants discussed technical challenges in developing a privacy-focused mobile app. Key concerns included:

1) *Device Compatibility and Integration*: Developers emphasized the importance of compatibility with various smart devices, mentioning protocols like Zigbee[120],

[120]For more details, see: Zigbee

Z-Wave[121], and Wi-Fi[122]. Support for popular platforms like Amazon Alexa and Google Assistant was also highlighted [M3_1,D3_2].

2) *Scalability and Performance*: App developers addressed the challenge of handling the increasing number of smart devices and optimizing performance. Suggestions included using protocols like MQTT[123] and RESTful APIs[124] for effective communication [M3_1].

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

## 7.4 Developing and Evaluating the App

Drawing on the focus group outcomes, we identified key requirements for developing a privacy-focused mobile app for domestic workers in smart homes in Jordan. This section outlines these requirements and presents the prototype mobile application (the probe) that has been developed.

### 7.4.1 The App Features and Use

We collaboratively developed a prototype mobile app[125] in an iterative process to meet identified requirements (cf. Table-7.3). While not fully implementing all proposed features, the app serves as a demonstration of elements supporting privacy protection. We present the key features and functions in Section §7.3.1.2.1 (cf. Figure-7.2 for a depiction of how users can utilize the app, and Figure-7.3 for details of the app's screens).

The probe (the app) includes operational and mock screens, with certain demo functions for privacy notifications, user profiling, device access and data control, reporting privacy breaches, an advisory hotline, and live chat with a privacy advisor.

[121]For more details, see: Z-Wave
[122]For more details, see: 802.11x: Wi-Fi standards
[123]For more details, see: MQTT: The Standard for IoT Messaging
[124]For more details, see: RESTful APIs: What is a REST API?
[125]Android- Copy of the privacy app

For example, the app features a chat screen with a privacy advisor, indicating a potential need for such a service within Jordan's government. In the absence of an official chatting service, a real-time chat simulation is achieved using OpenAI's[126] API to allow users to test the chat function. Another demo involves reporting privacy violations or seeking information from a proposed official entity, which is currently nonfunctional. The scanning function for nearby smart devices remains restricted, dependent on household permission. In summary, this technology probe (the app), encompassing full range of functional and nonfunctional features, enables us to explore how such an intervention can serve as an auxiliary tool to enhance privacy protection for smart home bystanders.

**Table 7.3:** Requirements for The App

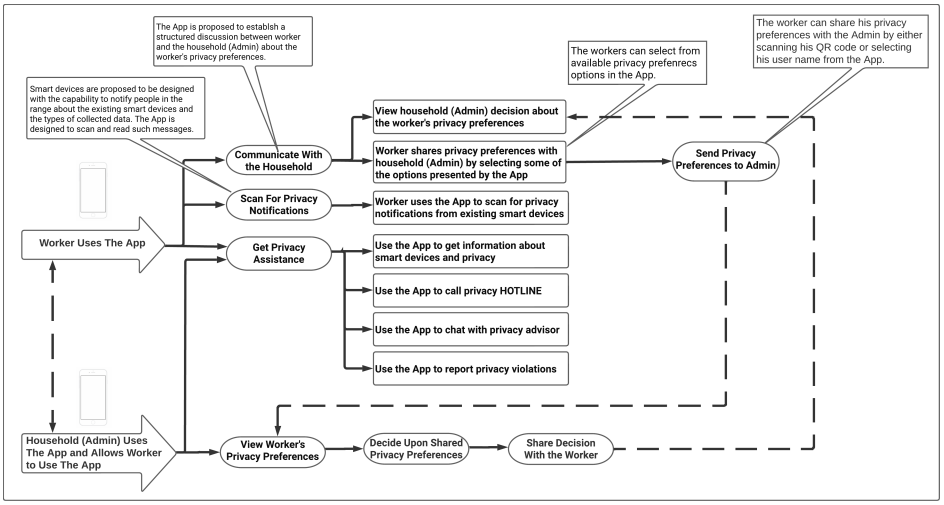
| Requirement | Sub Requirements |
|---|---|
| **The App to have Two Versions** | Domestic Workers and Households (Admin) |
| **User Account Management** | Create Accounts, Reset Password, Settings, and Login |
| | The App to be Available in Relevant Languages |
| | User Recognition and Profiling Utilizing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

### 7.4.2 Evaluation of The App

This section presents the outcomes of the probe (the app) evaluation phase. All participants engaged with the app to assess its potential in supporting privacy protection for domestic workers in Jordanian smart homes. In this phase, we included recruiters and regulators (as mentioned in Section §7.2) to seek their views on the app, even though they are not direct users of the app. However, they are involved indirectly in the privacy protection of domestic workers in smart

[126] OpenAI-API for chat services

**Figure 7.2:** Guidance on How to Use the App

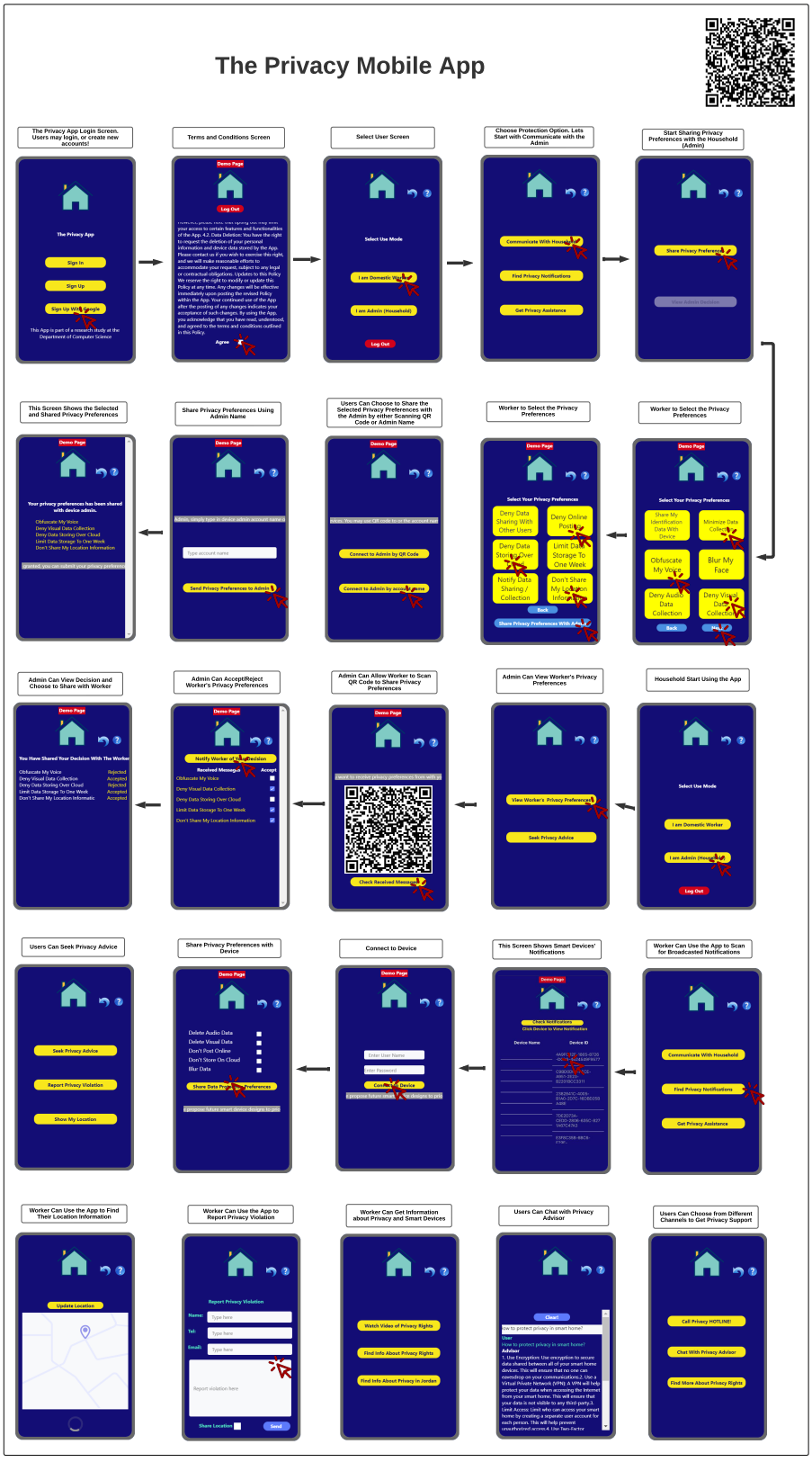



homes. Throughout this phase, we consistently enhanced the app by incorporating participants' feedback and engaging with them for further comments in an iterative feedback process until no further suggestions were received. The results of this phase are presented under two categories. The first category is *"The App Supports Privacy Protection"*, where participants highly appreciated the app's value in fostering privacy discussions between workers and households, educating stakeholders about smart devices, privacy risks, legal rights in Jordan, and the proposed technical features of the app. The second category is *"Barriers Confronting the App"*, where participants discussed potential obstacles, including households' restrictions, workers' limited experience and agency, technical challenges, and strategies for promoting app adoption. In the subsequent sections, we discuss the results (cf. Table-7.4).

**Table 7.4:** Evaluation of the App- Categories and Themes

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

**Figure 7.3:** The Mobile App Screens



#### 7.4.2.1 The App Supports Privacy Protection

This section highlights participant appreciation for the app's role as an auxiliary tool for supporting domestic workers' privacy protection in Jordanian smart homes.

**7.4.2.1.1 Facilitate Privacy Discussion.** Many participants recognized the app's effectiveness in facilitating structured privacy discussions between workers and households that adopt the app and allow their workers to use it [H3_1,W1_2]. They believe that the app establishes a framework for privacy discussions, as it offers a user-friendly interface for workers to share their privacy preferences [D4_1,W4_2,A0_1], and enables households to gain insight into these preferences, fostering collaborative privacy discussions [H1_1,A0_3], and enhancing understanding and trust between workers and households [D4_1]. They added that the app enables workers to make informed decisions by informing them about smart devices, privacy threats, and rights [H2_2,W1_1,A0_2,D3_1]. However, some participants argued that households retain the ultimate decision in their homes [H3_1,A0_4,W2_1,R0_1].

**7.4.2.1.2 Educate Stakeholders.** Many participants acknowledged the app's role in educating stakeholders about smart devices and privacy threats, emphasizing the need for regular updates [H2_1,W2_1,W4_1,A0_5,R0_3]. Improvements were suggested which included providing detailed explanations of device functionalities, privacy practices, and risks to empower informed decision-making [W1_2,W4_1,A0_3]. The app was valued for raising awareness about privacy rights in Jordan and offering information on legal rights [R0_2,R0_4,W1_1,H4_1]. Understanding these rights was seen as crucial for fostering respectful and privacy-conscious environments [H2_1,W4_2,A0_1]. The provision of privacy best practices and practical tips for workers and households was highly appreciated, and participants thought this could significantly enhance privacy protection [H2_1,W2_1,W4_2,A0_4, W4_2]. Among workers, the feature for reporting privacy breaches was particularly endorsed [W3_1], and humorously referred to as 'The Privacy Police' by households [H4_2]. Workers, recruiters, and households all acknowledged its

value in expanding the collective knowledge of privacy threats and protection practices [H4_1,A0_3,W4_2].

**7.4.2.1.3 Technical Features.** Many participants were satisfied with the technical features in the app. These include: scanning and discovering smart devices, establishing connections with devices to view and manage collected data, and notifying workers about existing smart devices and potential privacy threats, all subject to households' permission [W4_2,A0_5,R0_1]. They believed that this helps to support more informed privacy decisions [H4_2,A0_4,D2_1]. Some participants argued that the app could support smart devices for user profiling and data segregation by collecting user identification data and sharing it with the devices, subject to household's permission. Many participants valued user profiling for data segregation [W4_2,A0_1], although concerns arose regarding family members' data mixing [H3_1,R0_1], as workers often stay with family members, and the data collected for workers may also include information about other family members, making it challenging to separate data [H2_1].

### 7.4.2.2 Barriers Confronting the App

This section outlines identified barriers to app adoption and usage. Understanding and addressing these challenges is crucial for optimizing app utilization. These barriers include:

**7.4.2.2.1 Households' Restrictions.** Households' restrictions on worker access to the internet and smartphones pose challenges, potentially hindering app usage. The study revealed key factors contributing to households' resistance in adopting the app and engaging in privacy discussions with workers [H4_2,A0_5,W1_2]. These factors encompass household autonomy, as households emphasize their final say and ultimate authority in decisions affecting their homes [H1_1,H2_1,H4_1]. Participants discussed that power imbalances within the household-worker relationship contribute to challenges in privacy discussions, leading to restrictions on app utilization, with workers expressing fear of job loss [H4_1,W2_2,A0_1]. Moreover,

participants noted that some households avoid open discussions with workers due to reasons such as a lack of trust [H2_2,A0_5], and weak awareness about privacy risks [H4_1]. Trust issues manifest as some households distrust workers, fearing data misuse or privacy breaches [H2_1,W1_2,A0_2]. Participants emphasize the necessity of addressing household restrictions on app adoption by raising awareness among households and communicating the positive impact of the app on workers' performance, their relationships with households, and the overall security and safety of the home [R0_2,D3_1]. Moreover, findings underscore the importance of open discussions and building trust to create a respectful and trustworthy environment that values workers' privacy, and home safety [A0_4,R0_3,D4_1,H2_1].

**7.4.2.2.2 Strategies for Promoting App Adoption.** Participants discussed several strategies to enable app utilization in smart homes. These strategies include:

a) **Promote App Adoption Among Households**: Participants emphasized the need to promote household use of the app for creating a privacy-conscious environment [A0_5,D3_1]. Suggestions included awareness campaigns through social media, booklets, and community groups to educate households about the app's role in improving the overall home environment and the qualities of relationships (i.e., trust, respect) with workers. The aim is to encourage open privacy discussions that lead to building trust, promoting the app's value, and potentially increasing app adoption. [H3_1] noted: *"I think many families do not understand how important it is to respect the privacy of the workers... If we help them understand, workers will become more respectful of the privacy of households, and this will have a positive impact on their relationships with families and contribute to building a healthy home environment".*

b) **Encourage Recruitment Agencies to Incorporate the Use of the App into the Work Contract**: Most participants acknowledged the pivotal role of recruitment agencies in shaping relationships and employment contracts between workers and households [H3_1,W2_1,D3_1,A0_3,R0_4]. The inclusion of app adoption clauses in work contracts was deemed crucial for protecting workers' privacy

rights [W2_1,W3_1,H3_1,H4_2]. Recruiters endorsed the idea [A0_3,A0_5]. However, concerns were raised about potential challenges due to the lack of explicit regulation, highlighting imbalanced power dynamics favoring households [A0_1]. Recruiters emphasized that while workers seek employment, they may defer to household decisions in case of disagreement. [A0_2] mentioned, *"If households disagree, I believe workers will ultimately defer to household decisions"*. Participants underscored the importance of educating recruitment agencies about the app's functionalities and benefits [A0_3], enabling effective communication of its value to workers and households for broader adoption in smart homes [H2_2].

c) **Encourage Workers to Only Accept Jobs that Permit them to Use the App**: Some participants noted that encouraging workers to prioritize jobs that allow them to access the internet and use smartphones and similar apps can significantly enhance their privacy protection [W1_1,W3_1,H3_1]. Recruitment agencies, social entities, and relevant organizations can conduct workshops and awareness campaigns to inform workers about such app's capabilities and how it could support privacy protection [W2_2,D1_1]. Recruiters endorsed the proposal but expressed concerns due to economic power dynamics that do not favor workers [A0_3].

**7.4.2.2.3 Workers' Limited Experience and Agency.** Findings uncovered that some workers may face challenges using the app due to limited experience and technical skills [W4_2,A0_4,R0_2]. This includes a lack of familiarity with technology, making it difficult for them to navigate the app's features and set privacy preferences effectively [W1_2,A0_4]. [W2_1] suggested training programs and workshops for hands-on experience, while households and recruiters recommended ongoing technical support and help-desk services [H2_2,A0_1]. Language and literacy barriers were also identified, with workers struggling to understand the app [W4_2,A0_2]. Providing multilingual support, clear instructions, and visual aids can help overcome these barriers. Additionally, concerns about potential retaliation may lead to workers hesitating to use the app [W2_2,A0_2]. Participants

recommend fostering a culture that prioritizes workers' privacy and ensures positive impacts on the home context [R0_4,A0_1].

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

## 7.5 Discussion and Recommendations

Our third study (cf. Chapter 6) highlights the significance of considering a mobile app in supporting bystanders' privacy protection in Jordanian smart homes. The prevalence and affordability of smartphones[127] in Jordan make mobile apps a practical intervention. This study focuses on exploring design insights to co-design a privacy-focused mobile app aimed at protecting domestic workers' privacy in these homes.

### 7.5.1 Summary of the Findings

Aligning with findings from our previous studies (cf. Sections §4.3, §5.4, and §6.4), and prior research [7, 129], this study provides valuable insights into the privacy of smart home bystanders, the aspirations for protection, and the potential, feasibility and viability of the proposed app (the probe). In the focus groups, our aim was to

[127]Jordan: Smartphone Prices

gather design insights on privacy to co-design an app (a technology probe) to explore potential for privacy protection of workers with smart home devices. The results (cf. Section §7.3) reveal two main themes. Firstly, under *"Privacy Protection with the App,"* participants discuss multifaceted privacy concerns in domestic settings, proposing app features to address challenges and foster an informed and equitable environment within smart homes. Secondly, in *"Considerations and Challenges,"* concerns regarding the app's feasibility, adoption, legal and ethical aspects, and development intricacies are explored.

The probe (the app) evaluation study (cf. Section §7.4.2) unveils two main themes. In the first theme, *"The App Supports Privacy Protection,"* participants commend the app potential for enhancing communication, empowering workers, and educating stakeholders on smart devices and privacy. Technical aspects, including privacy notifications, and user profiling, are highly appreciated. The second theme, *"Barriers Confronting the App,"* addresses challenges such as households restricting worker access, avoiding privacy discussions, workers' limited experience, and technical issues. As discussed in Section §7.4, the development of the probe (the app) was guided by requirements identified in the focus group study. The app encompasses both functional and mock screens, with certain features designed for future activation. Further discussions are provided in the subsequent sections (cf. Figure-7.3 for details of the app's screens).

#### 7.5.1.1 App Adoption and Ethical Consideration

In line with our prior studies [9, 11], this study findings [12] reveal variations in households' practices, with some allowing workers internet and smartphone access while others restrict it to family members. Such restrictions can impede app usage for workers in more restrictive households. We argue that effective deployment of the app relies on discussions with these households, encouraging them to permit workers' app use. Recruitment agencies can play a significant role in initiating and moderating discussions between households and workers, especially during the hiring process, and intervening when necessary to facilitate persuading households

and reaching a consensus. We endorse this suggestion; however, prioritizing home safety and the need for relevant regulations will be necessary.

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

#### 7.5.1.2 The App as a Communication Tool

Findings reveal that spontaneous and unstructured communication between workers and households is often impractical due to existing imbalanced power dynamics (cf. Section §7.3.2.1.1). For instance, in conformity with our previous studies (cf. Sections §4.3.3.5, and §5.4.1.2), workers refrain from initiating discussions about privacy with households, fearing job loss and potential consequences. Similarly, households avoid engaging in privacy conversations with workers due to power dynamics and mistrust. Additionally, the findings reveal that workers lack an adequate level of awareness about smart technologies and associated privacy risks [9, 10, 12]. This weak awareness hinders the workers' ability to discuss their privacy needs effectively with households when these households adopt the app and allow privacy discussions. Therefore, the app could provide practical support to guide and structure an effective privacy discussion between workers and households.

#### 7.5.1.3 The App as an Educational Tool

Complementing our discussion in Section §7.5.1.2, we argue that the probe (the app) can help as an educational tool to enhance the learning experiences of households and workers. This approach aligns with previous studies [550, 551] supporting the use of mobile apps for education. The app can be equipped with relevant resources to offer insights into smart devices, their potential impact on users' privacy, recommended

privacy practices, and an overview of laws and regulations in Jordan governing personal privacy within home contexts, promoting a safe and respectful environment.

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

#### 7.5.1.4 The App to Alleviate and Balance Power Dynamics

Consistent with our previous findings (cf. Sections §4.3.3.5, and §5.4.1.2), and aligned with prior research [7, 178], this study underscores that workers often face restricted autonomy and agency due to power imbalances, tending to compromise their privacy for job security and other benefits. Participants also raised concerns about multi-user consent and accessibility, emphasizing the critical importance of privacy protection, transparent data practices, trust-building, balancing power dynamics, and empowering users to control their data. While it is not a panacea, the adoption of the app could serve as a step in a broader initiative to reshape household-worker relationships and address these imbalances.

Persuading households to adopt the app and enabling workers to use its features can help to foster open discussions, impart knowledge about devices and privacy threats, and provide guidance for privacy protection. Considering the app as an auxiliary tool, complemented by social, technical, and legal interventions, has the

potential to address privacy concerns, alleviate power dynamics, and encourage a secure environment.

#### 7.5.1.5 Concerns with the App

In addition to addressing adoption barriers and ethical considerations, as discussed in Section §7.5.1.1, this study uncovered several challenges with the proposed intervention (the app). These include technological challenges such as the lack of standardized privacy protection design guidelines, resulting in varying data collection practices and privacy settings across different smart devices, thus impeding the app's ability to offer consistent privacy protection. Another issue is the oversight of bystanders' privacy in current smart devices, prompting designers to call for industry collaboration in establishing integrated privacy standards for such apps. They also suggest enhancing the app's capabilities to manage bystanders' privacy preferences or implementing automatic protection mechanisms for bystanders. Overcoming these technical challenges necessitates collaborative efforts among designers, policymakers, and end-users. Furthermore, the study found that some workers face difficulties using the app due to limited technical skills and experience, with suggestions including training programs, hands-on workshops, ongoing technical support, multilingual assistance, and fostering a privacy-focused culture to address language barriers and concerns about potential retaliation, thereby ensuring positive impacts within the home context.

### 7.5.2 Recommendations

In this section, we offer recommendations to stakeholders aiming to enhance privacy protection for domestic workers. These suggestions are based on the insights gained from exploring the potential of the probe (the app) as a part of a comprehensive solution.

#### 7.5.2.1 To Recruitment Agencies

Findings underscore the influential role of recruitment agencies in shaping household-worker relationships. In addition to initiating and moderating app adoption discussions with households, as discussed in Section §7.5.1.1, we argue for recruiters to leverage their influence to incorporate a greater consideration of worker privacy into employment contracts. Given the lack of explicit legislation around domestic worker employment and privacy rights, recruiters would initially need to employ persuasive techniques to encourage households to do this [552], rather than imposing it on households. Additionally, recruiters should take the initiative to educate workers about privacy risks associated with smart devices, utilizing educational materials in languages spoken by the workers (e.g., Philippines[86], Indonesia[87], Ethiopia[88], Ghana[89], and Bangladesh[90]).

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

#### 7.5.2.2 To Users

We recommend that both workers and households acquaint themselves with smart devices and the associated privacy risks. While the probe (the app) and similar tools serve as a central hub for accessing relevant information, additional sources of guidance, such as building informal support networks among domestic workers, can also be beneficial. Households are urged to adopt a trust-building approach with their workers, respecting their privacy requirements and emphasizing home security. Utilizing tools like our app, households can enhance awareness of smart devices and privacy issues, structure discussions with workers, comprehend their needs, and prioritize both home safety and family privacy, thereby fostering trust.

Importantly, workers should use supporting privacy tools (like the probe app) responsibly, prioritizing household safety and security above all else.

#### 7.5.2.3 To Companies and Designers

We argue for the development of smart devices that seamlessly integrate with privacy-enhancing tools like the probe app discussed in this study. These devices should be capable of leveraging data from such tools for user profiling and implementing data segregation measures. Furthermore, we suggest designing smart devices that actively broadcast information regarding their functionalities, data collection practices, and potential privacy risks. This information can be received and processed by these tools (the app), which then notify nearby users about relevant privacy concerns. However, this feature needs to be designed carefully to ensure usability, and should not disclose too much information about household devices which would undermine privacy and security. We suggest utilizing protocols like WiFi(802.11x)[122], BLE[93],Z-Wave[121], Zigbee[120], MQTT[123], UPnP[91] for scanning functions, and to connect to devices.

Furthermore, we urge designers to integrate innovative technologies, such as AI, and adopt differential privacy and data partitioning techniques [95, 505]. Multi-user consent [9, 11, 12, 98] should be accommodated, and semiotics[32] should be considered as a vital tool to ensure culturally sensitive signals in smart devices. We argue that the app can serve as a semiotic tool, aiding in the creation of a language to facilitate privacy discussions between domestic workers and household. Furthermore, the integration of Privacy by Design (PbD) principles [506] is essential, emphasizing the incorporation of privacy considerations at every stage of the design process. PbD should leverage contextual influences and norms, encompassing social, religious, and geopolitical factors. More work should be undertaken to identify common privacy-preserving permissions, both in the app and in smart devices, to mitigate conflicts and ensure widespread household acceptance. We strongly encourage the exploration of ethical business models that prioritize user data protection, emphasizing the adoption of responsible innovation (RI) principles, with adherence to established frameworks, such as the AREA framework[30].

#### 7.5.2.4 To Policy Makers and Social Entities

In Section §2.2.5.2, we highlighted the lack of explicit data protection regulations in Jordan to address privacy conflicts among smart home users. To promote data protection and strike a balance between the needs of workers and households, we complement our previous recommendations (cf. Sections §4.4.3, §5.5.2.1.1, §6.5.5) and urge Jordanian policymakers to consider the adoption of similar apps within regulatory frameworks. We also argue for broader regulatory interventions to navigate the complex privacy landscape and support vulnerable groups, such as domestic workers facing reduced agency and contract slavery [312, 553]. This includes the establishment of privacy advisory chat services, addressing reported privacy violations, and providing guidance on best privacy practices to raise awareness and support privacy protection. We call for collaboration among social entities, policymakers, and recruitment agencies in Jordan to conduct awareness campaigns by leveraging channels like social platforms, public media, the education system, and the proposed app.

As discussed previously, while existing regulations like the European GDPR, USA data protection laws (CCPA[43] and CPRA[44]), Brazil's LGPD[39], India's DPDP[49], Turkey-DPL[38], and Malaysia-PDPA[50] primarily address data protection with service providers, they overlook explicit privacy concerns within smart homes. We emphasize our previous recommendations for governments to collaborate with international organizations (ITU[82], GSMA[8] and TMForum[83]) to address these gaps. Additionally, we emphasize the importance of countries like Jordan enforcing data protection prerequisites on devices before granting market access. Measures such as type approval certificates and data protection tests should be implemented in this regard.

## 7.6 Conclusion

In this chapter, we employ a co-design approach to investigate privacy concerns, power dynamics, and protection means for domestic workers in Jordanian smart homes. Our aim is to co-design and develop a technology probe (mobile app) to

assess it as an auxiliary tool for enhancing privacy protection for this vulnerable user group. To achieve this goal, we conducted a two-phase study. The first phase focused on understanding users' privacy concerns related to smart homes in Jordan and gathering requirements for co-designing the proposed probe. The second phase aimed to evaluate how the probe could effectively enhance privacy protection for domestic workers in Jordanian smart homes. This chapter introduces a technology probe study designed to delve into design insights concerning privacy. The objective is to explore how a privacy-focused mobile app, integrated into a comprehensive solution involving interventions from all stakeholders, can enhance the privacy protection of domestic workers in smart homes in Jordan. We summarize the key findings of the two study phases and discuss their implications.

# 8 DISCUSSION

In this chapter, we engage in a comprehensive discussion of the findings presented in Chapters 4, 5, 6, 7. Initially, we address the oversight of the non-Western context of Jordan in privacy research, especially concerning smart home bystanders[1] (cf. Section §8.2.1). Subsequently, we discuss the increasing privacy concerns among smart home bystanders, especially with the proliferation of smart devices in Jordan and the limited awareness among stakeholders (cf. Section §8.2.2). Following this, we discuss the imbalanced power dynamics between domestic workers and households (cf. Section §8.2.3), along with a lack of explicit data protection regulations for smart home users in Jordan (cf. Section §8.2.4). Furthermore, we discuss the challenges associated with privacy protection design in smart devices (cf. Section §8.2.5). Then, we discuss the feasibility for co-designing and adopting an app (the probe) as an auxiliary tool to support bystanders' privacy protection (cf. Section §8.2.6). Finally, we highlight the importance of adherence to established principles of responsible innovation (cf. Section §8.2.7), and we discuss the technology ethical responsibility in Section §8.3. In this chapter we provide several social, legal, technical and business recommendations for enhancing protection of bystanders privacy in Jordanians smart homes.

## 8.1 Summary of Findings

Our literature review (cf. Chapter 2) revealed the dearth of privacy research in the MAME[14] region, particularly for smart home bystanders in Jordan. Therefore, our research fills this gap and focuses on exploring the privacy concerns of domestic workers (i.e., bystanders) in smart homes in the Jordanian context. This section presents a summary of the outcomes of the collective research conducted through four studies reported in this dissertation. It is noteworthy to highlight that the conducted studies in this research have demonstrated a convergence in some prominent themes and complement each other, particularly with a specific focus on themes related to privacy concerns, regulatory considerations, and power dynamics. The convergence on some of the identified findings fortifies the reliability, robustness, and credibility of our research outcomes, underscoring the significance and authenticity of this research.

Our first study has unveiled five key themes concerning smart home bystander privacy concerns in Jordan: a limited awareness of smart technologies and privacy rights, a basic understanding of privacy notions, audio-visual devices are the most concerning devices, vague regulations, and a lack of explicit data protection and privacy rightsm for smart home users. Additionally, the study explored the impact of imbalanced power dynamics among smart home users (households and workers), exploring the influence of social norms and religious background on privacy concerns, expectations, and rights. Moreover, the study shed light on user aspirations to enhance privacy protection (cf. Section §4.3).

Building on the insights from our first study, our second study examined the complex power dynamics within Jordanian smart homes, which are shaped by contextual norms, customs, religious backgrounds, and economic status. These factors significantly influence and mirror the dynamics and qualities in relationships (e.g., trust and respect) between households and workers in Jordanian smart homes. Moreover, the study explored how smart technologies impact, and reinforce these power dynamics, as well as how these dynamics influence users' privacy concerns with smart technologies. The study findings highlighted a tendency

among domestic workers to compromise their privacy rights to secure benefits and avoid conflicts. Particularly, foreign domestic workers face challenges like contract slavery[81], diminished agency, and marginalization within the Jordanian context. Moreover, the study revealed a gendered dimension, with female workers experiencing reduced rights. The primary concerns for both households and workers revolved around audio-visual devices, including concerns about spying or controlling workers. Additionally, there were concerns about other smart device types (e.g., smart lights and smart door locks). The study affirms the limited awareness among users regarding smart devices and privacy, the lack of explicit data protection regulations for smart home users in Jordan, and concluded by proposing interventions to balance power imbalances, empower domestic workers, prevent technological exploitation, and protect privacy (cf. Section §5.4).

Building on the insights from our first two studies, our third study brought to the forefront the dearth of manufacturers and designers in the MAME region. This scarcity presents a host of challenges for localizing smart devices, as the localization process often overlooks contextual privacy concerns, opting to focus more on superficial aspects like language and regional settings. Furthermore, the study underscores the lack of attention to Jordan and the MAME region in the design of smart home devices. It also sheds light on users' frustrations with deceptive design patterns and complex privacy policies. Additionally, the study examined challenges faced in privacy protection design, including the high cost associated with implementation and the difficulty in aligning data protection with business goals. The findings affirm the limited awareness among users and reveal that limited awareness among designers restricts design freedom, compounded by the absence of explicit regulations and standard design guidelines for privacy protection both a globally and regionally. The study concludes by offering suggestions for potential mitigations to these challenges and discussing various interventions for all key stakeholders involved in privacy protection design (cf. Section §6.4).

Finally, drawing on insights from our prior studies, our fourth study obtained design insights into bystanders' privacy concerns and protection strategies. Drawing

on these insights, we co-designed and evaluated the practicality and feasibility of a mobile app as an auxiliary tool for privacy protection among domestic workers in Jordanian smart homes. This study unfolded in two phases: the first entailed co-designing and developing the mobile app with key stakeholders through a focus group study, and the second involved evaluating the app via semi-structured interviews. Some of the findings from both phases resonated with our previous observations on limited awareness of smart devices and privacy, and asymmetric power dynamics. The results of the study's first phase present design insights on bystander privacy and discuss how the prototype app can support protection. The results of the study's second phase indicate positive perceptions of the app, highlighting its potential to support privacy protection by enhancing communication between households and workers, educating stakeholders, empowering workers, and mitigating power dynamics. However, the findings also bring to light barriers to app adoption, including households restricting workers' access to the internet and smartphones, along with various challenges. The study concludes by suggesting recommendations for interventions to enhance privacy protection. (cf. Sections §7.3, and §7.4.2).

In the subsequent sections, we discuss the primary findings, considerations, concerns, and proposed interventions for privacy protection of domestic workers as a bystander user group in Jordanian smart homes.

## 8.2 Bystanders' Privacy with Smart Homes in Jordan

Our results in Chapter 4, 5, 6 underscore the oversight of the Jordanian context in privacy research, especially regarding smart home bystanders, and show that domestic workers (bystanders[1]) face potential privacy breaches and exploitative practices due to the increasing use of smart devices [10] in Jordanian smart homes. The concerns about bystanders' privacy are influenced by awareness levels and contextual factors, including social norms, customs, religious beliefs, and the prevailing socio-economic power dynamics among users, all within the background of vague data protection regulations for smart home users. Furthermore, domestic workers play

dual roles as both employees and residents in smart homes. This duality adds complexity to the smart home environment, serving as both a private space for households and a workplace for domestic workers.

Drawing from previous research [2, 144, 178, 184, 187, 192, 455], this thesis aligns with established outcomes regarding privacy concerns, power dynamics, and the impact of data protection regulations. Building upon these insights, in the subsequent sections, we discuss identified findings, and offer recommendations aimed at supporting privacy protection for domestic workers within Jordanian smart homes.

### 8.2.1 Overlooked Jordanian Context

Our literature review in Chapter 2 highlights a predominant focus on privacy research in Western contexts (Europe and North America), with limited attention given to MAME contexts, including Jordan. Jordan, situated in the Middle East, is a southwest Asian Arab country with a predominantly Muslim population deeply rooted in Middle Eastern customs, social norms, and a moderate Islamic background [8]. The power dynamics within Jordanian homes (cf. Sections §5.4.1.1.1) reveal a patriarchal hierarchy, where the family head holds the highest power while domestic workers occupy the lowest. Despite progress in empowering women in Jordan, some may still experience marginalization and social stigma for deviating from expected behavior [39, 41]. These challenges are compounded by socio-economic backgrounds and cultural norms. In Jordan, the increasing adoption of smart technologies [10] raises concerns regarding household and domestic workers' (bystanders) privacy. Foreign domestic workers, primarily women from Far East and African countries, encounter challenges such as limited agency and rights, restrictions on movement without employer consent [51, 52], and limited access to smart devices, the internet, and smartphones.

In addition to the above, it's crucial to consider the unique aspects of the Jordanian cultural context, as discussed in Section §2.1, which distinguish it from Western contexts. These unique contextual factors significantly shape the findings of this research, especially those related to the privacy concerns of female

domestic workers, offering valuable insights into privacy perceptions and practices differences between Western and non-Western contexts. Understanding these differences enriches our comprehension of privacy dynamics and informs more contextually relevant design strategies for smart devices in Jordan and similar regions (consistent with contextual integrity theory [63]) . Some findings in this research resonate across different studies [76, 190–193], with new insights specific to the Jordanian context rooted in religious, cultural, and social norms, such as sensitivity surrounding audio-visual data collection concerning females, households' autocratic practices, limited agency of domestic workers, and imbalanced power dynamics within Jordanian smart homes.

Moreover, in Chapters 2, 6, we found that designers and companies primarily focus on Western contexts, overlooking the Jordanian context. This, combined with various business barriers and challenges in the Jordanian and MAME region, such as limited market size, smart device penetration rates[7], lack of local manufacturers, high localization costs, and regulatory limitations, contributes to this oversight. Prior studies [519, 520] have emphasized the impact of unknown and hard-to-manage factors on design processes, including designers' contextual values, norms, and concerns. Findings (cf. Section §6.5.4.2) underscore the significance of addressing contextual privacy concerns (e.g., social, religious, cultural) in smart device design to avoid potential privacy and security implications such as design flaws, inability to recognize bystanders, and concerns about privacy policies and consent. We discuss considering the Jordanian context in the following two sections.

#### 8.2.1.1 Designers and Policymakers to Consider the Jordanian Context

We emphasize the need for designers to take into account Jordanian smart home contextual influences and asymmetrical power dynamics. This consideration is essential to minimize or balance the impact on users with limited agency and leverage privacy-supportive contextual influences in the design of smart devices. Findings underscore the challenge posed by the lack of manufacturers in Jordan and the broader MAME region, hindering the development of contextually suitable devices

for the Jordanian context. Aligning with McGregor et al.'s recommendations [523], we argue for adopting organizational strategies to address specific contexts like Jordan. Notably, we found that staff influence on design processes remains limited within large companies in comparison to Small and Medium Enterprises (SMEs) [526]. Nevertheless, we argue that the growing smart home device markets in Jordan and the MAME region[117] present an opportunity for manufacturers and designers to consider these contexts. This, we believe, can lead to the production of devices that align seamlessly with local contexts. Additionally, we recommend the recruitment and training of skilled designers from local contexts, such as Jordan, to effectively address contextual concerns throughout the design processes. We believe enhancing designers' awareness of contextual concerns is essential for companies to meet the expectations of domestic workers while empowering them.

Furthermore, we argue for the proactive engagement of designers in developing and documenting new design guidelines specifically tailored to privacy considerations in Jordan and the MAME region. This active involvement aligns with the principles of Privacy by Design (PbD) [471] as we discuss later in Section §8.2.5.3, ensuring that privacy protection strategies cater to the diverse needs of different contexts. It is crucial for both local and international policymakers to focus on integrating contextual concerns, especially the inter-playing power dynamics, into the design of smart devices for specific contexts. This includes considerations for privacy checks and obtaining type approval certification before allowing devices into local markets. Our recommendation emphasizes the importance of international manufacturers collaborating closely with local policymakers to establish design guidelines that align with the expectations and needs of users in Jordanian context. This collaboration should explicitly address the requirements of vulnerable user groups, promoting a balance between business interests, user expectations, and contextual privacy needs.

#### 8.2.1.2 Localization to Cover Jordanian Contextual Concerns

In Chapter 6, we highlight the crucial role of smart device localization, noting that current practices often overlook contextual sensitivities, including social, religious,

and cultural aspects. These practices primarily focus on language translation, regional settings, avoidance of offensive content, and consideration of local geopolitical sensitivities. However, they often lack a comprehensive approach to *Inclusivity*[109], *Accessibility*[110], *Non-Offensiveness*[111], *Ethics*[112], and *Relevance*[113] design principles. Our observations indicate that localization efforts are mainly driven by business considerations, such as associated costs, and companies base investment decisions on feasibility. To address the challenges associated with localization, we recommend the implementation of 'Universal Design Settings [491]'—a system that automatically adapts to users' contexts, such as their location, ensuring a more inclusive and relevant user experience.

We argue for regulations mandating the localization of smart home devices to address contextual privacy concerns in Jordan and other regions before their entry into local markets. This localization process requires a deep understanding of contextual concerns and user needs to effectively address them. Furthermore, we argue for companies to establish a compelling business case to justify investments in localizing their products, emphasizing that privacy is a collective responsibility shared among all stakeholders involved.

### 8.2.2 Awareness is Cornerstone for Privacy Protection

In Chapters 4, 5, 6, we underscore a limited awareness regarding smart technologies and privacy concerns among various stakeholders, including households, domestic workers, regulators, and designers. This limited awareness poses challenges to informed decision-making about privacy breaches and practices, and straining relationships between users (households and workers). This strain leads to an erosion of trust between workers and households, fostering feelings of disrespect among workers and diminishing their agency. Our investigation reveals a divergence in household practices, while some inform their workers about existing smart devices, others choose not to disclose this information. Additionally, many workers lack the knowledge to identify smart devices and understand their functions, leaving them vulnerable to data-collection activities, whether intentional or incidental. This

research also highlights the lack of active support from domestic worker recruitment agencies, regulatory bodies, and societal entities in informing, empowering, and protecting this vulnerable user group, leaving workers exposed to various privacy threats. More importantly, findings in line with previous research [188, 189, 492–494] underscore the significant impact of limited awareness on both design freedom for privacy protection and the ability to formulate effective protection regulations.

In Section §6.4.2.2.4, findings highlight that limited awareness among stakeholders, especially smart device designers, restricts design freedom, impedes privacy protection design capabilities, and influences design outcomes. Our third study (cf. Chapter 6), uncovered that designers and companies are skewed toward cultures and norms they are familiar with. For the value of personal data, we found that data is described as the *'new currency'* in the information economy [496, 497], and while users express a willingness to understand how companies utilize and monetize their collected data, findings indicate that users lack knowledge about whether and how companies monetize their data, and reveal that users have no clear understanding of the adopted monetization models. The concept of personal data as the "new oil" of the internet has been emphasized by various scholars, highlighting its immense value and importance in today's digital landscape [202, 371, 372]. Companies like Facebook and Google have built their business models around collecting and analyzing user data, contributing to the growth of personal data markets such as PFP (Paying For Privacy) and PDE (Personal Data Economy)[373]. These markets offer compensation to users for their data usage and are often seen as compliant with data protection laws like the GDPR. However, discussions around data property rights and the challenges of quantifying the monetary value of personal data remain prominent, with concerns about privacy commodification, regulatory limitations, and potential impacts on innovation and societal welfare[75, 377–383]. These complexities highlight the ongoing need for robust regulatory frameworks, ethical considerations, and research efforts to navigate the evolving landscape of personal data management and privacy. Furthermore, we found that companies are not making efforts to educate their designers and business

leaders about contextual concerns and considerations of users from diverse contexts and cultures. They also lack transparency in informing users about their data monetization strategies and fail to take serious actions to consider other contexts, such as Jordan, in their design processes.

#### 8.2.2.1 Educate Stakeholders

Taken together, our studies emphasize prior research [178, 224, 229, 230] suggestions, and argue that it is important for all stakeholders to be particularly aware of bystanders' privacy concerns with smart home devices and how their privacy is impacted by smart device design, regulation, and usage patterns in Jordan (cf. Sections §4.4.2, §5.5.2, §6.5.2.1, and §7.5.1.3). To improve awareness among all stakeholders, we suggest that stakeholders and social organizations collaborate to facilitate a public-private partnership to run public awareness campaigns. This can be achieved through educational material in schools and universities, as well as targeted messages in the media (TVs, newspapers, and social media). Moreover, we discuss that users have a responsibility to educate themselves about smart technologies and privacy implications, in addition to providing feedback and reporting privacy breaches to manufacturers and government entities (i.e., regulators). Companies are urged to educate their designers and business leaders, transparently inform users about their data collection and monetization models, and regulators should educate policymakers to facilitate the formulation of effective regulations and to incorporate public awareness into their regulatory strategies.

#### 8.2.2.2 Role of Domestic Workers' Recruitment Agencies

Findings in Chapter 4, 5 highlight the influential role recruitment agencies (recruiters) play in shaping relationships between workers and employing households, especially during the employment process and contract signing. Importantly, we found that agencies do not make efforts to inform workers about smart technologies and associated privacy threats or facilitate discussions between workers and households regarding privacy preferences with smart home devices. Furthermore, they do not make efforts to enable workers to provide consent to smart devices

use, and they do not intervene to foster a healthy relationship between the two parties, leaving workers vulnerable to exploitative uses of smart technologies and the existing imbalanced socio-economic power dynamics that favor households in the Jordanian context.

We believe that recruitment agencies can play a crucial role in supporting domestic workers' privacy in Jordanian smart homes. Therefore, we suggest that these agencies educate new domestic workers about smart devices, the potential privacy threats they entail, and the recommended privacy protection practices they should adopt. Additionally, agencies should facilitate and moderate transparent discussions on privacy concerns between recruiting families and workers. Finally, we argue for utilizing the proposed app as a tool for education, communication, and reporting violations, as detailed in Section §8.2.6. We emphasize that the role of recruitment agencies in supporting domestic workers' privacy is not specific to the Jordanian context, and we believe it has a significant impact on a global scale.

### 8.2.3 Power Dynamics and Contextual Influences

In line with insights from prior research [7, 91, 120, 210, 225, 228, 291, 292, 295, 296, 299], our second study delves into the prevailing power dynamics within Jordanian smart homes involving domestic workers and households (cf. Chapter 5). We examine how smart home devices influence, shape, and reinforce these power dynamics in the Jordanian context. Our examination aligns with the findings of Bernd et al.[7] study in Western contexts, showcasing the impact of these dynamics on privacy considerations, operational norms, and the cultivation of interpersonal attributes like trust, respect, and comfort within the household-worker relationship in Jordan. We highlight that Jordanian households adopt autocratic practices, which restrict workers' agency and limit their freedom. Unsurprisingly, we found that these dynamics lead workers to compromise their privacy rights in exchange for received benefits (e.g., job, salary, shelter) and defer to households' decisions regarding devices to avoid potential conflicts and consequences, which is consistent with findings from prior research[134–136]. Furthermore, findings reveal that foreign

domestic workers, especially female workers, suffer marginalization and contract slavery in the Jordanian context. For instance, they cannot quit the work as they have to pay back recruitment cost, which is beyond their financial capabilities, leaving them captive to contract terms and enforced to continue the full work contract period before they can leave back to their home countries. Moreover, many families do not inform workers about existing smart devices, restrict access to these devices, restrict movement outside the home, and even limit workers' access to the internet and smartphones.

#### 8.2.3.1 Balance Power Dynamics and Leverage Contextual Influences

To address these imbalanced power dynamics, we argue that collaboration among governments, social organizations, recruitment agencies, and companies is essential to empower domestic workers. We recommend prioritizing awareness about smart technologies and associated privacy risks. Complementing the proposed interventions in Section §8.2.2, we suggest providing information about smart devices in workers' native languages, incorporating it into work contracts, and facilitating informed consent. Another key aspect is developing good practices for households to respect workers' privacy in smart homes. Targeted awareness campaigns should be conducted to promote privacy-respecting practices. It is essential to consider foreign workers' cultural and religious beliefs, informing employing families about their specific needs before hiring them. Clear communication channels with workers should be established, utilizing the proposed app as one possible channel. Families should also be encouraged to consider the ethical implications of undermining workers' rights, and legal protections and support networks for workers are recommended.

In Sections §4.3.3.5, §4.3.4, and §5.4.1.3.3, we highlight positive and negative impacts of contextual influences (i.e., social norms, customs, and religious background) on privacy concerns, practices, and expectations in the Jordanian context (consistent with contextual integrity theory [63]). Positive impacts include households respecting workers privacy rights, and treating workers in good manner. In turn, workers respect household rights and make efforts to create a comfortable

environment. However, negative impacts include households adopting autocratic and patriarchal practices toward their workers and allowing them limited privacy, particularly in private locations such as bedrooms and toilets. This thesis identifies Islam as a supportive foundation for addressing privacy needs, suggesting it as a basis for constructing a comprehensive framework for privacy protection in the Jordanian context. Participants in this research expressed the belief that Islamic principles can influence social norms, legal considerations, and technical practices related to privacy. Furthermore, drawing on previous studies [210, 211], we argue for interventions that leverage the positive aspects of Jordanian social norms and religious backgrounds to promote a fair and respectful treatment of domestic workers. Leveraging Jordan's distinctive social and religious norms, such as values associated with hospitality and Islamic moral principles like kindness and honesty, should inform proactive discussions on privacy between households and workers. Through awareness and educational initiatives, we aim to cultivate an environment of mutual respect and trust, fostering healthier and more equitable relationships within smart homes.

Finally, designers are encouraged to leverage innovative technologies to incorporate privacy protection features into smart device designs, as detailed in Section §8.2.5. These initiatives collectively empower domestic workers, facilitating informed decision-making and protecting privacy rights within the smart home context. Ultimately, these efforts aim to address and balance the existing asymmetric power dynamics in Jordanian smart homes.

### 8.2.4 Vague Data Protection Regulation

At the time of conducting this multi-studies research, the new data protection law[55] in Jordan had not been officially announced. However, findings in Chapters 2, 5, and our review of the regulatory landscape in Jordan (cf. Section §2.2.5.1) uncover that the newly announced data protection law in Jordan lacks explicit privacy regulations for smart home users. Moreover, the legal landscape in Jordan, including the Telecommunications Law No. 13/1995: Article 56[56], Cyber-Crime Law[57], Penal Code-Article 348[58], Anti-Terrorism Law No.55/ 2006-Article 4[59],

The Labour Law[60], Credit Information Law No.15/2010-Article 8[61], and Access to Information Law-Article 13[62] lack explicit privacy regulations for smart home users.

This vague regulation, compounded with the lack of clarity around what is deemed acceptable, leaves workers exposed to privacy threats, and asymmetric power dynamics with households in smart homes. Moreover, findings highlight the limited coverage of existing global data protection regulations for smart home users (e.g., European GDPR[29], USA data protection laws –CCPA[43], CPRA[44], Brazil-LGPD[39], India[49], Turkey[38], Malaysia[50]), which primarily regulate users' data protection with service providers (e.g., Amazon, Google). These regulations focus on users' data protection with service providers, overlooking the specific privacy concerns of smart home users. The findings identify several challenges associated with this vague regulatory context. These challenges include diverse concerns and expectations among users regarding their privacy rights. The dependency on standard privacy protection regulations to inform design guidelines results in the absence of the latter. The inconsistency of data protection regulations across countries makes it difficult for companies to predict the consequences of non-compliance, emphasizing the need for globally standardized privacy protection regulations. Additionally, non-compliance fines disproportionately impact SMEs more than large organizations, hindering their ability to expand their design experience and address overlooked contexts, such as Jordan. Building upon the insights from previous studies [314–317], our research highlights the significant impact of recent global data protection laws on business data management practices, especially for multinational companies. These companies, operating on a global scale, are under pressure to align their policies with regulations like the GDPR, which is considered the "Golden Standard" in Data Protection Law worldwide [327]. This situation raises critical questions about how laws can address interpersonal data practices within smart homes both in Jordan and globally, how regulatory enforcement can be ensured regarding personal practices, how regulators can adapt laws to specific contexts, and the effectiveness of such laws. These questions necessitate further studies to explore and provide suggestions for improvement and enhancement in data protection practices.

#### 8.2.4.1 Legal Protection for Privacy in Smart Homes

This thesis uncovers that Jordan's new data protection law[55] lacks explicit provisions to address user data protection and privacy conflicts among smart home users [366] (cf. Section §2.2.5.2, and §5.5.2.1.1). To address this, in addition to raising awareness among policymakers (cf. Section §8.2.2.1), we suggest that regulators (labour and data) collaborate with all stakeholders to develop standardized global privacy protection regulations. This collaborative effort should involve governments, international, and regional entities such as ITU[82], GSMA[8], TMForum[83], Accessnow[84], and AADR[85]. Furthermore, we recommend the implementation of privacy certificates for smart devices entering local markets. Additionally, we argue for Jordanian regulators and policymakers to address the specific needs of marginalized user groups, with a particular focus on domestic workers, especially females. While this complex challenge requires actions from various entities and stakeholders, we propose a suggestion to empower this vulnerable user group through the establishment of a dedicated *"privacy advice channel"* (cf. Section §7.5.2.4) through relevant authorities and societal entities in Jordan. This channel would serve as a platform for workers and household members to seek guidance on privacy matters, propose good practices, and report autocratic practices and privacy violations. The proposed app could be utilized to provide users access to such channels. Moreover, we argue for future updates of the new law in Jordan to leverage social norms and religious backgrounds within Jordanian society. This involves explicitly addressing the privacy concerns of smart home users, defining data ownership, specifying collection and processing mechanisms, establishing consent-taking procedures, and granting users the right to be aware of the collected personal data.

We argue that the effectiveness of new data protection (DP) laws in addressing privacy challenges remains uncertain, especially when considering the dynamics observed in both Western and non-Western contexts. Experiences from both contexts [313–318, 321–324] highlight various barriers that may hinder the successful implementation of DP laws, such as challenges in enforcement, evolving technology landscapes, and differing cultural attitudes towards privacy and data protection.

Additionally, the success of interventions and design recommendations may vary based on the nature of relationships between stakeholders. Cooperative relationships, characterized by trust and respect, may foster better adoption of privacy-supportive measures, whereas adversarial relationships, marked by distrust and excessive monitoring, could pose significant barriers to implementing privacy preferences and needs discussions. We emphasize that it's essential to explore these dynamics further and consider tailored strategies that address specific barriers within Jordanian societal contexts, leveraging social norms and religious backgrounds to promote effective privacy protection measures.

### 8.2.5 Technical and Business Support for Privacy Protection

In this section, we discuss and present some recommendations for technical and business interventions to support bystanders' privacy protection in Jordanian smart homes.

#### 8.2.5.1 Utilize Innovative Technologies and Multi-User Consent

We argue for leveraging the potential of innovative technologies like Artificial Intelligence (AI) and Machine Learning (ML) to develop algorithms and statistical models (cf. Section §6.5.3.1). These technologies can enable smart devices to learn from data collected in specific applications, improving privacy protection and enhancing user agency in different contexts. AI-enabled devices can adapt over time, understanding contextual power dynamics, usage patterns, and integrating data protection with user recognition technologies. This includes user identification, profiling, and the ability to hide or delete bystanders' data. Empowering workers with control over collected data is crucial, requiring either family consent or the implementation of new regulations in Jordan. Our findings underscore concerns about single-user consent impacting passive users, emphasizing the need for research on multi-user consent mechanisms tailored to Jordanian expectations and values. Devices should be designed to prioritize data management across privacy settings, addressing challenges outlined in previous studies [476, 477], such as granularity,

complexity, user awareness, interoperability, managing changes in privacy settings, and transparency.

#### 8.2.5.2 Semiotics For Smart Devices

We propose that designers should engage more deeply into semiotics[32] (cf. Section §6.5.3.2), the study of signs and symbols, to create culturally sensitive signals for smart devices. Given the diverse range of users interacting with these devices, including children, adults, elderly, disabled users, and bystanders such as neighbors or domestic workers, semiotics can help design appropriate and effective communication methods. Smart devices introduce more sophisticated interaction methods, requiring consistent signs, symbols, and a privacy language that resonates with the target audience. Considering the complexities of different languages, educational levels, and cultural norms, semiotics can play a crucial role. We argue that the proposed app in our fourth study can serve as a semiotic tool, aiding in the creation of a language to facilitate privacy discussions between domestic workers and households. We emphasize the findings of prior studies [97, 98] that indicate semiotic design features strongly influence user expectations in different contexts. These features contribute to the shared language between users and smart devices, leading to improved privacy protection practices and decisions.

#### 8.2.5.3 Adopt Privacy by Design (PbD)

This thesis emphasizes the crucial need for companies and designers to embrace the principles and practices of Privacy by Design (PbD) [498, 506, 507] (cf. Section §6.5.3.3). This approach should serve as a continuous process of learning and improvement, incorporating user feedback and reported incidents specific to the Jordanian context. To facilitate this, regulators should collaborate with the private sector to offer clear guidance on design principles, providing instructions on balancing users' privacy needs and business interests, coupled with robust oversight mechanisms. A globally applicable set of Privacy by Design principles and practices must be developed, taking into account essential contextual considerations for Jordan and the MAME region. We argue that Privacy by Design (PbD) ensures

compliance with privacy best practices in design and adherence to local regulations that fit different contexts. These should be developed alongside standard global data protection regulations and design guidelines.

#### 8.2.5.4 Address Cost Challenges in Privacy Protection Design

Our research indicates that cost poses a significant challenge for considering non-Western contextual privacy concerns (MAME) in the design of smart home devices, particularly for SMEs (cf. Section §6.5.4.1). Previous studies have explored how financial strength enables better consideration of data protection [513, 514]. To overcome these financial challenges, informed by outcomes from prior studies and the discount usability engineering movement [144, 515–517], we argue that both researchers and businesses need to collaborate in developing, improving, and applying cost-effective design practices (e.g., heuristics such as generalizations [518], workarounds, common sense, and shortcuts) to mitigate privacy protection design challenges. Our contention is that these proposed business interventions can effectively address the MAME context of Jordan, as well as other overlooked contexts regionally and globally.

#### 8.2.5.5 Adopt Ethical Design and Business Practices

This thesis highlighted a lack of trust among Jordanian users towards companies employing deceptive data collection practices (cf. Section §6.5.4.3). We argue that building trust necessitates companies incorporating data protection into corporate strategies, adopting ethical and transparent practices, and providing tools for workers to protect their data. To foster a sustainable and healthy smart device market, companies must explore ethical business models that respect user data. Understanding and leveraging contextual values, including social, religious, and geopolitical factors, can inform business practices that better align with user preferences. Investigating the influence of business values and practices on privacy protection is crucial, and we propose the development and 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.

### 8.2.6 Design Insights for Privacy Mobile App

Our fourth study focused on obtaining design insights to collaboratively design, develop, evaluate, and assess the potential of employing an app ( a technology probe) as an adjunct tool to enhance the privacy protection of domestic workers in Jordanian smart homes. As discussed in Chapter 7, our findings show how an app can help to educate users, facilitate communication between workers and households, alleviate power dynamics, empower workers, scan for nearby devices and provide notifications, and provide channels for reporting privacy violations and autocratic practices. Several challenges were identified with the app, including adoption barriers, lack of standardized privacy protection design, workers' limited tech literacy, and a vague regulatory landscape. In addition to raising awareness among users and arguing for standard regulations and design guidelines, the study emphasizes utilizing persuasive measures to promote app adoption, rather than adopting coercive measures (regulations and work contracts). In line with prior studies, we emphasize the significance of employing privacy-supporting tools that contextualize privacy preferences within users' daily lives. This approach considers social dynamics, privacy notifications, and the utility of privacy labels. Our focus is on accountability measures and tools for informed decision-making rather than direct control mechanisms [83, 84, 125, 127–129].

Among the suggested features for the app (the probe), we believe that four features would gain mainstream adoption: the feature to facilitate privacy discussions between households and workers, scanning and notifying nearby users about existing devices and data collection activities, educating users about smart devices and data protection laws, and providing a platform to inquire about privacy concerns and report privacy violation incidents. These features may find more relevance in certain contexts compared to others, both in Western and non-Western settings. Determining which context will adopt and best utilize these features will depend on

practical application and testing in real-world situations, incorporating user feedback for ongoing improvement and enhancement. However, we firmly believe that these features will contribute significantly to privacy protection in various contexts, fostering better communication, awareness, and adoption of privacy practices.

### 8.2.7 Responsible Innovation

We emphasize that the overarching recommendation remains that the design of innovative smart technologies should adhere to established principles of responsible innovation (RI)[92, 93] (cf. Section §6.5.3.4). Specifically, this emphasizes the importance of considering security and privacy when designing new technologies. An example of this approach is the AREA framework[509], 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. Additionally, we argue for the implementation of a certification system that spotlights those employing ethical and responsible practices in data protection, incorporating data protection within their design processes. We believe such a certification system will support global efforts for more ethical design [510–512].

## 8.3 Moral Obligations and Ethical Responsibility

To address the question of whether technologists have an ethical responsibility to design technology that either integrates into and potentially reinforces existing social and cultural issues or strives to mitigate these problems. In this thesis, we touched upon various social concerns such as wage slavery, gender power imbalances, and the dehumanization of domestic workers. We argue that technologists should design solutions in a way that actively works to mitigate or alleviate these challenges. This approach would involve creating tools and systems that empower workers, promote fair wages and working conditions, and challenge discriminatory practices. On the other hand, some might argue that technology should align with existing social norms to avoid disrupting societal structures. This viewpoint acknowledges

the complexity of societal dynamics and suggests that technological interventions should not aim to radically change social norms but rather complement and enhance existing practices while ensuring ethical considerations are upheld.

A solution-oriented approach could involve technologists collaborating with social scientists, ethicists, policymakers, and affected communities to develop inclusive and responsible technological solutions. For instance, in the case of wage slavery, technology could be used to create transparent payment systems, provide workers with tools to negotiate fair wages, and monitor labor practices for compliance with ethical standards. Regarding gender power imbalances, technology could support initiatives that promote gender equality, such as AI tools for detecting and addressing workplace discrimination or platforms for promoting diverse representation and inclusivity. When addressing the dehumanization of domestic workers, technologists could develop technologies that prioritize privacy, dignity, and autonomy for workers, such as secure communication platforms, tools for reporting abuse or harassment, and educational resources on labor rights. Importantly, these solutions should be co-created with input from impacted communities and designed with a deep understanding of the cultural, social, and economic contexts in which they will be deployed.

Overall, the thesis could argue for a nuanced approach that recognizes the potential of technology to both reinforce and challenge societal issues, emphasizing the importance of ethical considerations, inclusivity, and collaboration in technological design and implementation.

## 8.4 Conclusion

This research aims to tackle the gap of privacy research in the MAME region by focusing on the privacy concerns of domestic workers in Jordanian smart homes. In better understanding the problem domain, our research has uncovered core themes related to individuals' privacy concerns, regulatory considerations and power dynamics, and smart device design challenges. In exploring how to intervene in

this space, we have uncovered several challenges focusing on the design, adoption, and regulatory aspects of auxiliary privacy tools.

In our discussion of the wider implications of our research, we make a number of recommendations for future interventions across social, technical, business, and legal domains to enhance privacy protection. These interventions include educating stakeholders, leveraging innovative technologies, adopting Privacy by Design principles, and collaborating on global privacy protection regulations. Ultimately, the aim is to empower domestic workers and foster a culture of privacy awareness and respect in Jordanian smart homes.

# 9
# CONCLUSION

As the prevalence of smart devices continues to rise, so do privacy concerns [554], this dissertation explores the impact of smart devices on the privacy of smart home bystanders[1], particularly domestic workers, in the non-Western context of Jordan. Smart home bystanders may unknowingly undergo data collection without awareness of the installed devices or their functions. Another challenge in addressing privacy concerns of smart home bystanders in Jordan is that existing research are predominantly from a Western perspective, overlooking non-Western contexts such as Jordan. Our goal was to identify potential enhancements for the privacy of this vulnerable user group.

This dissertation is motivated by the overarching research question: RQ: *To what extent can we understand and support the privacy needs and protection means of bystanders in the smart home in Jordan?* To better address this research question, we broke it down into three main sub-questions:

- RQ 1. What are the privacy concerns of the households and their domestic workers (i.e., the bystanders) in the smart home in Jordan?
- RQ.2 How do smart home socio-economic power dynamics affect the privacy of households and domestic workers (i.e., bystanders) in the smart home in Jordan?

- RQ.3 How can we support privacy protection for domestic workers (i.e., bystanders) in the smart home in Jordan?

The dissertation addresses these questions through an exploration of privacy concerns and practices among households and domestic workers (bystanders) in smart homes in Jordan (cf. Chapter 4). It delves into the power dynamics within smart homes and the status of data protection regulations (cf. Chapter 5), seeking insights from smart device designers regarding privacy protection through smart device design (cf. Chapter 6). Additionally, we gain design insights and evaluate the feasibility of a co-designed technology probe prototype (mobile application) as an auxiliary tool supporting privacy protection for smart home bystanders in Jordan (cf. Chapter 7). Utilizing Grounded Theory and Thematic Analysis, four qualitative studies were conducted, employing semi-structured interviews and focus groups with participants such as smart device designers, business leaders, recruiters, regulators, app developers, households, and domestic workers. This dissertation concludes with recommendations for interventions aimed at enhancing privacy protection for smart home domestic workers (bystanders) in Jordan.

## 9.1 Key Findings

This research aimed to investigate the impact of smart devices on the privacy of bystanders in smart homes, particularly domestic workers, within the non-Western context of Jordan. The aim was to identify potential privacy improvements for this user group. Our identified research questions guided the exploration, leading to the following key findings:

### 9.1.1 Jordanian Context Oversight

In this study, we highlight a gap in privacy research, particularly in MAME[14] contexts like Jordan. Jordan, deeply rooted in Middle Eastern customs, is a patriarchal society with a power hierarchy favoring men. The power map in Jordanian homes reflects this hierarchy, with family heads holding the highest power

and domestic workers the lowest. The widespread adoption of smart technologies [10] in Jordan raises privacy concerns, especially for foreign domestic workers who face challenges such as limited agency, restricted movement, and limited access to smart devices.

### 9.1.2 Limited Awareness of Smart Technologies and Privacy

Our research highlights the limited awareness about smart technologies and privacy concerns among key stakeholders, including households, domestic workers, regulators, and designers. This weak awareness poses significant challenges, impeding informed decision-making on privacy breaches and practices, straining relationships between users (workers and households), and eroding trust and agency for workers. Notably, disparities in household practices emerge, with some disclosing smart device information to workers while others do not. Furthermore, while users are primarily concerned about audiovisual devices, many workers lack the knowledge to identify smart devices and understand their functions, making them susceptible to data-collection activities. This research underscores the absence of active support from recruitment agencies, regulatory bodies, and societal entities in informing, empowering, and protecting this vulnerable user group, exposing workers to various privacy threats. Additionally, it highlights the impact of limited awareness on design freedom for privacy protection and the formulation of effective protection regulations.

To raise awareness among stakeholders, we emphasize collaborative efforts and argue for a public-private partnership. We recommend conducting awareness campaigns through educational channels in schools, universities, and targeted media platforms. This research underscores user responsibility, emphasizing the importance of self-education on smart technologies and encouraging feedback and reporting of privacy breaches to manufacturers and regulators. We argue for transparent practices within companies, urging the sharing of information with users about data collection and monetization models. We call for companies to educate designers and business leaders about privacy concerns and contextual needs. Simultaneously, this research emphasizes the importance of regulators incorporating public awareness into

their regulatory strategies. Moreover, it underscores the significance of domestic worker recruitment agencies in educating workers about smart devices, privacy threats, and best practices. Additionally, it argues for promoting and facilitating open discussions between households and workers regarding privacy concerns.

### 9.1.3 Asymmetric Power Dynamics and Contextual Influences

Our research highlights how smart home devices affect and reinforce power dynamics between Jordanian households and their domestic workers, impacting privacy concerns and relationship dynamics. Jordanian households often adopt autocratic practices, limiting workers' agency and privacy rights, while workers compromise privacy rights for received benefits. Additionally, foreign domestic workers face marginalization and restricted freedoms. Contextual influences, such as social norms and religious backgrounds, play a significant role in shaping privacy practices. Positive influences lead to respectful treatment, while negative impacts result in autocratic practices. To address these imbalances, collaboration among various stakeholders is recommended, emphasizing awareness, cultural sensitivity, and privacy protection measures. Moreover, the proposal includes leveraging Jordan's unique norms through awareness campaigns, incorporating them into the design process, and forming regulations to foster equitable relationships within smart homes.

### 9.1.4 Lack of Explicit Privacy Regulation

This research highlights a vague regulatory landscape and a lack of explicit regulations for smart home users in Jordan's recently announced data protection law[55], leaving workers vulnerable to privacy threats and power imbalances with households. Furthermore, it reveals that the current legal framework in Jordan lacks these regulations, emphasizing the need for specific privacy guidelines tailored to smart home users. It also notes that global data protection regulations primarily focus on protecting data with service providers, inadequately addressing the unique privacy concerns of smart home users. Recommendations emphasize collaborative

efforts between regulators and stakeholders to establish standardized global privacy protection regulations, engaging international and regional entities. Proposed measures include implementing privacy certificates for smart devices, addressing the needs of marginalized user groups, and leveraging social norms and religious backgrounds in future updates to Jordan's law to explicitly address smart home users' privacy concerns. The establishment of a *'privacy advice channel'* is suggested for guidance, best practices, and reporting privacy violations, utilizing the proposed app as a platform.

### 9.1.5 Design Challenges for Privacy Protection

We highlight the design challenges related to privacy protection for domestic workers in Jordanian smart homes, providing several recommendations to enhance privacy-focused design. Our research unveils the influence of business strategies, regulations, and contextual factors, such as culture, religion, and norms, on privacy design. It emphasizes the impact of limited awareness among designers and business leaders on design freedom, emphasizing the need to educate concerned stakeholders about smart devices, privacy concerns, contextual influences, and local data protection regulations. This research identifies a bias toward Western cultures and norms in smart device design, exacerbated by a lack of designers in Jordan and the MAME region. Current localization practices often overlook contextual concerns in Jordan, focusing on language translation, regional settings, and avoiding offensive elements. It reveals user challenges with dark patterns in design and tricky privacy policies undermining their agency. Designers underscore the importance of global data protection regulations and design guidelines, whereas Jordan lacks explicit data protection regulations for smart home users, with absence of global standard regulation. Proposed interventions include developing design guidelines, ethical business models aligned with regional values, using semiotics[32] for effective communication about privacy, and expanding smart device localization to address contextual privacy concerns in Jordan. Addressing power dynamics in smart homes requires collaboration among stakeholders, and agile-cost-effective approaches

can help SMEs and companies overcome financial challenges to address various contextual privacy concern in smart device design. This research aligns with the principles of Responsible Innovation, emphasizing the need to anticipate, reflect, engage, and act to minimize negative impacts from smart technology innovations.

### 9.1.6 Auxiliary Tools for Privacy Enhancement

Building on insights from our first, second, and third studies, we gained design insights to co-design, prototype, and examine the potential of a technology probe (the app) as an auxiliary tool to support privacy protection for domestic workers in Jordanian smart homes. This research examines the app's potential to empower workers and enhance their agency (1) by facilitating structured and effective discussions between workers and households; (2) by providing education on smart devices, privacy threats, and relevant data protection regulations in Jordan; and (3) by exploring how this can be done within existing power structures and dynamics in smart homes. The app faces several challenges such as household restrictions on app usage, limiting workers' access to the internet and smartphones, literacy barriers among workers, and some technical challenges.

We provide recommendations to address these challenges and leverage the app's features. We argue for the comprehensive development of all proposed features in the app, with continuous improvements based on user feedback. Additionally, we call upon policymakers, recruitment agencies, and other stakeholders to actively endorse and support the adoption of such apps for enhancing privacy protection. Furthermore, we call upon future research to address privacy enhancement auxiliary tools (such as apps, smart devices, websites, etc.) and assess their potential for privacy protection. While recognizing that the app represents a step in addressing the complex privacy landscape in Jordanian smart homes, it is acknowledged as just one component within a broader ecosystem of strategies that encompass social, technical, legal, and business interventions. Ultimately, the adoption of such apps remains contingent on persuading households to adopt them and allow workers access and use.

## 9.2 Critical Review

We identify and outline areas of weaknesses and limitations (e.g., flaws or shortcomings) within the research presented in this dissertation. We discuss major limitations below:

*Selection of Participants:* In this research, our selection of participants focuses on individuals who have consciously chosen to use and adopt smart home products. However, intentional users of such devices do not fully represent the entire users of smart home devices in Jordan. Non-users and bystanders of smart home products may hold distinct perspectives, experiences, and perceptions regarding their usage. Additionally, individuals with concerns about security and privacy might opt to refrain from using smart home devices. Future research should address the concerns and perspectives of various bystander types (e.g., guests, passersby, other types of domestic workers) within Jordanian smart homes.

*Language:* Participants were provided with the option to carry out interviews in either English or Arabic. The majority of interviews were conducted in English, with the exception of some interviews conducted in Arabic, accommodating participants who preferred their native language. The translations of these interviews into English were carefully executed to preserve the participants' perspectives. While some non-native English speakers encountered challenges in articulating themselves clearly, we are confident that this did not substantially influence our analysis, as we cross-verified the outcomes of all conducted studies.

*Recruitment:* Recruiting participants for this qualitative research proved challenging due to legal and company obligations, as well as the sensitive and confidential nature of the research topic. The sensitivity of privacy, and data protection topics among designers and business leaders, especially those in significant organizations, may have influenced biased responses. To address this, participants were briefed on security and privacy measures, emphasizing data encryption and compliance with the General Data Protection Regulation (GDPR[29]). Additionally, we utilized snowball sampling [443], a method commonly used to engage with hard-to-reach

groups [445, 446]. Further details on addressing these limitations are provided in Sections §4.2.5, §5.3, §6.3, §7.2.5.

*Gender Diversity:* In our fourth study (cf. Chapter 7), we acknowledge the limitation of gender diversity among our participants, as we were only able to recruit male designers, mobile app developers, recruiters, and regulators. While this may have influenced their perspectives, we believe that it did not significantly affect the effectiveness of the study outcomes, as our emphasis was primarily on capturing professional viewpoints rather than personal experiences.

*Topic Sensitivity:* Due to the sensitivity of topics related to security, privacy, and regulations, participants might have offered biased or incomplete responses due to considerations for corporate responsibilities and reputation. To mitigate this potential bias, we provided a comprehensive explanation of our security and privacy measures, highlighting aspects such as data anonymization, encryption, and compliance with the GDPR. Further details on addressing these limitations are provided in Sections §6.3, and §7.2.5.

*Research Quality:* The effectiveness of qualitative research depends on researchers' proficiency and can be susceptible to personal biases. Inexperienced researchers may encounter challenges in conducting interviews effectively and exploring crucial topics, potentially leading to the omission of pertinent data [462, 486]. To address this concern, the primary researcher is trained in how to design and conduct interviews carefully, asking questions in a neutral and open manner to avoid influencing interviewees. Further details on how we addressed this limitation are provided in Sections §6.3, and §7.2.5.

*Bias:* Self-reporting bias, a common challenge in interview studies [463], may lead participants to forget details or respond inaccurately, influenced by their desired perception. Additionally, participants might alter their responses influenced by their understanding of researchers' perspectives, potentially leading to bias [464]. To enhance validity and mitigate bias, our strategies focused on avoiding leading questions and instead relying on open-ended inquiries. By utilizing these methods,

participants were encouraged to freely express themselves, leading to more comprehensive responses and contributing to the overall validity of the studies reported in this thesis. Further elaboration on our approach to addressing these self-reporting bias limitations is provided in Sections §5.3, §6.3, §7.2.5.

*Sample Size:* Our qualitative studies conducted in Chapters 4, 5, 6, 7 face limitations related to the size and diversity of the participant sample. Securing the participation of regulators, designers and business leaders willing to discuss their experiences with security, privacy, and data protection, is challenging due to the sensitive and confidential nature of legal matters. Despite extensive efforts, recruitment of business leaders from large companies for this research proved unsuccessful. Consequently, the qualitative research is constrained by the limited size and diversity of the participant pool. Further details on how these limitations were addressed can be found in Sections §5.3, §6.3, §7.2.5.

*Focus Group Dynamics:* The dynamics within a focus group can create situations where participants feel pressured to conform to the majority's opinions or where one individual dominates the conversation. To address these challenges, the moderator actively guides the discussion, promoting productivity, balancing participation, and ensuring that every participant has the opportunity to voice their viewpoints. Further details on how these limitations were addressed can be found in Section §7.2.5.

*Generalization:* It is important to emphasize that this thesis adopts a qualitative approach, intending not to quantify findings or draw generalized conclusions applicable to a broader population. The insights presented herein are rooted in the perspectives of our participants and should not be considered universally applicable. The primary objective of this qualitative research is to offer an in-depth understanding of the subject matter rather than generating broadly generalizable outcomes. Any hypotheses derived from our findings and grounded-theoretic analysis would necessitate further testing in a confirmatory study to ascertain their broader applicability and generalizability. Further details on how these limitations were addressed can be found in Sections §4.2.5, §5.3, §6.3, §7.2.5.

*Research Validity:* We acknowledge the limitations of Inter-Rater Reliability (IRR) in validating the robustness of our findings. IRR relies on coder agreement, but interpretations can remain subjective, leading to variability even with high agreement levels. High agreement in coding may indicate surface-level consensus but could miss the accuracy and depth of interpretations. Additionally, IRR's focus on coding consistency might overlook broader research validity aspects such as theme relevance or contextual understanding, lacking direct participant input and being influenced by raters' biases. Despite these constraints, IRR is valuable for assessing consistency, aiding in quality control, and enhancing the reliability of findings. To strengthen credibility and robustness, complementing IRR with Peer Debriefing, various triangulation methods (e.g., Methodological, Data, Investigator, Theory), and other validation approaches is essential, especially as interpretations evolve during early-stage themes and theory building. Further details can be found in Section §3.2.4.

## 9.3 Future Research

The key findings of our studies inspire future research areas that are well-suited for further evaluation and investigation. These areas are outlined below:

### 9.3.1 Explore Privacy Concerns in other MAME Contexts

The findings outlined in Chapter 4 reveal the privacy concerns identified for domestic workers acting as bystanders in Jordanian smart homes. While our research focuses on the Jordanian context, it triggers interest in future research for other MAME contexts such as Egypt, Syria, Lebanon, and Gulf States. Subsequent research in these MAME contexts is encouraged to either validate the findings in the Jordanian context or complement them, contributing to a more comprehensive understanding of privacy concerns with smart home devices for bystanders in the broader MAME region.

### 9.3.2 Explore Data Protection Regulation in MAME Region

The insights presented in Chapters 4 and 5 reveal the lack of explicit data protection regulations for smart home users in Jordan. This gap persists even with the introduction of the recently announced data protection law[55] in Jordan, which lacks explicit privacy protection for smart home users. These findings trigger interest for future research to explore how privacy protection can be navigated within the existing legal framework in Jordan. Additionally, it encourage an investigation into regulations in other MAME contexts, aiming to offer valuable insights for future regulatory developments. Policymakers can benefit from understanding the nuances and considerations necessary when formulating new policies and regulations in these contexts.

### 9.3.3 Investigate Other Bystanders

The findings in Chapter 5 identified power dynamics and contextual influences within the Jordanian context, exploring their impact on, reflection of, and influence on privacy concerns of domestic workers in Jordanian smart homes. While we believe these identified findings offer comprehensive insights, they encourage further examination of power dynamics with other types of bystanders, including guests, passersby, and passive family members. The proposed investigation to explore power dynamics with other types of bystanders aims to complement the findings with domestic workers, providing additional insights.

### 9.3.4 Innovation in Smart Device Design

The findings outlined in Chapter 6 explore challenges for privacy protection in smart device design. While this research provides valuable insights, it triggers an interest in studying how specific innovative technologies (e.g., AI, ML) could be utilized to improve privacy protection for bystanders with smart home devices, how businesses can seek to balance users' privacy needs with business interests in innovative ways, and in exploring the feasibility to develop standard global design

guidelines. Additionally, we encourage an investigation into how the localization of smart devices could be improved to incorporate specific contextual privacy needs.

### 9.3.5 Improving Communication Among Different Stakeholders

Our findings and recommendations emphasize the need for collaborative communication among all stakeholders. The need for structured communication and collaboration triggers an interest in further research in this area to explore how different stakeholders can effectively communicate about privacy concerns, the design of privacy protection in smart home devices, how future regulations can address privacy protection of smart home users, and to explore the intricate power dynamics and contextual influences of smart homes.

### 9.3.6 Explore Innovative Ways for Consent Taking

The findings outlined in Chapters 5 and 6 highlight concerns regarding the tricky privacy policies and the dark patterns adopted by manufacturers, in addition to deceptive consent-taking mechanisms. This triggers an interest in further researching how to develop privacy policies, and design consent-taking mechanisms that respect users' privacy rights and convey necessary information transparently to users. While we believe the provided insights are valuable for privacy protection design, we also believe more research is needed to explore the relationship between innovation and privacy, and how to maintain responsible innovation principles while designing smart devices.

### 9.3.7 Explore Privacy-Enhancing Interventions

The findings presented in Chapter 7 offer insights into the feasibility and practicality of using a mobile application as an auxiliary tool to enhance privacy protection for bystanders in Jordanian smart homes. We argue for further research to explore how novel socio-technical designs, features and functionalities can enhance privacy protection for all bystander user groups. Additionally, we call for future research

to investigate different contextualised interventions for privacy enhancement, such as websites, specialized smart devices, and other innovative tools tailored to the needs of different communities worldwide.

# Appendices

# A
# Thesis Definitions

## A.1 Definitions

In this section, we present definitions for key terms and concepts that are the focus of this thesis. We provide a definition for The Smart Device, The Smart Home, The Smart Home Bystanders, The Privacy, The Design Process of Smart Devices, and the Designers.

### A.1.1 The Smart Home Device

It is obvious that the ubiquity of smart home devices and platforms has enabled security applications that adapt to user's preferences and interests. In recent years, we have seen a rapid increase in internet connected smart home devices, inter-operable between different vendors, and controllable via different smartphone operating systems. Smart home devices are either standalone smart devices that connect to the internet through existing Wi-Fi networks, such as: thermostats like Nest, lights like Philips Hue, and motion detectors, or devices that communicate to the internet using a bridge, like Z-Wave[121], and Zigbee[120]. There are two types of smart home platforms: The first type is Hubs, such as: Samsung Smart Things [188], Vera [555], and Wink [556], which are central devices that are designed to be used by other smart devices to communicate with, such as: Z-Wave or Zigbee bridge.

Similar to hubs, are the smart personal assistants, such as Google Home and Amazon Echo/Alexa, that can communicate with other smart devices, allowing users to use users' defined controllers to control their smart home devices. The second type of smart home platforms is the cloud-based devices that could be controlled via the cloud, like IFTTT cloud services (If This Then That) that can connect stand-alone devices together.

We did not find agreement on a definition of smart home device, however, drawing on our understating as discussed above, and integrating the existing definitions of smart home devices in the literature [38, 60], we develop our own definition of smart home devices that states: *"Smart home device is a controllable device that is equipped with an embedded processor, memory, sensors, and a network connection to connect to other devices or to the internet to provide useful services to the users and can store or share data on a local storage-device or over the internet."*

### A.1.2 The Smart Home

The concept of a smart home was first defined[557] in 1992 as *"the integration of different services within a home by using a common communication system that assures an economic, secure, and comfortable operation of the home and includes a high degree of intelligent functionality and flexibility"* . However, this definition did not consider home intelligence. Berlo's definition [558], which came later, adds home intelligence, stating that *"a home or working environment, which includes the technology to allow the devices and systems to be controlled automatically, may be termed a smart home"*. Briere and Hurley [5] defined smart homes as a group of products and skills based on networks in the home, but this definition was considered too broad. In 2003, Intertek's smart home project offered a more detailed interpretation[4], stating that *"A smart home is a dwelling incorporating a communications network that connects key electrical appliances and services and allows them to be remotely controlled, monitored, or accessed"*. Satpathy[559] provided an even more comprehensive definition, stating that a smart home is *"a home which is smart enough to assist the inhabitants to live independently and*

*comfortably with the help of technology is termed as smart home. In a smart home, all the mechanical and digital devices are interconnected to form a network, which can communicate with each other and with the user to create an interactive space".* From his side, Alam's [560] described smart home as *"an application of ubiquitous computing that is able to provide user context-aware automated or assistive services in the form of ambient intelligence, remote home control or home automation"*, and Aldrish [561] explained that smart homes are designed to address households' concerns about safety, privacy, and peace of mind. Another definitions[560, 562] stated that smart homes are known as intelligent house, home automation, and aware house.

There isn't agreement on a definition of what smart home is; however, there is a kind of overlap in describing the smart home, thus, we develop our own definition that states: *"Smart Home is the home that is equipped with smart devices that provide the inhabitants with useful services and benefits. The smart devices in the smart home can connect to other devices and/or to the internet and can be either locally or remotely accessed, controlled and/or monitored, and can collect, store, or share data on local storage device or over the internet."*

### A.1.3 The Smart Home's Bystanders

We will use the definition used by Yao et al.[1]. which states that *"smart home's 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 the Smart Home's Bystanders might be subject to data collection, and they may not be aware of the installed smart devices, or the functions of these devices. Our research focuses on domestic workers as a group representing smart home bystanders. For simplicity, we will define bystanders by *"Users who are subject to others' use of smart devices in the smart home"*.

### A.1.4 Usability

Usability denotes the measure of how easily and efficiently a smart system can be employed by users to accomplish specific objectives in an efficient manner. This encompasses several facets, such as user interface design (UI[106]), accessibility, user experience (UX[100]), and overall user satisfaction. A smart system is deemed highly usable when it proves intuitive, user-friendly, and minimizes the learning curve for users in performing tasks. Essential components of usability include clear navigation, effective feedback, error prevention and recovery, and efficiency in task completion. Usability stands as a paramount consideration in smart systems development, ensuring that users can interact with the system with minimal friction and frustration [563].

### A.1.5 Designers of Smart Device and Design Process

We provide definitions of the smart device designers and design process in Section §6.4.1.1.

# B

# Chapter 4 Supplementary Material

We present in this appendix supplementary material relating to Chapter.4. We provide copies of the first study advertisement poster, screening survey questions, families' interview guideline questions, and workers' interview guideline questions.

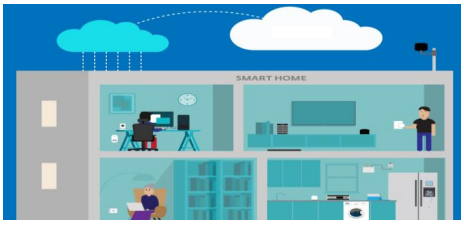
# B.1 First Study - Advertisement Poster

DEPARTMENT OF COMPUTER SCIENCE

## VOLUNTEERS NEEDED FOR INTERVIEWS

CUREC Approval Reference: (CS_C1A_21_001)

**Exploring Bystanders' Privacy Concerns with the Smart Home in Jordan**




**What: -**

- *45-60 minutes* of audio recorded interview.
- Do we use smart devices, or deal with it in the home?
- What are the expectations of the smart device's effects on people's privacy?
- How could we improve the technology to protect users' privacy?

**Who**: *over 18s*, owns a "smart home device", or deal with a smart device.

**Where: Online, or anyplace at the interviewee convenience.**

**When: at a convenient time**

**We appreciate filling this online questionnaire:**
https://oxford.onlinesurveys.ac.uk/demographic-information-for-bystanders-privacy-with-smart-3

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 (wael.albayaydh@cs.ox.ac.uk )

## B.2 First Study - Screening Survey Questions

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-13]

**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-13]
- Few months
- 1 Year

- 2 years

**Involvement with Smart Devices**

8- Describe your level of involvement with smart home devices?
   - User [Jump to Question-10]
   - Working in a home with smart devices [Jump to Question-11]

**Job Type**

9- What is your job type?

**Bystanders**

10- Do you have domestic worker [full time/part time] in your home?
   - Yes
   - No [Jump to Question-13]

**Permission**

11- 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**

12- 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**

13- Thank you for participating in this survey.

# B.3 Families Interview Guideline Questions

**A- Warm Up Questions (5 Min)**

1- How many people live in the house?
2- Do you have a domestic worker?
3- [If yes] How long have you had your domestic worker?
4- What are the pros and cons about hiring a domestic worker?
5- Do you think it is easy to find a good domestic worker in your area?
6- How did you recruit your domestic worker?
7- [In your opinion] How you can build good working relation with your domestic worker?
8- What is your general knowledge of smart devices and smart homes?

**B- Skill Assessment.** We'll ask questions and observe responses to understand 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)**

Here we will collect information about the employers (families) experience and decision-making about smart device(s)

1- Do you use smart devices in your home?
2- What are the smart devices that you use in your home? Why?
1- Do you have specific device(s) to check on domestic worker(s) inside your home?
2- Regarding the functions of [this/these] device(s)?
    - [Do they/Does it] record video/audio?
    - [Is it/are they] only livestreaming device(s)?
    - Is the data sent over the Internet?
    - Do you know where the data is stored?
      [ If stored on the cloud] Do you know what they do with the data?
    - Do you know for how long the data is stored?
    - Do you know who else can [see/hear] the data?
      [ If participant can see/hear the data] How do you use the collected data?
    - Do you keep the device turned on while you are in home?
    - How often do you check the data? Has that changed over time?
3- Who made the decision to get the device(s)?
4- [If the kids are in an age that you may discuss and consult with them] Did you consult with your kids? Did they accept the idea of being unintentionally monitored?

5- Who [is/are] the admin(s) of the smart device(s)?
3- [Is/Are] the device(s) hidden?
4- [Does/Do] the domestic worker(s) know that they are monitored by these devices?
6- Before purchasing the smart device(s), did you think about:
   - How the data will be stored?
   - How the data will be processed?
   - Where the data will be stored?
   - How you will have access and control of your own home data?
   - The laws and privacy rights about monitoring and recording people in your home?
7- [In your opinion] Do [Would] you feel comfortable having smart device in your home? [Why]?
8- Did you hire your domestic worker through an agency?
9- [If yes] Did the agency offer you any information or advice about smart device(s) in homes where domestic workers are working?
10- Do you know whether they offer domestic workers any information or advices with regards to smart devices?
11- Do they get involved or help with negotiations between [employers/families] and domestic workers about smart device(s)?
12- Is there advice or information that you wish they had given your domestic worker, or that you think they should have given [her/him/them] about smart devices? [Like distributing an information sheet]

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

1- Can you tell us how you understand what privacy is in the home as an employer?
2- Do you [**think/trust**] that the smart devices are well designed to protect people's privacy?
3- Did you install the smart device(s) Before/ or After hiring the domestic worker(s)?
4- Have you told your domestic worker that you are using smart device(s)in your home? [Yes/No]] [If Yes]
5- Did you inform the domestic worker(s) before [she/he/they] ask(s) about the smart device(s)?[Yes/No] [If No] Why?
6- Have you told your domestic worker about the function(s) of these smart devices?
7- Did [she/he/they] request anything or put any condition(s) to agree to work with the smart device(s)?
8- Did your domestic worker(s) initiate a conversation with you about that privacy settings of the smart devices?[Yes/No]
9- [If No] Did you discuss with your domestic worker whether [she/he/they] had any preferences about privacy settings or what type of setup you use to protect the data?
10- [If No] Why did you decide not to tell domestic worker?
11- What pros and cons did you consider in making the decision?
12- Have your domestic worker(s) ever asked about the smart device(s) in the home? [Yes/No] [Do you know why?
13- Have you ever had a domestic worker who figured out you had a smart device(s) without you saying so? [Yes/No] [If Yes] What happened?
14- Did you think of any risks associated with **informing** domestic worker(s) about the smart device(s)?
15- Did you think of any risks associated with **NOT informing** domestic worker(s) about the smart device(s)?
16- Have you ever hired a domestic worker(s) who did not accept to work with smart device(s)? [Yes/No] [If Yes] Why?
17- What would you have said or done if your domestic worker(s) had refused to work with the smart device(s) in the home?
18- Would you hire a domestic worker(s) who would not accept to work with smart device(s)?
19- What circumstances might force you to hire a domestic worker(s) without being able to use smart device(s)?
20- Do you currently have a contract with your domestic worker?
21- [If yes] Does the contract specify anything about smart device(s)? [If yes] Who suggested what to put in the contract about that?
22- Is there a way that the domestic worker(s) or whoever else can tell when the device(s) [Is/Are] on?
23- [Do/Does] your domestic worker(s) have access to the data?[ Yes/No]
24- [If No] Do you know whether [she/he/they] [Has/Have] ever accessed the data?
25- [If Yes] Do you know what [she/he/they] do with the data?

26- Do you think that using the smart devices have any effects On the domestic worker's behaviour?
27- Do you think that there might be anything different in your relationship with your domestic worker if you didn't have the smart device(s)?
28- Have you ever talked to your domestic worker about something based on what you [saw/heard] on the smart device(s)? [Yes/No]
29- Would you tell a one-time domestic worker (i.e. babysitter) about the smart device(s)?
30- Do you tell other visitors to your house that you have smart device(s)? [If No] Why?
31- Do you think it would affect your relationship with your domestic worker if they find out about the smart device(s) before you inform them?
32- Do you think whether domestic worker(s) would prefer that you to inform them? [If Yes] Can you guess when exactly?
33- If you went to someone else's house, would you expect them to tell you if they had smart device(s)? Why?
34- Do you know whether there are cameras in your workplace? [If yes] Are you okay with that?
35- What do you think is different between that situation and working as a domestic worker?
36- Do you think domestic workers need to know about devices that are collecting data about them?
37- Do you think there are associated benefits for the domestic workers with the smart device(s)?
38- Does your smart device have an interface where you can review what people have use it for?
39- Do you have concerns about passive [listening/watching] of the domestic worker to you [or/and] your smart device(s)?
40- Do you think it is common for [employers/families] who employ domestic worker(s) to monitor them?
41- [**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?
42- Do you think that **it is the** [**employers/families**] **right** to use smart device(s) whit out informing their domestic worker(s) about them? [Why?
43- Do you think, it would be good if there is a mechanism/function in the smart device that allow domestic worker to inform the device not to record them [audio/video]? What could you think of in this regard?
44- Thank you, I am done. Would you like to add anything or, do you have any comments?

# B.4 Workers Interview Guideline Questions

**A- Warm Up Questions**

1- What is your job type?
2- How long have you had this job?
3- Is it full time job? [**If no**] How often you go to work?
4- Is this your first Job? [**If n**o] For how many [**employers/families**] have you worked before?
5- Do you think it is easy to find a job in your region?
6- How did you get your current job?
7- What do you LIKE about your job? What you DO NOT like?

**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.**

Here we will collect information about the domestic worker's experience of the smart device(s) (e.g. smart speakers, and surveillance (monitoring cameras)).

1- Can you explain what is a smart home in your opinion? And a Smart Device? You may draw what you think of, if you wish?

2- Did you work in smart home before?
[**If yes**]
- When?
- How many times?
- For how long time in total?

3- What are the smart device(s) that [**is/are**] used in the home(s) you are [**working in/have worked in**]?
4- Regarding the smart device functions:
- [**Do they/Does it**] record video/audio?
- [**Is it/are they**] livestreaming 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 how many copies of the data are stored?
- Do you know who can [**see/hear/read**] the data? …Who?

- Do you know how many copies of the data are stored?
- Can you access the data? [If Yes] How do you access it? How do you use it?
- Do the [**employer/family**] keep the device turned on while you are in home?
- [**Is/Are**] the device(s) hidden? [**If yes**] Where inside the home are they hidden?

5- Are there **[kids / elderly people / patients]** living the smart home(s) you [**have worked / are working**] in?
6- [**In your opinion**] Why do you think that the [**employers/families**] have installed the smart device(s)?
7- Do [**employers/families**] use security surveillance cameras?
8- Do you know, if [**employers/families**] use specific device(s) to monitor [**kids/elderly people/patients**] inside their home? Or to monitor you? or to monitor non-family members? Do you know why?
9- Do you know, if the smart device(s) [**is/are**]used for other purposes as well?
10- In your opinion, what are the pros and cons of smart device(s) with:
    - The **[kids'/Elderly's/Patients']** Privacy? Safety?
    - Other family members' convenience? Privacy?
    - Your convenience? Privacy?
    - The home security?
11- Are you aware of the laws and privacy rights about monitoring and recording people in Jordan?
12- [**In your Opinion**] What could make you feel more comfortable about having a smart device in the home?
13- Did you get your job through an agency?

[**If yes**]

- Did the agency offer you any information or advice about smart device(s) in homes?
- Do you know whether they offer domestic workers any information or advices?
- Do they get involved or help with negotiations between [**employers/families**] and domestic workers about smart device(s)?
- Is there advice or information that you wish you had about smart devices? [**Like distributing an information sheet]**
- What information or advices do you think would be helpful for them to give [**employers/families**] about smart device(s)?

[**If no**]

- If you were going through an agency, what kind of information or advice do you think it would be helpful for them to give [**employers/families**] about smart device(s)?

**D- Questions to Explore Domestic Workers' Expectations, behaviours, and attitudes, toward smart devices.**

14- Can you tell us how you understand what privacy is in the home for you as a domestic worker?
15- Can you tell us how you understand what privacy is in the home if you are the employer?
16- Do you [**think/trust**] that the smart devices are well designed to protect people's privacy?
17- Did your [**employers/families**] inform you about the smart devices in the home?

[**If yes**]

- Did you accept working with smart devices? Why?
- Did you give your consent to be observed and [**audio/video**] recorded?
- Did you [**agree/disagree**] directly?
- Did you show any concerns?
- Did you request anything? Did your employer accept?

[**If No**]

- Tell us about that experience?

18- Have you felt that your privacy is affected by working in smart homes?
    - [**If yes**] Tell us how did you feel about that? Did you do anything?
19- Do you think that your performance has been improved with the smart devices in the home?
    - [**If yes**] What are the reasons?
20- Have your attitudes changed over time with the smart devices in the home? [**If yes**] How?
21- Did you experience any privacy conflict that is related to smart devices with your [**employer/family**]?

[**If yes**]

- Did you negotiate with your [**employer/family**]?

- How did you negotiate it with your [**employer/family**]?
- Did you resolve it? [**If yes**] How, [**If no**] Why?

22- What risks are you Concerned about smart devices?
23- What risks are you **NOT** Concerned about smart devices?
24- Did you try to take any technical action toward the smart devices?
[**If yes**]
- Why?
- Did you try to switch it off while you are around?
- Did you try to stop it from recording while you are around?
- Did you try to disconnect it from the internet while you are around?
- Did you try to change the way it is functioning?
- Did you succeed? [If no] Why?
- Did you tell your employers about that or did they know about it? What happened?

25- [**In your opinion**] What are the pros and cons of informing you about the smart device(s)?
26- Did you think of any privacy risks associated with **NOT** informing you about the smart device(s)?
27- Have you ever figured out smart device(s) in the home before you were informed?
[**If yes**]
- What happened?
- How did you figure it out?
- Did you say anything to your employer? What did they say?
- Do you think it affected your relationship with your employer after you found out?
- Do you think, they should have told you before? Or they do not have to?

28- What would you have said or done if your employer **insists** on using the smart device(s) in the home without your consent?
29- Have you ever refused to work in smart homes before? Why?
30- Have you ever discussed with your employer your preferences about privacy settings that make you able to tell when the device(s) [**is/are**] recording or live streaming?
31- [**In your opinion**] Do you think that smart device(s) affect your behaviour? [If Yes] How? The [**employers/families**] behaviour?
32- Do you think there are associated benefits for you with the smart device(s)? Legal benefits?
33- [**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?
34- Do you think that **it is the** [**employers/families**] **right** to use smart device(s) whit out informing their domestic worker(s) about them?
- [**If yes**] Why?
- [**If no**] Why? Do you think they should ask domestic worker's permission?
- [**If no**] Do you think they should ask whether the domestic worker(s) want them to turn off or unplug the smart device(s) while they are working?

35- [**From your experience**] What approaches could be effective in increasing domestic workers/visitors **visibility** in smart devices design?
36- Do you think, it would be good if there is a mechanism/function in the smart device that allow domestic worker to inform the device not to record them [audio/video]? What could you think of in this regard?
37- [If you know] Can you tell me according to your understanding, what [**is/are**] the difference(s) between privacy rights and data protection rights?
38- Thank you, I am done. Would you like to add anything or, do you have any comments?

# C

# Chapter 5 Supplementary Material

We present in this appendix supplementary material relating to Chapter.5. We provide copies of the second study advertisement poster, screening survey questions, families' interview guideline questions, and workers' interview guideline questions.

# C.1 Second Study - Advertisement Poster

DEPARTMENT OF COMPUTER SCIENCE

## VOLUNTEERS NEEDED FOR INTERVIEWS

CUREC Approval Reference: (**CS_C1A_021_038** )

**Exploring How Smart Home Devices Affect and Reflect Users' Relations**



**What: -**

- *45-60 minutes* of audio recorded interview.
- Do we use smart devices, or deal with it in the home?
- Do you have any concerns about smart home devices?
- How do smart devices affect users' relations in the smart home?
- Are you aware of data protection regulations in Jordan?
- How could we improve smart devices to address concerns uses may have?

Who: ***over 18 years*, know about 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-2

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

## C.2 Second Study - Screening Survey Questions

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

**Language**

2- What is your preferred language to communicate with?
- English
- Arabic
- Both are fine
- None

**Age**

3- Age (Only 18+ years participants can participate in this survey)
- Less than 18 years [
- 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
- Few months
- 1 Year

- 2 years

**Involvement with Smart Devices**

8- Describe your level of involvement with smart home devices?
- User
- Working in a home with smart devices
- Regulator
- Labour Law Expert
- Activist

**Bystanders**

9- Do you have domestic worker [full time/part time] in your home?
- Yes
- No

**Permission**

10- 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**

11- 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**

12- Thank you for participating in this survey.

## C.3 Second Study Families Interview Guideline Questions

**A- Warm Up Questions**

1- How many people live in the house?
2- Do you have a domestic worker? Is it fulltime worker? [IF NOT] How often do your domestic worker work in your home? For how long have you had your domestic worker?
3- Is your worker Jordanian? [IF NOT] What is his country of origin?
4- Is it easy to find a good worker? Is it easy for workers to find a job?
5- [In your opinion] How you can build good working relation with your domestic worker?
6- What is your general knowledge of smart devices and smart homes?

**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)**

7- Do you use smart devices in your home? What are the smart devices that you use in your home? What they do? Why do you use them? What is your general knowledge of smart devices and smart homes? What they record data about people in the home? Where the data is stored? Who [is/are] the admin(s) of the smart device(s)?
8- Do you allow the worker to use the devices? Can she/he control her/his data? Please explain
9- Do you have specific device(s) to check on your [kids/elderly] inside your home? Please explain.
10- Do you have specific device(s) to check on domestic worker(s) inside your home? Please explain.

**D- Power Dynamics from the Families' perspectives.**

1- Did you install the smart devices before or after hiring you worker? Can you describe your relation with your worker? Do you think using smart devices have affect this relation? Please explain. How do you think you can build good relation with the worker?
2- Do [Would] you feel comfortable having smart device in your home?
3- Does your worker know about the devices? Have you told your domestic worker about the devices, and what they do? Please explain. What was the worker's response? Did she/he discuss or negotiate anything about using the devices with you?

4- [ if the worker accepts working with the devices] Why do you think she/he accept working with the devices?
5- [If the worker rejects the job because of the devices] Can you explain why? Did she/he put any request or condition to take the job? [ If so] would you accept these requests/conditions? Please explain
6- Do you currently have a contract with your domestic worker? Does the contract specify anything about smart device(s)? in addition to the salary, what other benefits do you provide to your worker? [ phone, weekly vacation]
7- Do you think that using the smart devices have any effects on the domestic worker's behaviour, performance?
8- Have you ever talked to your domestic worker about something based on what you [saw/heard] on the smart device(s)? Did you mention what you [saw/heard] directly? Did you find another way to bring it up? How did that conversation go? Have you ever shared a collected data with anyone?
9- Do you think it is your right to use the devices inside your home? Would you ask the domestic worker for a permission? Do you think it is the worker's right to be informed and/or to consent for the smart devices? Please explain.
10- Do you think there are associated benefits for the domestic workers and for you with the smart device(s)? [Legal benefits]
11- Would the gender or the nationality of the worker make any difference in how you deal with her/him?
12- Do you think households' and workers' rights are well defined? Please explain.
[Will see if participant will mention data protection regulation in Jordan, and regulation could support privacy protection of people, and support building good relation with the workers]
13- Thank you, I am done. Would you like to add anything or, do you have any comments?

## C.4 Second Study Workers Interview Guideline Questions

**A- Warm Up Questions**

1- What is your job type?
2- How long have you had this job?
3- Is it full time job? [If no] How often you go to work?
4- Is this your first Job? [If no] For how many [employers/families] have you worked before?
5- Are you Jordanian? If not, what is your country of origin?
6- Do you think it is easy to find a job in your country/region? How did you get your current job?

**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, smart devices.**

1- During the recruitment phase of this study, you mentioned that you have worked for families that have smart devices. Can you tell me how many devices were in the home(s) you have worked in? do you know what these devices are/were?
2- Do you know if these devices are connected to the internet? What kind of data the devices are collecting? Where is it stored? Do you have access to it?
3- [In your opinion] Why do you think that the [employers/families] have installed the smart device(s)?
4- Do you have any concerns with the devices and the data collection process?
5- Do you know, if [employers/families] use specific device(s) to monitor [kids/elderly people/patients] inside their home? Or to monitor you? or to monitor non-family members? Do you know why?

**D- Questions to Explore power dynamics between households, and domestic works.**

1- Can you describe your relation with the family? Do you feel ok with the smart devices in the home? please explain? [ will see if participant will mention if devices affect relation with families]
2- Do you know about the devices? please explain. Do you know how to use the devices? Are you allowed to use them? Do you have access to data collected by the devices (i.e., images, videos, sounds)?
3- Do you know if the family can access the devices remotely? Why do you think they access the devices remotely?
4- Do you feel comfortable with the devices? Explain please.
5- Did the family take your permission to monitor the place where you work in?

6- Do you know if they family has the right to monitor people in the home? Please explain.
7- Have you rejected a job because of smart devices? Why would you accept a job in a home with smart devices?
8- How could you build good relation with the family?
9- How could you manage your concerns about smart devices? Have you discussed this situation with the family? If yes, can you tell me, how was it? Did you resolve it?
10- What effects do you think smart devices have on your attitude, practices, and performance?
11- Do you think there are associated benefits for you with the smart device(s)? [Legal benefits]
12- Thank you, I am done. Would you like to add anything or, do you have any comments?

## C.5 Second Study Regulators Interview Guideline Questions

**A- Warm Up Questions**

1- Can You tell me briefly about yourself and your job?
2- Did you work for private or public sector?
3- How many years of experience do you have in this field?
4- Can you tell me briefly about your experience with privacy/data protection regulations/policies in Jordan?

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 participants' experience with smart devices**

1- What is your understanding and experience of the smart devices/homes?
2- Do you think people use smart devices to watch/monitor their workers inside their homes?

**D- To explore participants' understanding of privacy in the smart home**

3- Do you think smart devices are threatening the workers/family's privacy? Please explain
4- Do you think it is the family's right to use smart devices to monitor/watch their workers in the smart home? Please explain
5- Do you think it is the workers' right to be informed about the installed smart devices in the house? please explain.

**E- To explore participants' understanding of the power dynamics between user groups in the smart home**

6- Do you think workers can enforce their privacy preferences in the smart home? In your opinion, how can we reduce the impact of the asymmetric power dynamics between workers and families in the smart home?
7- What are domestic workers rights in Jordan?
8- Are families allowed to use smart devices inside homes? Please explain.

9- Do you think it is the workers' right to be informed about the installed smart devices in the house? Do you think it is the workers' right to consent to be monitored/recorded by the smart devices in the smart home? Please explain.
10- How do you think culture, norms, and religious back ground affect the power dynamics between workers and households? How can we empower workers to balance the power dynamics with the households?

**F- To explore participants' experience with data and privacy protection regulations**

11- Does Jordan have data/privacy protection regulations for smart homes users? Please explain
12- Do you think people consider privacy regulations and rights about monitoring and recording workers/guests in their homes before they do that? Please explain
13- Do you think the existing policies and regulations in Jordan are taking into consideration users' privacy concerns? Please explain.
    - [ If No Laws exist] What are the implications of the lack of explicit data protection laws on people's privacy in the smart home? Please explain. How close is Jordan to issue the new data protection law?
    - [From your experience and knowledge] Is the expected data protection law will be inspired by the European GDPR? How could it be tailored to fit the Jordanian context? Will the Jordanian policymakers take into consideration people's privacy concerns and the contextual influences (i.e., norms and religious background of the country? please explain
    - How do you expect the new data protection law will be different from the exiting cybercrime law in Jordan? How can the new data protection law improve and support users' agency in the smart homes?
    - How could new data protection law influence/enforce smart devices vendors to produce smart devices with enhanced privacy protection features? please explain
    - How can the new data protection law limit the family's autocracy inside the home and enforce families to consider privacy concerns of their domestic workers?
14- How do you think people practices could support protecting their privacy in the smart homes in Jordan? Please explain
15- Do you think there are any associated benefits for the domestic workers and families from the new data protection law in Jordan? How can we support privacy protection of people in the smart home?
16- I am done with my questions. Do you like to add anything?

## C.6 Second Study Activists Interview Guideline Questions

**A- Warm Up Questions**

1- Can You tell me briefly about yourself and your job?
2- Did you work for private or public sector? How many years of experience do you have in this field?

**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 participants' experience with smart devices**

1- What is your understanding and experience of the smart devices/homes?
Do you think people use smart devices to watch/monitor their workers inside their homes? Please explain. Why do you think they do so?
2- In your opinion, what are the pros and cons of using smart device(s) to monitor domestic workers in home by the families?
3- Do you think smart devices are threatening workers privacy in the smart home?

**D- To explore participants' understanding of power dynamic with the smart home**

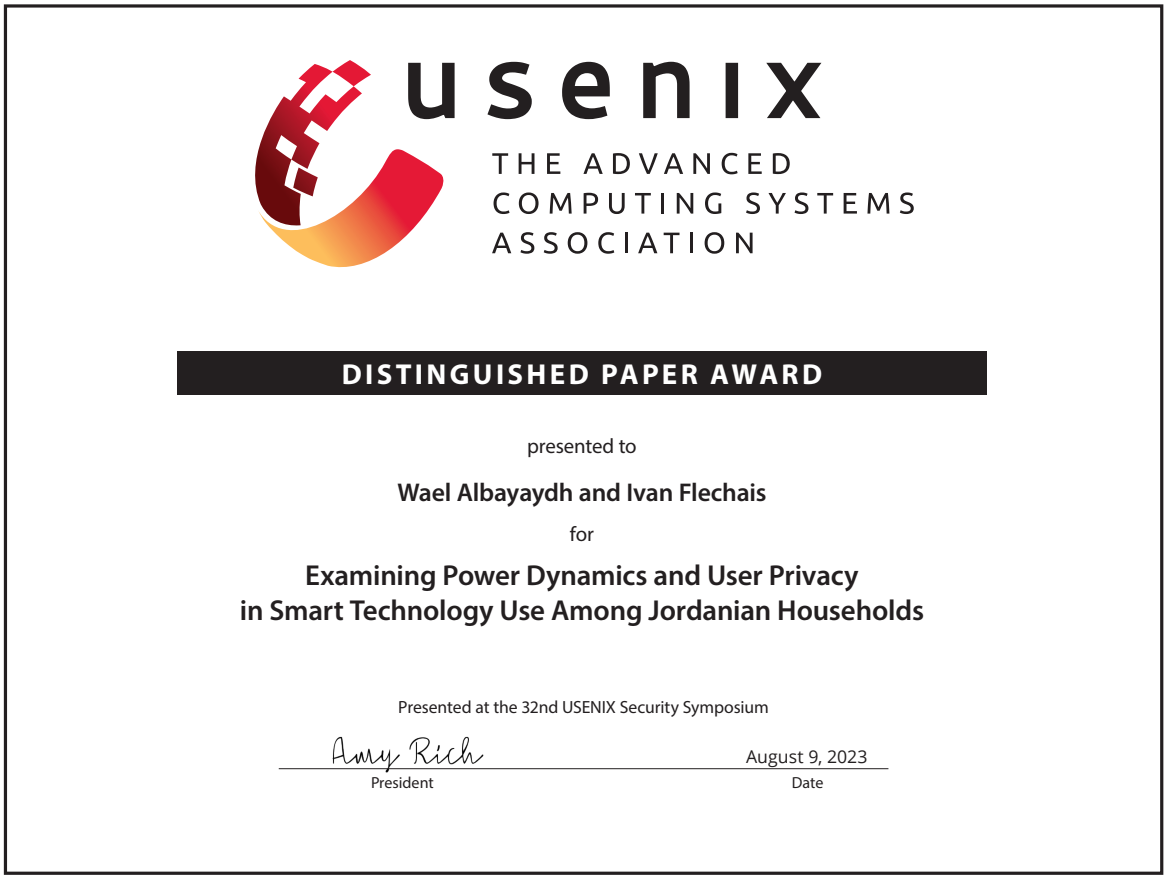
4- What is your understanding of domestic workers rights in Jordan?
[ will see if participant mentions any sufferings, or challenges]
5- Are families allowed to use smart devices inside homes? Do you think it is the family's right to use smart devices to monitor/watch their workers in the smart home? Please explain.
6- Do you think it is the workers' right to be informed about the installed smart devices in the house? Do you think it is the workers' right to consent to be monitored/recorded by the smart devices in the smart home? Please explain.
7- Do you think workers can enforce their privacy preferences in the smart home? Please explain.
8- How do you think culture, norms, and religious back ground affect the power dynamics between workers and households?
How can we empower workers to balance power dynamics with the households? how can we reduce the impact of the asymmetric power dynamics between workers and families in the smart home?

**E- To explore participants' experience with data and privacy protection regulations**

9- What do you know about existing data/privacy protection policies in Jordan? Are they taking privacy concerns into consideration? Do you think they can support privacy protection of domestic workers and families in the smart homes? Please explain

10- Do you think the existing privacy policies and regulations are taking into consideration the contextual influences (i.e., norms and religious background of the society)?
11- How do you expect the new data protection law will be different from the existing laws in Jordan?
12- How can the new data protection law improve and support users' agency in the smart homes? How can the new data protection law address privacy protection of workers in the smart homes, where the family's home is the domestic worker's workplace? Please explain
13- How can new data protection law influence/enforce smart devices vendors to produce smart devices with enhanced privacy protection features?
14- How can the new data protection law limit the family's autocracy inside the home and enforce families to consider privacy concerns of their domestic workers and guests?
15- What are the challenges that face enactment of the new data protection law in Jordan?
In your opinion, how can we support privacy protection of people in the smart home
16- I am done with my questions. Do you like to add anything?

## C.7 USENIX - Distinguished Paper Award



usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

**DISTINGUISHED PAPER AWARD**

presented to

**Wael Albayaydh and Ivan Flechais**

for

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

Presented at the 32nd USENIX Security Symposium

Amy Rich — President

August 9, 2023 — Date

# D

# Chapter 6 Supplementary Material

We present in this appendix supplementary material relating to Chapter.6. We provide copies of the third study advertisement poster, screening survey questions, families' interview guideline questions, and workers' interview guideline questions.

# D.1 Poster - Users

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 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

# D.2 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

# D.3 Poster - Designers and Industry 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 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.4 Screening Survey Questions

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.

# D.5 Families Interview Guideline Questions

**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?

# D.6 Workers Interview Guideline Questions

**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?

8- Do you feel comfortable working with smart devices? What could make you feel comfortable about having a smart device in the home?
9- Do you have any concerns with smart devices?
10- What are the most concerning smart devices for you? Why?

**C Questions to Explore Domestic Workers' Expectations, behaviours, and attitudes, toward smart devices.**

1- Do you [think/trust] that the smart devices are well designed to protect people's data?
2- Do you have any concerns with smart devices design or functions regarding data collections, and protecting people's data?
3- Did families inform you about the smart devices in the home? Please explain.
4- Have your attitudes/behaviours changed over time with the smart devices in the home? How?
5- Did you try to take any actions [technical or non-technical] to reduce risks of working in smart home with the smart devices? Please explain
6- Have you ever refused to work in smart homes before? Why?
7- Have you ever discussed with your employer your preferences about smart device settings?
8- Do you think that it is the [employers/families] right to use smart device(s) whit out informing their domestic worker(s) about them? Please explain
9- What approaches could be effective in protecting data of people with the smart devices design?
10- Do you think, it would be good if you are notified about smart devices?
11- How could we improve data protection of people with smart devices?
12- Who is responsible for protecting people's data in your opinion?
13- Thank you, I am done. Would you like to add anything or, do you have any comments?

## D.7 Local Leaders Interview Guideline Questions

**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?

# D.8 Designers Interview Guideline Questions

**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?

# D.9 International Leaders Interview Guideline Questions

**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?

# E

# Chapter 7 Supplementary Material

We present in this appendix supplementary material relating to Chapter.7. We provide copies of the fourth study advertisement poster, screening survey questions, families' interview guideline questions, and workers' interview guideline questions.

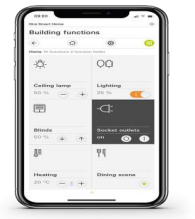
# E.1 Poster - Users

DEPARTMENT OF COMPUTER SCIENCE

## VOLUNTEERS NEEDED FOR FOCUS GROUP STUDY

CUREC Approval Reference: [CS_C1A_23_012]

**Focus Group Study – Mobile Application to Support Privacy Protection in Smart Home**




**What: -**

- *60-90 minutes* of audio recorded group discussion.
- Do we use smart devices, or deal with it in the home?
- Are you concerned about smart home devices?
- Do you have general understanding of MENA Arab culture?
- How could a mobile application protects users' privacy in the smart home?

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

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

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

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

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

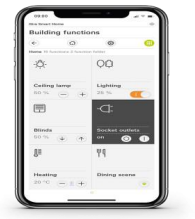
# E.2 Poster - Designers and Mobile Developers

DEPARTMENT OF COMPUTER SCIENCE

## VOLUNTEERS NEEDED FOR FOCUS GROUP STUDY

CUREC Approval Reference: [CS_C1A_23_012]

**Focus Group Study – Mobile Application to Support Privacy Protection in Smart Home**




**What: -**

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

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

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

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

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

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

# E.3 Screening Survey Questions

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

**Consent**

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-11]

**Language**

2- What is your preferred language to communicate with?
   - English
   - Arabic
   - Both are fine
   - None [Jump to Question-11]

**Age**

3- Age (Only 18+ years participants can participate in this survey)
   - Less than 18 years [Jump to Question-11]
   - 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

**Involvement with Domestic Workers and Smart Devices**

6- Describe your level of involvement with domestic workers and smart home devices? [Check all that applies]
   - Owner or User of Smart Devices
   - Employer of Domestic Workers
   - I am Domestic Worker (e.g., Nurse, Nanny, Babysitter) in Smart Home [Jump to Question-15]
   - Designer of Smart Devices
   - Developer of Mobile Applications
   - Regulator / Policy Maker
   - Domestic Workers Recruiting Agency
   - Other

**Used smart devices**

7- What are the smart devices that you use? (You may choose multiple answers)
   - None [Jump to Question-11]

- Smart Cameras
- Smart Speakers/Assistance
- Smart TV
- Smart Door Look / Door Bell
- Smart Toys
- Smart Security Systems
- Smart Heating System
- Others

**Experience with Smart Devices**

8- How many years of experience do you have with smart devices?
- No Experience [Jump to Question-11]
- Novice
- Competent
- Expert

**Permission**

9- 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**

10- 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**

11- Thank you for participating in this survey.

# E.4 Focus Group Guidelines

**Focus Group Guide: Enhancing Bystander Privacy Protection: A Mobile App Approach for Jordanian Smart Homes.**

**Welcome and Focus Group Introduction.**

**Skill Assessment.** Before we start the discussions, we will ask questions and observe responses to understand participants' 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?

**[Then We Start the Group Discussions]**

**Discussion 1: Smart Home Technology and Privacy Concerns:**

- Discuss smart home technology.
- Explore prevalent devices and systems.
- Engage in a conversation about participants' experiences with using smart home devices.
- Explore concerns regarding data privacy with smart home devices.

**Discussion 2: Mobile App for Privacy Protection:**

- Explore how a mobile app could contribute to enhancing privacy for domestic workers.
- Delve into the feasibility and practicality of implementing such a solution.
- Investigate the challenges associated with adopting this privacy-focused app.
- Explore participants' preferences regarding features that effectively address privacy concerns.
- Discuss key desired features, seeking participants' perspectives and insights.

**Discussion 3: Stakeholder Responsibilities with Privacy Protection.**

- Delve into thoughts on who bears the responsibility for privacy protection of domestic workers in smart home devices.
- Discuss the roles of households, workers, designers, developers, and policymakers in addressing privacy concerns.
- Explore participants aspirations in this regard.

**Discussion 4: Balancing Privacy and Convenience:**

- Explore the importance of smart home device for users.
- Explore the importance of addressing privacy concerns with smart home devices for all users and specifically the domestic workers.
- Discuss scenarios where participants would compromise privacy for convenience.
- Investigate how mobile apps can support as a helping tool to find a balance.

**Discussion 5: Features for Protecting Workers Data and Privacy**

- Engage in a discussion about participants' perspectives on potential features within a mobile app designed to protect workers' data and privacy.
- Explore further ideas regarding predefined features and invite suggestions for additional functionalities.
- Discuss the feasibility and practicality of the proposed features and functionalities.
- Delve into the challenges and concerns associated with the suggested features.

**Discussion 6: User Feedback:**

- Encourage participants to share their thoughts, concerns, and additional ideas.
- Ask participant to make a final comment on the discussed topics.

**Conclusion and Closing Thoughts**

# E.5 App Evaluation Interview Guidelines

## Interview Guide

**Warm-up Questions:**

1- How was your overall experience using the privacy protection app for domestic workers in smart homes during the past three weeks?
2- Can you share any specific positive or challenging situations you encountered while using the app?
3- What are your thoughts on this application designed to enhance privacy protection for domestic workers in smart homes? The App's merits, drawbacks, and the practicality of this solution?
4- How do you think the app could contribute to privacy protection in a smart home environment?

**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?

**Main Questions**

1- Did you find the app to be a practical solution for addressing privacy concerns in smart homes? What about utilizing websites? Why or Why not?
2- Can you explain your detailed perspective on the features and functionalities of the app?
3- Are there specific features of the app that you found particularly useful or effective in promoting privacy protection?
4- What features do you believe are currently missing or could be improved to enhance the app's functionality?

5- In your opinion, do you think that actively encouraging and facilitating privacy discussions between domestic workers and families could practically improve privacy protection for domestic workers?
6- In your opinion, what additional functionalities or features would you like to see implemented in the app to better support privacy discussions between workers and families?
7- Based on your experience, do you believe families would be willing to allow domestic workers to use this app, and why or why not?
8- In your opinion, what are the challenges or limitations in using the app for enhancing privacy protection?
9- What measures or guidelines provided by the app did you find most helpful in maintaining privacy within the smart home environment?
10- Were you able to easily scan and identify smart devices using the app's scanning feature? How do you think this could support privacy protection?
11- How user-friendly did you find the proposed communication channels within the app for reporting privacy violations, providing feedback, and seeking guidance?
12- How do you think the chat feature with privacy experts is helpful and supportive to privacy protection?
13- What do you think about enforcing families to use the App, and to allow workers to use it? How do you think we can achieve this?
14- In your view, can recruitment agencies play a role in ensuring the utilization of the app in smart homes? If so, how?
15- How about incorporating the use of the app into employment contracts for enforcement?
16- Does the new data protection law in Jordan support data and privacy protection of individuals in smart homes?
17- Can regulatory measures and policies be employed to enhance the implementation of app usage in Jordanian households? Why? How?
18- Lastly, do you have any additional comments or suggestions for improving the app to better meet the needs of domestic workers in smart homes?

# F

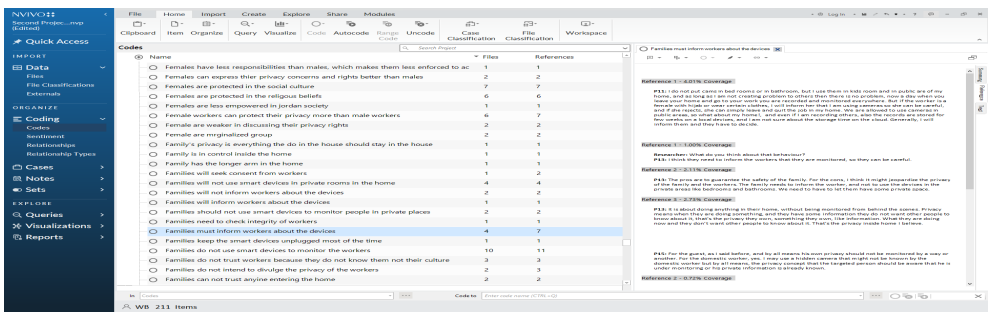
# Methodology and Approach Supplementary Material

In this section, we present illustrations of the activities conducted in this research study. This includes samples of posts on social media platforms, a screenshot demonstrating the utilization of Nvivo[76] for coding collected data, and another screenshot from the online focused group meetings held during the fourth study.

## F.1 Screenshot of NVivo Software

This section shows a screenshot of employing the software tool NVivo for coding the data scripts.

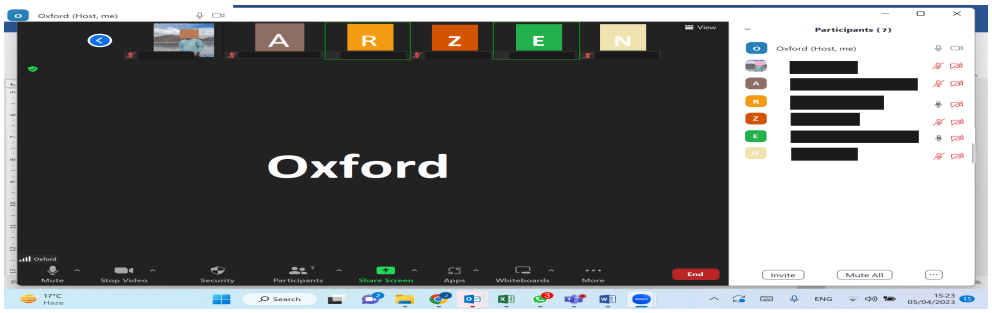
**Figure F.1:** Screenshot of the NVivo Software



## F.2 Screenshot of Focus Group Meeting

This section shows a screenshot from one of the online focus group meetings held during the fourth study.

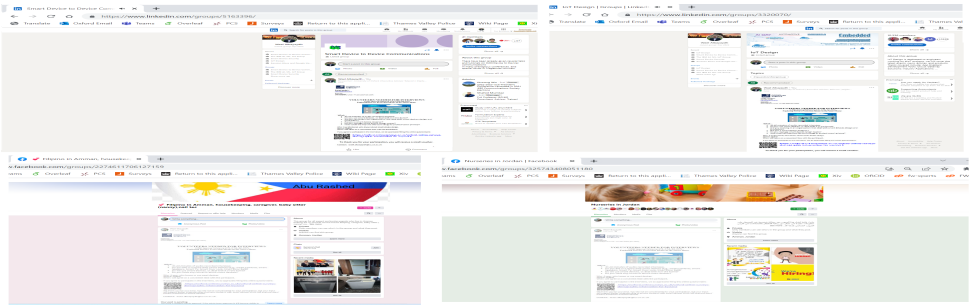
**Figure F.2:** Screenshot From a Focus Group Meeting




## F.3 Screenshot of Posting Study Posters on Social Media Platforms

This section shows a screenshot of sharing study posters on social media platforms.

**Figure F.3:** Screenshots of Posters Shared on Social Media Platforms



# G

# Ethics Applications and Approval

As detailed in Section.3.4, all studies presented in this thesis underwent a comprehensive review and received approval from the Central University Research Ethics Committee1 (CUREC) n the University of Oxford. CUREC holds the overarching responsibility for shaping Oxford University's Research Ethics Policy and overseeing the ethical review process at the university.

This appendix comprises the application materials for the CUREC-approved studies: CSC1A21001 (cf. Section §G.1), CS_C1A_021_038 (cf. Section G.2), CS_C1A_22_007 (cf. Section G.3),and CS_C1A_23_012 (cf. Section G.4). Each attached CUREC application includes information sheets, survey guidelines, interview question guides, consent forms, and poster advertisements. Participants were at liberty to skip any question, and to withdraw from the study at any point. (cf. Table 3.1).

## G.1 First Study - Ethics Application

### G.1.1 First Study - Advertisement Poster

For the advertisement poster of the first study, please refer to Appendix B.1.

### G.1.2 First Study - Survey Question Guidelines

For the survey question guidelines of the first study, please refer to Appendix B.2.

### G.1.3 First Study - Interview Question Guidelines

For the interviews' questions guidelines of the first study, please refer to Appendix B.3, Appendix B.4.

# G.1.4 First Study Ethics Application

**CENTRAL UNIVERSITY RESEARCH ETHICS COMMITTEE (CUREC)**

**Form CUREC 1A Checklist for the Social Sciences and Humanities**

The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

- Please check **"Where and how to apply for ethical review"** and the **CUREC flowchart** first to see if you need ethics approval.
- Please complete this form using a word processor and email it, together with your supporting documents, to your **Departmental Research Ethics Committee (DREC)** (**if applicable**). If you don't have a DREC please email this form to **ethics@socsci.ox.ac.uk** using your official **ox.ac.uk email** address. **Only type-written, emailed applications will be accepted.**

| **SECTION A: Filter for CUREC 2 application**<br>This section determines whether your study raises more complex issues requiring the completion of a full application for ethical review, known as the CUREC 2 application. **(Please mark 'X' in the Yes/No column.)** | | |
|---|---|---|
| 1. Are research participants classed as **people whose ability to give free and informed consent is in question**? (This may include under 18s (although see "competent youths"), prisoners, or adults "at risk".) Your attention is drawn to the University's **Safeguarding Code of Practice** and its implications for researchers involving children or adults at risk. This includes the need for the work to be risk assessed and for researchers to undertake related training.<br>(**Note**: If any of your participants are aged 16 or under, answer 'Yes' here **and** also answer question 5 below.) | Yes ☐ | No ☒ |
| 2. By taking part in the research, will participants be at risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)? | Yes ☐ | No ☒ |
| 3. Does the research involve the **deception** of participants? | Yes ☐ | No ☒ |
| 4. Does your research raise issues relevant to the **Counter-Terrorism and Security Act (the Prevent duty)**, which seeks to prevent people from being drawn into terrorism? Please see advice on this on our **Best Practice Guidance web page**. | Yes ☐ | No ☒ |
| If you answered 'No' to all the questions above, go to **Section B**. If you answered 'Yes' to any question above, continue to question 5 below. | | |
| 5. Is your project covered by a CUREC **Approved Procedure** (formerly known as "CUREC Protocols")? | Yes ☐ | No ☒ |
| If yes, give the specific Approved Procedure number(s): | | |
| If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **stop completing this checklist and do not submit it for ethical review**. Instead, complete the CUREC 2 application form from the CUREC website, then submit that for ethical review.<br>If you answered '**Yes'** to ANY of questions 1-3, **and** answered '**Yes'** to question 5, go on to **Section B**. | | |

| **SECTION B: Contact details and project description** | |
|---|---|
| **Contact details:** | |
| 1. **Principal investigator** OR supervisor (if student research) (give title and full name) | Prof. Ivan Flechais |
| 2. Name of student (if student research) | Wael Albayaydh |
| 3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil | DPhil |
| 4. Department or Institute name | Department of Computer Science |
| 5. Address for correspondence (if different from above) | Wael Albayaydh<br>St Hilda's College, Cowley Place<br>Oxford OX4 1DY<br>UK |
| 6. University (**not** private) e-mail address and telephone number | wael.albayaydh@cs.ox.ac.uk |
| 7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant) | |

| **Project description:** | |
|---|---|
| 8. Title of research project | Exploring Bystanders' Privacy Concerns with the Smart Home in the Middle East. |
| 9. List of location(s) where project will be conducted | Jordan |
| 10. If your research involves overseas fieldwork or travel and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This must be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.) Please also address any physical or psychological risks for Oxford researchers and local fieldworkers in Section 16 below and discuss with your safety officer. | Yes ☒<br>No ☐<br>Not required in this instance ☐ |
| 11. Anticipated duration of overall research project | months or 1 years (maximum 5) |
| 12.a) Anticipated start and end dates of the part of the research project involving human participants and/or personal data | From: (15/01/21)<br>To: (15/07/21)<br>**Note**: You will need ethics approval **before** you start your research. CUREC 1As may take up to 30 days to process. **Retrospective ethics approval cannot be granted.** |
| 12. b) In the case of international or collaborative research, will you submit or have you submitted this project for ethical review or consideration | Yes ☐<br>No ☒ |

| | |
|---|---|
| elsewhere (e.g. collaborator's/local ethics committee, or other local approval)? | If 'Yes', please attach ethics or other approvals and give more details below.<br>If 'No', please explain your reasons below. Please also refer to the Best Practice Guidance on Ethical Review of social-sciences based research conducted outside the UK and the Ethics Issues Checklist for International Research. Online at: https://researchsupport.admin.ox.ac.uk/governance/ethics/resources/bpg |
| 13. **External** organisation funding the research (if applicable) | |

14. a) Title and brief description of **research** (about 150 words) in lay language.
When describing the research, include your methodology, how you are applying professional guidelines, and the use to which results/data will be put. **Please also declare any conflicts of interest here.**

Title: "Exploring Bystanders' Privacy Concerns with the Smart Home in the Middle East"

This work is the first phase of my DPhil research study which aims to understand privacy concerns of bystanders in the smart home environments, the research study will focus on domestic workers (e.g. home maintenance workers, nannies, babysitters, care givers) in the smart homes. The project intends to understand domestic workers' perspectives of privacy in the smart home, their behaviours toward the smart devices, their understanding of these devices, and how these devices could affect their privacy, on the other hand, we will try to understand the employers' (i.e. families') perspectives of privacy in the smart home, how they use these devices, whether they inform their employees about them, whether they take their consents to be audio and video recorded by the smart devices, and do they care about the employees' privacy in their homes.

We will conduct a semi-structured interviews with both domestic workers (employee) and employers (the families). The participant's consent will be secured prior to the interview.

English language is the language of interaction for this research. But we may provide Arabic translation ( if needed, but this is very un-expected)

There is no conflict of interest associated with this research.

14.b) Description of participants and how you will **obtain informed consent** to take part in the research (about 200 words)

1. Description of participants **and** your criteria for inclusion/exclusion

   Participants include individuals (over 18) and households (groups of people over 18). Children will not be included.

   Interviews are to be conducted in Jordan, and hence participation is geographically limited. Because of the current pandemic (i.e. COVID-19), Skype/Zoom will be used to interview participants online as per their choice. The researcher will not use Zoom/Skype to audio record the interviews. The researcher will use his local laptop recoder to record the interviews.

2. Your method(s) of recruitment

The researcher will recruit participants through domestic workers agencies in Jordan, social media specialzed pages, and smart devices sellers. The recruitment poster will be posted on the social media specialzed pages, and will be sent to the domestic workers agencies in Jordan, and to the smart devices sellers.

Participants will be pre-screened before they are invited to participate in the interviews. Pre-screening is done using JISC Online Survey(Questionnaire) to collect anonymously the participants' Demographic Information.

Screening will be used to identify eligible participants. The online survey link will be announced on the recruitment poster. Interested participants will fill the online survey and will be requested to provide their names and email addresses if they wish to be contacted to participate in the research interviews.

After identifying the eligible participants, we will assign a unique ID code for each participant to keep her/him personal ID anonymous. The participants' names, email addresses, and the unique ID codes will be stored securely in a participants' information sheet on the researcher laptop only, and only the researcher can map the unique ID codes to the participants' personal IDs.

The collected names and email addresses will be used to contact the identified eligible participants for the research interviews. All information collected for any ineligible person who has filled the JISC Online Survey will be deleted permanently.

During the online survey, we will take consent from participants that the collected information during the screening stage will be used to generate some statistics and will be part of the research study outcomes.

The online survey will ensure that the submissions of the Demographic Information is safe and secure. Information on the pre-screening surveys will be a subset of the demographics informatuon questionnaire (e.g. form of housing (renter, owner); number of people in the household; and the types of the smart home devices (entertainment, health care, ...)).

During and after the interviews, the researcher will use the participants' unique ID codes to refer to the participants on the audio recorded interviews, and the transcribed Interview texts.

In the screening online Survey, the researcher will ask both the participants (employers and the employees) if they do mind that we contact their employees or employers respectively. If they agree, we ask them to share this online survey with their employees or employers. If they prefer not to contact them, we will not do that. We can interview employees and employers from different households (no pairing), and for those who agree, we will interview both parts from the same household (pairing).

For employers or employees who show interest in participating in the research interview, we will send them the Skype/Zoom link, and we will not interfere in how they will connect to Skype/Zoom to do the interview. We will not impose on both the employees or the employers how to connect to Skype/Zoom. We are aware of the huge power imbalance between both parties, and this is the reason that we ask both parties to tell us if they prefer that we contact the other party.

- If the employers agree, this means that they do not mind, and they will give the employees freedom to do the interview and to speak freely.
- For the employees who prefer not to contact their employer, we will ask them in the interview invitation to choose a suitable time and place to Connect to Skype/Zoom so they can speak freely.
- For employers and employee who prefer not to contact the other party, we will not do.
- For those who cannot secure a time and place to do the interview and speak freely, we will not interview them, and will tell them to contact us in the future if the situation changed.

To thank the participants for thier participation, They will receive an £10 Amazon voucher (or equivalent voucher)!

3. Your processes for obtaining consent from participants

> Oral consent for participation will be requested and recorded from individuals directly at the beginning of the interview.We will explain the purpose of the study and intended usage of collected data. The information sheet will be provided to the participants at least 24h in advance to their participation. The information sheet shows all details regarding data handling.

Please **attach separate supporting documents (in Word)** if appropriate for your research (English language versions only). Tick those you are submitting below. If appropriate supporting documents are not submitted, you will be asked to provide these separately, which may delay the ethical review process.

- ☒ Recruitment and advertisement material (e.g. a poster, social media recruitment text, or brief invitation letter/ email)
- ☒ Information for participants to read (or hear) before they agree to take part (e.g. written information or, if applicable, an outline oral information script).
- ☒ A document to record informed consent. Templates for written consent forms and/or oral information scripts (in case of an oral consent process) are available from the CUREC website
- ☒ Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire)
- ☐ (If relevant) debriefing document after participants have taken part
- ☐ If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants
- ☐ Please complete section 15 if you cannot obtain informed consent

*Please add any further details here.*

No further details to be added.

15. If you cannot obtain informed consent from participants according to CUREC guidelines and good practice in your discipline, please give a brief explanation and justification of this decision below.

16. What are the ethical issues connected with your research and what steps have you taken to address them? **Please do not answer 'none'.** We need to see evidence that you have identified potential ethical issues with respect to your research and have taken steps to address them. If applicable, please address:

- Participant burdens and/or risks

> 1. Privacy issues – participants are queried about personal information. We ensure participants' data will be kept anonymized, secure, not shared, and all information treated as highly confidential.
> 2. Use of direct quotes; participants' data will be pseudonymised and referenced by a code that is known to the researcher only.

- Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the University's and Social Science Division's Safety in Fieldwork guidance)

  1- The research does not cover political, religious, or any kind of sensitive topics that may lead to risky consequences to the researcher's safety and privacy. The researcher will explore the use of smart devices and it is effect on privacy in the smart homes.

  2- The research will be conducted online (e.g. Skype or Zoom), with no in-person interaction with the participants, which will minimise the health & safety risks for the researcher of being physically in a risky area or environment.

  3- To avoid any conflict with participants, or unwanted reactions:

  - We will inform participants that they may skip any question and choose not to answer, and it will be removed from the interview transcript.
  - We will inform participants that they can withdraw of the study at any point in time before the interviews.
  - We will inform participants that they can Withdraw within 4 weeks from the date the interview took place.

- Data protection/ confidentiality (also see Section 18).

  Confidentiality of collected data; precautions and safeguards to protect the collected data will be taken, and data will be securely anonymized and stored.

For more guidance on ethical issues, please see
http://researchsupport.admin.ox.ac.uk/governance/ethics/resources

*Discuss other ethical issues here*

| | | |
|---|---|---|
| 17. Will your research involve discussing sensitive issues?<br>This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities. | Yes ☐ | No ☒ |

| |
|---|
| *If you answered 'Yes', make sure you include some supporting information (as directed in Section 14 b.) above, showing the range of questions covering these issues.* |

| **18. Management and handling of personal and other research data** | |
|---|---|
| For the purpose of completing this section, all information provided by participants is considered **research data**. Any research data from which participants can be identified is known as *personal data*; any personal data which is sensitive is considered *special category data*.<br>Management of **personal data** and **special category data** of human participants, either directly or via a third party, must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. In answering the questions below, please also consider the points raised in the Data Protection Checklist. For advice on research data management and security, please consult with the University's Research Data Team (researchdata@ox.ac.uk) and/or your local IT department, and the University's web pages on research data management.<br><br>a.) **Please mark 'X' against the data you will collect for your research** | |
| Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name | ☒ |
| Online consent (may be anonymous) | ☒ |
| Opt-out forms | ☐ |
| Contact details for research purposes only (destroyed when no longer needed for this research) | ☒ |
| Contact details kept for future studies | ☒ |
| Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive) | ☒ |
| Video recordings | ☐ |
| Transcript of audio/video recordings | ☒ |
| Photographs | ☐ |
| Task results (e.g. paper/online tasks, diary completion) | ☒ |
| Questionnaire answers | ☐ |
| Field notes | ☐ |
| Other (please specify below) | ☐ |
| | |

| | | |
|---|---|---|
| b.) For **each** of the types of data selected above, state how this will be physically transferred from where it is collected to a local secure storage site (and backed up as necessary). This includes paper records and data captured electronically. | | |
| All data gathered as part of this research will be securely anonymized and stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Participants' Personal data will be destroyed as soon as it is no longer needed for the study. | | |
| c.) How and where will **each type of data** be stored during the research (until the end of all participant involvement)? Describe the arrangements for ensuring confidentiality, i.e. location of storage (e.g. Nexus 365 OneDrive for Business, SharePoint), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives. | | |
| All data gathered as part of this research will be securely anonymized and stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Participants' Personal data will be destroyed as soon as it is no longer needed for the study. | | |
| d.) Will you use a unique participant number on research data instead of a participant name?<br>If **yes,** state whether or not you will retain a list of participant names against numbers (i.e. pseudonymisation via a linkage list). Where will the list be stored, and when will it be destroyed? | | |
| We will use a unique ID code for each participant instead of the participant explicit name.<br><br>During the execution of the interviews, we will retain a list of participant names against codes. The list will be stored on the researcher's laptop only, and only the researcher can access it. That list will be permanently destroyed as soon as it is no longer needed for the study. | | |
| e.) Who will have access to the research data? | | |
| The researcher only. | | |
| f.) If research data is to be shared with another organisation, how will it be transferred / disclosed securely? | | |
| The research data will not be shared with another organization. | | |
| g.) When and how will identifiable data (including audio/video recordings & photos) be destroyed or deleted?<br>**Note:** Records of consent should be retained for a **minimum of three years after publication or public release**. Some funders may require longer periods (see http://www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies). If you wish to retain contact details in order to re-approach participants about future studies, you must detail this in information provided to them and obtain specific consent for this. | | |
| All identifiable data will be securely stored on Oxford Nexus 365 OneDrive.<br><br>The data will be destroyed after the stated periods according to data retention policies of the university. | | |
| h.) Please confirm that you will store **other research data** safely for at least 3 years after final publication or public release and adhere to any additional research funder policies. For more information about the University policies, please see the University's web pages on research data management. | Yes ☒ | No ☐ |

| If '**Yes'**, please give details of who will store the data and on storage format, location and security.<br>Note that open science is encouraged.<br>If **'No',** please provide further details below. | | |
|---|---|---|
| The data will be stored on secure servers controlled by the university of Oxford.<br><br>The stored data includes the fully pseudonymized transcripts with all other relevant information that could NOT be used to re-identify participants again.<br><br>In the beginning of the interviews, and before we start the recording, we will ask the interviewees not to mention their names, address, email address, phone number, workplace address, or any other information that may lead to identify them. If participants overshare information that may lead to identify them, we will remove it from the original recordings before we store them and before the transcription.<br><br>We will delete all recordings after we finish the transcriptions, as we will not need them after that stage.<br><br>We will make sure that the transcriptions are fully anonymized. | | |
| i.) Does your research involve the use of secondary (i.e. previously collected) data? Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally collected for other research purposes<br>(If "**No**", please go to section **19**.) | Yes ☐ | No ☒ |
| j.) Do you have data access agreements for the use of this secondary data? (If so, please attach these.) | Yes ☐ | No ☐ |
| k.) Is your use of this secondary data compatible with what data subjects/participants agreed that their data should be used for? | Yes ☐ | No ☐ |
| l.) Could this data be linked back to an individual or individuals?<br>If yes, address how securely any personally identifiable data will be transferred to you, and where and for how long it will be stored during or after the research. Who will have access to it? | Yes ☐ | No ☐ |

| **19. Publication and dissemination of research data** | |
|---|---|
| How will you disseminate and feedback project outcomes at the end of the research? | We will seek to publish the research study results in academic conferences and journals (e.g. SOUPS, CHI, CSCW, IJHCS).<br><br>The published papers will not include any kind of data that might lead to uncover participants' identities, or create any risks/threats for the participants (e.g. their privacy and safety). |

| **SECTION C: Methods and procedures to be used** | |
|---|---|
| **Method used:** Please ensure you have addressed any potential ethical issues related to these methods in Section 14 and in your Participant Information Sheet | **Please mark 'X'** |
| 1. Analysis of existing records | ☐ |
| 2. Snowball sampling (recruiting through contacts of existing participants) | ☒ |
| 3. Use of casual or local workers e.g. interpreters | ☐ |
| 4. Participant observation | ☐ |
| 5. Covert observation | ☐ |
| 6. Observation of specific organisational practices | ☐ |
| 7. Participant completes questionnaire in hard copy | ☐ |
| 8. Participant completes online questionnaire or other online task | ☐ |
| 9. Using social media | ☐ |
| 10. Participant performs paper and pencil task | ☐ |
| 11. Participant performs verbal or aural task (e.g. for linguistic study) | ☐ |
| 12. Focus group | ☐ |
| 13. Interview | ☒ |
| 14. Audio recording of participant (you will generally need specific consent from participants for this) | ☒ |
| 15. Video recording of participant (you will generally need specific consent from participants for this) | ☐ |
| 16. Photography of participant (you will generally need specific consent from participants for this) | ☐ |
| 17. Others (please specify below) | ☐ |
| | |

| **SECTION D: Professional guidelines and training** | | |
|---|---|---|
| 1. In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. **Note**: this is not an exhaustive list. | | **Please mark 'X'** |
| **Research specialism/ methodology** | **Association and guidance document** | |
| Anthropology | Association of Social Anthropologists of the UK and Commonwealth | ☐ |
| Criminology | http://www.britsoccrim.org/ethics/ | ☐ |
| Education | British Educational Research Association Ethical Guidelines for Educational Research | ☐ |
| Geography | Association of American Geographers Statement on Professional Ethics | ☐ |
| History | Oral History Society of the UK Ethical Guidelines | ☐ |
| Internet-based Research | British Psychological Society: Conducting Research on the Internet<br>Association of Internet Researchers Ethics Guide<br>Also see our Best Practice Guidance on internet-based research | ☐ |
| Law (Socio-Legal) | Socio-Legal Studies Association: Statement of Principles of Ethical Research | ☐ |
| Management | Academy of Management's Professional Code of Ethics | ☐ |
| Political Science | American Political Science Association (APSA) Guide to Professional Ethics in Political Science | ☐ |
| Politics | Political Studies Association. Guidelines for Good Professional Conduct | ☐ |
| Psychology | British Psychological Society Code of Ethics and Conduct | ☐ |
| Social Research | Social Research Association: Ethical Guidelines | ☒ |
| Sociology | The British Sociological Association: Statement of Ethical Practice | ☐ |
| Visual Research | ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research | ☐ |
| Other professional guidelines. Please specify the other guidelines used here*:* | | ☐ |
| | | |
| 2. Please indicate what training in research ethics (or research methodology) the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at http://researchsupport.admin.ox.ac.uk/support/training/ethics), or discussions between researchers and supervisors, if applicable. | | |
| I have taken a training course from the MPLS research training courses list: "Your successful DPhil".<br><br>The course has addressed ethics management during the research.<br><br>The course was taken in 24-Nov-2020. | | |

**SECTION E: Signatures or email endorsements (The SSH IDREC Secretariat accepts either option below. If you have a DREC, check which signature option it prefers.)**

- **Option 1:** Email confirmations from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities. **Pasted images of signatures cannot be accepted.**
- **Option 2:** Handwritten (wet-ink) signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email to us.

**Please ensure this checklist is signed by:**

| **For staff research**: | **For student research**: |
|---|---|
| 1. **Principal investigator** | 1. **Principal investigator (project supervisor)** |
| 2. **Head of Department (or nominee)** | 2. **Head of Department (or nominee)** |
| | 3. **Student researcher** |

1. **Principal Investigator signature/supervisor signature (if student research)**

I understand my responsibilities as **principal investigator** as outlined in the CUREC glossary and guidance on the CUREC website.

I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal investigator on this project and supply the name and contact details of my successor if appropriate.

**Signature** (or email endorsement using the above declaration): …this is for use by other departments. In Comp Sci we just ask for an email from the PI to ethics@cs.ox.ac.uk confirming they've seen and approved the application ……..

**Print name** (block capitals): ……IVAN FLECHAIS…….. **Date**: ……11-01-2021……..

2. **Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

(i) consider the principal investigator to be aware of her/his ethical responsibilities in regard to this research;
(ii) consider that any ethical issues raised have been satisfactorily resolved or are covered by relevant professional guidelines and/or CUREC approved procedures, and that it is appropriate for the research to proceed (noting the principal investigator's obligation to report should the design of the research change in a way which would alter any of the above responses so as to require completion of a CUREC 2 full application);
(iii) am satisfied that: the proposed project design and scientific methodology is sound; the project has been/will be subject to appropriate **peer review**; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the **public interest**.

**Signed by Head of Department or nominee** *(example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies)*:

**Signature** (or email endorsement using the above declaration): In Comp Sci the Ethics Committee organises this for you

**Print name** (block capitals): …….. **Date**: ……..

3. **Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal investigator properly authorised by the CUREC system.

**Signature by student** (or email endorsement using the above declaration): just email the application to ethics@cs.ox.ac.uk from your Oxford address.

**Print name** (block capitals): …WAEL ALBAYAYDH..... **Date**: …5-1-2021……..
...

## G.1.5 First Study - Information Sheet




**Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Researcher**
Wael Albayaydh
wael.albayaydh@cs.ox.ac.uk

**Exploring Bystanders' Privacy Concerns with the Smart Home in Jordan**

**PARTICIPANT INFORMATION SHEET**

Ethics Approval Reference: (CS_C1A_21_001)

1. ***What is the purpose of this study?***
   This research aims to provide insights into the privacy concerns of the bystanders' (domestic workers) in the smart home context. An understanding of which privacy concerns, both the primary and non-primary users might have with the smart homes, whether domestic workers are affecting the privacy of the families in the mart homes, or the smart devices in these smart homes are invading their privacy, and with which intended purpose are being carried out in the home is essential for our future research.

2. ***Why have I been invited to take part?***
   You have been invited to take part in this study as we aim to include people who are above 18 years old and are interested in understanding the effect smart home devices on their privacy.

3. ***Do I have to take part?***
   No. You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself and your data from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision. All your data will be erased from our records. Withdrawal is possible within 4 weeks from the date your interview took place.

   You can ask me to remove any particular information from my transcript, or you can withdraw from the study entirely. If you choose to withdraw, We will delete all transcripts, recordings and other data we hold about you. For the Voucher, you may keep it in case of withdrawal after the interview has taken place.

4. ***What will happen to me if I take part in the study?***
   If you are happy to take part in the study, you will be asked a number of questions about yourself, the household you are living in, activities in the home, and smart devices you use or deal with.
   This should take approximately 45 minutes, but not longer than one hour. The study will take place online only. The oral consent includes the option to withdraw of follow up enquiries we might have. If you wish to do so, just tell the researcher during taking the oral consent. You are invited to volunteer and take part in this study. While there is no compensation for your participation, your input will contribute to a deeper understanding of privacy concerns associated with smart devices, ultimately enhancing privacy protection for users in smart homes. With your consent, the interview will be recorded on audio. If you don't wish to be audio recorded, please inform the researcher. Audio recording is mandatory for the interviews. The

researcher will transcribe the interview to generate an anonymized data. However, neither the audio file nor the transcription made available to any other person than the researcher and principal investigator.

5. ***Are there any potential risks in taking part?***
   We collect information about yourself and your household. To guarantee appropriate data management we will fully anonymize this information and store it on an encrypted and password-protected hard drive within the University. We will apply appropriate safe-guards to protect your data.

6. ***Are there any benefits in taking part?***
   To thank you for your participation, you will receive an £10 Amazon voucher (or equivalent voucher)

7. ***What happens to the data provided?***
   The **research anonymized data** will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

   If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts.

   **Personal/sensitive data** will be stored separately and confidentially, only accessible to the researcher.

   All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

   Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

8. ***Will the research be published?***

   The research will be published as part of the RISCS research scheme. Future research papers might be published at academic conferences.

   The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

   If you agree to participate in this study, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published open access.

   Please visit https://www.oerc.ox.ac.uk/

9. ***Who is organising and funding the research?***
   This research is part of a DPhil thesis investigating privacy concerns of bystanders in smart homes

10. ***Who has reviewed this study?***
    This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: CS_C1A_21_001)

11. ***Who do I contact if I have a concern about the study or I wish to complain?***

If you have a concern about any aspect of this study please contact Mr. Wael Albayaydh (wael.albayaydh@cs.ox.ac.uk) or Ivan Flechais (Supervisor - ivan.flechais@cs.ox.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Computer Science Department Research Ethics Committee:
Email: ethics@cs.ox.ac.uk.
Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***12. Further Information and Contact Details***

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

**Researcher**
Wael Albayaydh,
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY
UK
Oxford email address: wael.albayaydh@cs.ox.ac.uk

# G.1.6 First Study - Consent Form

**Exploring Bystanders' Privacy Concerns with the Smart Home in Jordan**
Researcher: Wael Albayaydh
Document Version: 22/01/2021

**Participant Oral Consent Form**

CUREC Approval Reference: CS-C1A-21-001

**Exploring Bystanders' Privacy Concerns with the Smart Home in Jordan**

**Purpose of Study:**

This study aims to provide insights into the privacy concerns of the bystanders' (domestic workers) in the smart home context. An understanding of which privacy concerns, both the primary and non-primary users might have with the smart homes, whether domestic workers are affecting the privacy of the families in the mart homes, or the smart devices in these smart homes are invading their privacy, and with which intended purpose are being carried out in the home is essential for our future research.

**Consent Taking**

Record this consent process using a digital recorder (if the participant has consented to this) or by using a Record of Consent Form. PIN-protect the recorder if possible (particularly for sensitive data].

**1. Oral information giving to participants**

- ***Introduction* (*)***:* Hello, my name is Wael Albayaydh. I'm doing some research and I wondered if you'd be interested in being involved. I'm currently doing my DPhil Research at the University of Oxford in the Department of Computer Science. Can I tell you more about the study? *[Await confirmation].*
- ***Project details and aims:*** In my study, I want to investigate the Bystanders' Privacy Concerns with the Smart Home in the Middle East. I'm interested in meeting families that live in smart homes, and their domestic workers to talk about smart devices and their privacy concerns. If you choose to be a part of this project, here is what will happen:
- ***Interviews/surveys/ tasks description:*** I will have a conversation with you where I will ask a range of questions about smart devices and privacy.
- ***Data sharing/access/confidentiality:*** The data you give will form the basis of my DPhil research thesis. The research anonymized data will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

  If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts. Personal/sensitive data

will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

***Data storage:*** The collected data will be stored separately and confidentially on servers controlled by the university of Oxford, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit. All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

- ***Anonymity/pseudonyms/identifiable data:*** In any publications a fake name/ID number will be used (i.e. a pseudonym)/**or** your name and other identifying details will be anonymised by using a unique ID code for each participant, and we will ask the interviewees not to mention their names, address, email address, phone number, work place address, or any other information that may lead to identify them. If participants overshare information that may lead to identify them, we will remove it from the original recordings before we store them and before the transcription. We will delete all recordings after we finish the transcriptions, as we will not need them after that stage. We will make sure that the transcriptions are fully anonymized. / **or** you will be named (if you would like to be identified and if it is safe for you).
- ***Risks****:* There is no risks associated with the interviews, but to make sure that we eliminate any risks that may not be clear to us, we will anonymize the data to make sure there is no information that may lead to identifying participants personal IDs.
- ***Rights:*** You don't have to agree to take part; you can ask me any questions you want before or throughout; you can also withdraw at any stage without giving a reason before you do the interview, and you can withdraw within 4 weeks after the interview took place.
- ***Audio/video recording/photos/notes/keeping contact details:*** With your permission, I would like to make an audio recording of our discussion to make sure I'm getting an accurate record of your thoughts. I may want to re-contact you to clarify information you gave me in your interview.
- ***Publication plans:*** The project may/will be published in a(n) [thesis / dissertation/ academic journal/ academic book / academic website]. A copy of my [thesis / dissertation], will be deposited both in print and online in the University archives.[1]
- ***Complaints/concerns procedure:*** If you have any complaints or concerns please feel free to contact me in the first instance.

**Researcher:**
Wael Albayaydh,
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY
UK
Phone Number: +44 1865 283604

Oxford email address: wael.albayaydh@cs.ox.ac.uk

**Or the Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Or, the Chair, Computer Science Department Research Ethics Committee**

Email: ethics@cs.ox.ac.uk.

Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***Ethics review details:*** This research project has been reviewed and approved by an Oxford University ethics committee. Ethics Approval Reference: (CS_C1A_21_001). If, after contacting me with any concern, you're still unhappy and wish to make a formal complaint, please contact the ethics committee. Their email address ethics@cs.ox.ac.uk. Address: Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

- ***Data Protection statement****:* The University of Oxford is responsible overall for ensuring the safe and proper use of any personal information you provide, solely for research purposes. Further information about your rights to information you provide is available from the University's data protection web site (https://compliance.web.ox.ac.uk/individual-rights.
- ***Questions/concerns?*** Do you have any questions?

**2. Oral consent seeking stage, after participant has had sufficient time to think about whether s/he wants to take part. Record the participant response to below questions.**

- Do you give your permission for me to interview you and audio record you?
- Do you give permission for me to re-contact you to clarify information?
- Do you give me permission to quote you (using your pseudonym)?
- Are you happy to take part?

Ok, thanks, let's start.

## G.2 Second Study Ethics Application

### G.2.1 Second Study - Advertisement Poster

For the advertisement poster of the second study, please refer to Appendix C.1.

### G.2.2 Second Study - Survey Question Guidelines

For the survey question guidelines of the second study, please refer to Appendix C.2.

### G.2.3 Second Study - Interview Question Guidelines

For the interviews' questions guidelines of the second study, please refer to Appendix C.3, Appendix C.4, Appendix C.5, Appendix C.6.

# G.2.4 Second Study Ethics Application

**CENTRAL UNIVERSITY**
**RESEARCH ETHICS COMMITTEE (CUREC)**

**CUREC 1A Checklist**
**for the Social Sciences and Humanities**




The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

Please refer to Where and how to apply for ethical review and the CUREC flowchart first to see if you need ethics approval.

Please complete this form using a word processor and email it, together with your supporting documents, to your Departmental Research Ethics Committee (DREC) (if applicable). If you don't have a DREC please email this form to ethics@socsci.ox.ac.uk using your official ox.ac.uk email address. Only type-written, emailed applications will be accepted.

| **SECTION A: Filter for CUREC 2 application** | | |
|---|---|---|
| This section determines whether your study raises more complex issues requiring the completion of a full application for ethical review, known as the CUREC 2 application.<br>**(Please mark 'X' in the Yes/ No column.)** | | |
| 1. Are research participants classed as people whose ability to give free and informed consent is in question? (This may include under 18s (although see competent youths), prisoners, or adults at risk.) Your attention is drawn to the University's Safeguarding Code of Practice and its implications for researchers involving children or adults at risk. This includes the need for the work to be risk assessed and for researchers to undertake related training. (**Note**: If any of your participants are aged 16 or under, answer 'Yes' here **and** also answer question 5 below.) | Yes ☐ | No ☒ |
| 2. By taking part in the research, will participants be at risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)? | Yes ☐ | No ☒ |
| 3. Does the research involve the deception of participants? | Yes ☐ | No ☒ |
| 4. Does your research raise issues relevant to the Counter-Terrorism and Security Act (the Prevent duty), which seeks to prevent people from being drawn into terrorism? Please see advice on this on our Best Practice Guidance web page. | Yes ☐ | No ☒ |
| If you answered 'No' to **all** the questions above, go to **Section B**.<br>If you answered 'Yes' to **any** question above, continue to question 5 below. | | |
| 5. Is your project covered by a CUREC Approved Procedure (formerly known as "CUREC Protocols")? | Yes ☐ | No ☒ |
| If yes, give the specific Approved Procedure number(s): | | |
| If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **stop completing this checklist and do not submit it for ethical review**. Instead, complete the CUREC 2 application form from the CUREC website, then submit that for ethical review.<br>If you answered '**Yes'** to ANY of questions 1-3, **and** answered '**Yes'** to question 5, go on to **Section B**. | | |

| **SECTION B: Contact details and project description** | |
|---|---|
| **Contact details:** | |
| 1. Principal Investigator **or** supervisor (if student research) (give title and full name) | Prof. Ivan Flechais |
| 2. Name of student (if student research) | Wael Albayaydh |
| 3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil | DPhil |
| 4. Department or Institute name | Department of Computer Science |
| 5. Address for correspondence (if different from above) | Wael Albayaydh<br>St Hilda's College, Cowley Place<br>Oxford OX4 1DY<br>UK |
| 6. University (not private) e-mail address and telephone number | wael.albayaydh@cs.ox.ac.uk |
| 7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant) | |

| **Project description:** | |
|---|---|
| 8. Title of research project | Exploring Smart Home Power Dynamics and the Status of Data Protection in Jordan |
| 9. List of location(s) where project will be conducted | Jordan |
| 10. If your research involves overseas fieldwork or travel and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This must be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.) Please also address any physical or psychological risks for Oxford researchers and local fieldworkers in question 16 below and discuss with your Safety Officer. | Yes ☒<br>No ☐<br>Not required in this instance ☐ |
| 11. Anticipated duration of overall research project | months or 1 years (maximum 5)<br>4 years |
| 12. Anticipated start and end dates of the part of the research project involving human participants and/or personal data | From: 01/11/21)<br>To: (01/02/22) |

| | |
|---|---|
| | Note: You will need ethics approval before you start your research. CUREC 1As may take up to **30 days** to process. Retrospective ethics approval **cannot** be granted. |
| In the case of international or collaborative research, will you submit or have you submitted this project for ethical review or consideration elsewhere (e.g. collaborator's/ local ethics committee, or other local approval)? | Yes ☐<br>No ☒<br>If 'Yes', please attach ethics or other approvals and give more details below.<br>If 'No', please explain your reasons below.<br>Please also refer to the Best Practice Guidance on Ethical Review of social-sciences based research conducted outside the UK (BPG 16), which includes an Ethics Issues Checklist for International Research (Appendix A) |
| Please supply further details in response to question 12b here.<br><br>I am not cooperating with local institutions in Jordan.<br>Reference the Best Practice Guidance 10_Version 1.0, we will follow it strictly<br>We will assure participants that the data collected will be managed with strict confidentiality, we will destroy it after we finish the analysis, we will avoid questions that might be sensitive or may create risks for both the researcher and the participants. We will inform participants that they can skip any question they do not wish to answer | |
| 13. External organisation funding the research (if applicable) | |
| 14. Brief description of research (about 150 words) in lay language.<br>a) When describing the research, include your methodology, how you are applying professional guidelines, and the use to which results/ data will be put. Please also declare any conflicts of interest here. | |
| Title: " Exploring Bystanders' Privacy Concerns with the Smart Home in Jordan"<br><br>This work is the second project of my DPhil research study which aims to understand Smart Home Power Dynamics and the Status of Data Protection in Jordan. We will conduct interviews with participants from Jordan who have relevant knowledge about privacy protection regulations such as experts in data protection regulations and policies, officials from labour organizations, officials from workers professional associations, privacy protection activists, human rights activists, lawyers, smart home device users (families and domestic workers) to explore current status of privacy protection in the smart home, the potential future privacy protection regulations in Jordan, and the effect of asymmetric power dynamics on domestic workers' agency and privacy concerns and practices in the smart home. Also, we will explore how can we leverage contextual influences and awareness about smart devices to support privacy protection in the smart homes in Jordan.<br><br>We will conduct semi-structured interviews. The interviews will be conducted online (e.g. skype, or zoom). The interviews will not start before the the participant's consent to be interviewed, to be audio recorded, and to give us his feedback.<br><br>Up to my knowledge, there is no conflict of interest associated with executing this reseach. | |
| b) Description of participants and how you will obtain informed consent to take part in the research. | |
| i. Description of participants and your criteria for inclusion/ exclusion. | |

Participants include individuals (over 18)). Children will not be included.

Interviews are conducted in Jordan, and hence participation is geographically limited. Because of the current pandemic (i.e. COVID-19), Teams/Skype/Zoom will be used to interview participants online as per their choice.

ii. Your method(s) of recruitment.

For the participants from private and public sectors (e.g., regulatory, labour organizations, and workers professional associations) we will contact these companies, organizations and associations directly to recruit participants after we explain the research plan and the objectives of this research. We will use snowball sampling as well.

Participants may be pre-screened before they are allowed participation in the study. Pre-screening follows initial email to the participant and is done using online survey. Participants will be registered with a unique ID which only the researcher can link to a name. Information on the pre-screening data will be a subset of the demographics questionnaire survey.The survey will at no point ask to provide the email address, the IP address , or the participant's name nor will this information be recorded online by other means known to the researcher.

Independent of the recruitment, consent for participation will be sought from individuals directly at the beginning of each interview.

To thank the participants for thier participation, they will receive a simple gift equivalent to £10 in local currency).

| | |
|---|---|
| iii. Your processes for obtaining informed consent from participants. | |
| At the beginning of each interview an oral consent wil be sought from all participants. An information sheet explaining the purpose of the study and intended usage of data (see attachement) will be presented alongside the consent form (in person or via email). The information sheet will be provided to the participants at least 24h in advance to their participation.<br>For interviews via Skype the consent form is either signed electronically (by typing initials) and emailed back to the researcher as the first step during the interview (see attached form), or by providing oral consent that the researcher will record in the beginning of each onterview. | |
| Please attach separate supporting documents (in Word), if appropriate, for your research (English language versions only). Tick those you are submitting below. If appropriate supporting documents are not submitted, you will be asked to provide these separately, which may delay the ethical review process. | |
| Recruitment and advertisement material (e.g. a poster, social media recruitment text, or brief invitation letter/ email). | ☒ |
| Information for participants to read (or hear) before they agree to take part (e.g. written information or, if applicable, an outline oral information script). | ☒ |
| A document to record informed consent. Templates for written consent forms and/ or oral information scripts (in case of an oral consent process) are available from the CUREC website. | ☒ |
| Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire). | ☒ |
| (If applicable) debriefing document after participants have taken part. | ☐ |
| Please add any further details. If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants Please answer question 15 if you cannot obtain informed consent. | |
| No further details to be added. | |
| 15. If you cannot obtain informed consent from participants according to CUREC guidelines and good practice in your discipline, please give a brief explanation and justification of this decision below. | |
| | |
| 16. What are the ethical issues connected with your research and what steps have you taken to address them? Please do not answer 'none'. We need to see that you have identified potential ethical issues with respect to your research and have taken steps to address them. If applicable, please address: | |
| a) Participant burdens and/or risks | |
| 1. Privacy issues. We ensure participants that their data will be kept secure, not shared, and all information treated as highly confidential.<br>2. Use of direct quotes; participant's data will be anonymised and only identified by a code that is known to the researcher only.<br>3. Each participant will have a unique code that is known to the research team only. | |

b) Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the University's and Social Science Division's Safety in Fieldwork guidance)

1- The research does not cover political, religious, or any kind of sensitive topics that may lead to risky consequences to the researcher's safety and privacy. The researcher will explore the use of smart devices and it is effect on privacy protection in the smart homes.

2- The research will be conducted online (e.g. Skype or Zoom), with no physical interaction with the participants, which will minimise the health & safety risks for the researcher of being physically in a risky area or environment.

3- To avoid any conflict with participants, or unwanted reactions:

- We will inform participants that they may skip any question and not to answer it, and it will be removed from the interview transcript.
- We will inform participants that they can withdraw of the study at any point in time in which case all their records will be erased.

c) Data protection/ confidentiality (also see Section 18).

Confidentiality of collected data; precautions and safeguards to protect the collected data will be taken, and data will be securely stored on the university of Oxford servers and/or the researcher PC.

Any other ethical issues. For more guidance on ethical issues, please see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources

| 17. Will your research involve discussing sensitive issues? This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/ mental health, trade union membership, sexual life or criminal activities. If you answered 'Yes', make sure you include some supporting information (as directed in **section 14b** above, showing the range of questions covering these issues. | Yes ☐ | No ☒ |
|---|---|---|

Please provide further details:

**18. Management and handling of personal and other research data**

All information provided by participants is considered research data for the purpose of this form. Any research data from which participants can be identified is known as personal data; any personal data which is sensitive is considered special category data.

Management of personal data, either directly or via a third party, must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. In answering the questions below, please also consider the points raised in the Data Protection Checklist and whether, for higher-risk data processing, a separate Data Protection Impact Assessment (DPIA) may also be required for the research. Advice on research data management and security is

| | |
|---|---|
| available from Research Data Oxford and your local IT department. Advice on data protection is available from information.compliance@admin.ox.ac.uk.<br><br>a) Please mark 'X' against the data you will collect for your research | |
| Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name) | ☒ |
| Online consent (may be anonymous) | ☒ |
| Opt-out forms | ☒ |
| Contact details for research purposes only (destroyed when no longer needed for this research) | ☒ |
| Contact details kept for future studies | ☒ |
| Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive) | ☒ |
| Video recordings | ☐ |
| Transcript of audio/ video recordings | ☒ |
| Photographs | ☐ |
| Task results (e.g. paper/ online tasks, diary completion) | ☒ |
| Questionnaire answers | ☐ |
| Field notes | ☒ |
| Other (please specify below) | ☐ |
| | |
| b) For each of the types of data selected above, state how this will be physically transferred from where it is collected to a local secure storage site (and backed up as necessary). This includes paper records and data captured electronically. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| c) How and where will each type of data be stored during the research (until the end of all participant involvement)? Describe the arrangements for ensuring confidentiality, i.e. location of storage (e.g. Nexus 365 OneDrive for Business, SharePoint), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| d) Will you use a unique participant number on research data instead of a participant name? If yes, state whether or not you will retain a list of participant names against numbers (i.e. pseudonymisation via a linkage list). Where will the list be stored, and when will it be destroyed? | |

| | | |
|---|---|---|
| We will use a unique code number for each participant instead of the participant explicit name.<br><br>During the execution of the interviews, we will retain a list of participant names against codes. The list will be stored on Oxford Nexus 365 OneDrive. That list will be permanently destroyed as soon as it is no longer needed for the study. | | |
| e) Who will have access to the research data? | | |
| The researcher only. | | |
| f) If research data is to be shared with another organisation, how will it be transferred/ disclosed securely? | | |
| The research data will not be shared with another organization. | | |
| g) When and how will identifiable data (including audio/ video recordings & photos) be destroyed or deleted?<br>Note: Records of consent should be retained for a minimum of three years after publication or public release. Some funders may require longer periods. If you wish to retain contact details in order to re-approach participants about future studies, you must detail this in information provided to them and obtain specific consent for this. | | |
| All identifiable data will be securely stored on Oxford Nexus 365 OneDrive.<br><br>The data will be destroyed after the stated periods according to data retention policies of the university. | | |
| h) Please confirm that you will store other research data safely for at least 3 years after final publication or public release and adhere to any additional research funder policies. For more information about the University policies, please see the University's web pages on research data management. | Yes ☒ | No ☐ |
| If 'Yes', please give details of who will store the data and on storage format, location and security. Note that open science is encouraged.<br>If 'No', please provide further details below. | | |
| The data will be stored on the Open Science framework.<br><br>The stored data includes the fully pseudonymized transcripts with all other relevant information that could NOT be used to re-identify participants again | | |
| i) Does your research involve the use of secondary (i.e. previously collected) data? Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally collected for other research purposes. (If "No", please go to question 19.) | Yes ☐ | No ☒ |
| j) Do you have data access agreements for the use of this secondary data?<br>(If so, please attach these.) | Yes ☐ | No ☐ |

| | | |
|---|---|---|
| k) Is your use of this secondary data compatible with what the data subjects/ participants agreed that their data should be used for? | Yes ☐ | No ☐ |
| l) Could this data be linked back to an individual or individuals? If yes, address how securely any personally identifiable data will be transferred to you, and where and for how long it will be stored during or after the research. Who will have access to it? | Yes ☐ | No ☐ |
| | | |

| 19. Publication and dissemination of research data and outputs.<br>How will you disseminate and feedback project outcomes at the end of the research? |
|---|
| We will seek to publish the research study results in academic conferences and journals (e.g. SOUPS, CHI, CSCW, IJHCS).<br><br>The published papers will not include any kind of data that might lead to uncover participants' identities, or create any risks/threats for the participants (e.g. their privacy and safety). |

| **SECTION C: Methods and procedures to be used** | |
|---|---|
| 1. Please indicate the methods to be used: | **Mark 'X'** |
| a) Analysis of existing records | ☐ |
| b) Snowball sampling (recruiting through contacts of existing participants) | ☒ |
| c) Use of casual or local workers e.g. interpreters | ☐ |
| d) Participant observation | ☐ |
| e) Covert observation | ☐ |
| f) Observation of specific organisational practices | ☐ |
| g) Participant completes questionnaire in hard copy | ☐ |
| h) Participant completes online questionnaire or other online task | ☐ |
| i) Using social media | ☐ |
| j) Participant performs paper and pencil task | ☐ |
| k) Participant performs verbal or aural task (e.g. for linguistic study) | ☐ |
| l) Focus group | ☐ |
| m) Interview | ☒ |
| n) Audio recording of participant (you will generally need specific consent from participants for this) | ☒ |
| o) Video recording of participant (you will generally need specific consent from participants for this) | ☐ |
| p) Photography of participant (you will generally need specific consent from participants for this) | ☐ |
| q) Others (please specify below) | ☐ |

| Please ensure you have addressed any potential ethical issues related to these methods in question B14 and in your Participant Information Sheet. |
| --- |
| I have taken two training courses from the MPLS research training courses list: “Your successful DPhil”, and the “Research Integrity”<br><br>The two courses had explained in depth the research ethics management.<br><br>The first course was taken in 24-Nov-2020, and the second course was taken in 25-July-2021. |

**SECTION D: Professional guidelines and training**

In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. This is not an exhaustive list.

| **Research specialism/ methodology** | **Association and guidance document** | **Please mark 'X'** |
|---|---|---|
| Anthropology | Association of Social Anthropologists of the UK and Commonwealth | ☐ |
| Computer Sciences | ACM Code of Ethics and Professional Conduct | ☐ |
| Criminology | British Society of Criminology | ☐ |
| Education | British Educational Research Association Ethical Guidelines for Educational Research | ☐ |
| Geography | Association of American Geographers Statement on Professional Ethics | ☐ |
| History | Oral History Society of the UK Ethical Guidelines | ☐ |
| Internet-based Research | British Psychological Society: Conducting Research on the Internet<br>Association of Internet Researchers Ethics Guide<br>ACM Code of Ethics and Professional Conduct<br>Association of Internet Researchers (AoIR)<br>Also see CUREC's Best Practice Guidance on internet-based research | ☐ |
| Law (Socio-Legal) | Socio-Legal Studies Association: Statement of Principles of Ethical Research | ☐ |
| Management | Academy of Management's Professional Code of Ethics | ☐ |
| Political Science | American Political Science Association (APSA) Guide to Professional Ethics in Political Science | ☐ |
| Politics | Political Studies Association. Guidelines for Good Professional Conduct | ☐ |
| Psychology | British Psychological Society Code of Ethics and Conduct | ☐ |
| Social Research | Social Research Association: Ethical Guidelines | ☒ |
| Sociology | The British Sociological Association: Statement of Ethical Practice | ☐ |
| Visual Research | ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research | ☐ |
| Other professional guidelines. Please specify the other guidelines used here: | | ☐ |

Please indicate what training in research ethics (or research methodology) the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at http://researchsupport.admin.ox.ac.uk/support/training/ethics), or discussions between researchers and supervisors, if applicable.

**SECTION E: Signatures or email endorsements**

The SSH IDREC Secretariat accepts either option below. If you have a DREC, check which option it prefers.
**Option 1**: Email confirmation from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities. Pasted images of signatures cannot be accepted.
**Option 2**: Handwritten signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email to us.

Please ensure this checklist is signed by:

**For staff research**:
1. Principal Investigator
2. Head of Department (or nominee)

**For student research**:
1. Principal Investigator (project supervisor)
2. Head of Department (or nominee)
3. Student researcher

**Principal Investigator signature/ supervisor signature (if student research)**

I understand my responsibilities as Principal Investigator as outlined in the CUREC glossary and guidance on the CUREC website. I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal investigator on this project and supply the name and contact details of my successor if appropriate.

**Signature** (or email endorsement using the above declaration): _____

**Print name**: _IVAN FLECHAIS_____ **Date**: ____12-10-2021_____

**Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

- consider the PI and student researcher (if applicable) to be aware of their ethical responsibilities in regard to the ethical issues associated with this research;
- am satisfied that: the proposed project design and scientific methodology are sound; the project has been subject to appropriate peer review; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the public interest.

Signed by Head of Department or nominee (example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies):

**Signature** (or email endorsement using the above declaration): _____

**Print name**: _____ **Date**: _____

**Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal investigator properly authorised by the CUREC system.

**Signature by student** (or email endorsement using the above declaration):



Wael.albayaydh@cs.ox.ac.uk

**Print** name: WAEL ALBAYAYDH _____ **Date**: _5-10-2021_____

## G.2.5 Second Study Information Sheet




DEPARTMENT OF
COMPUTER
SCIENCE

**Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Researcher**
Wael Albayaydh, DPhil student
wael.albayaydh@cs.ox.ac.uk

**Exploring Smart Hone Power Dynamics and Data Protection in Jordan**

**PARTICIPANT INFORMATION SHEET**

Ethics Approval Reference: (CS_C1A_021_038)

1. ***What is the purpose of this study?***
   This research aims to provide insights about smart home power dynamics, and the status of privacy protection in the smart home in Jordan. An understanding of how power dynamics inter-play between users on the smart home, how smart devices affect these dynamics, and about the privacy protection of both the primary and non-primary users in the smart homes, and whether domestic workers are affecting the privacy of the families in the mart homes and how to mitigate that effect, or how to protect both families and domestic workers from the smart devices in the smart homes that are invading their privacy.

2. ***Why have I been invited to take part?***
   You have been invited to take part in this study as we aim to include people who are above 18 years old and are interested in sharing their insights and experience about users relations in the smart home and the protection of users data and privacy in the smart home.

3. ***Do I have to take part?***
   No. You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself and your data from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision. All your data will be erased from our records. Withdrawal is possible within 4 weeks from the date your interview or focus group took place.

4. ***What will happen to me if I take part in the study?***
   If you are happy to take part in the study, you will be asked a number of questions about yourself, the smart devices, your insights and experience and experience about data and privacy protection, and how we can improve privacy protection. This should take approximately 45 minutes, but not longer than one hour. The study will take place online or at a public location convenient for you. The consent letter includes the option to withdraw of follow up enquiries we might have. If you wish to do so, please check the respective box, or you may just mention it if you are providing an oral consent. You are invited to volunteer and take part in this study. While there is no compensation for your participation, your input will contribute to a deeper understanding of privacy concerns associated with smart devices, ultimately enhancing privacy protection for users in smart homes. With your consent, the interview will be recorded on audio. If you don't wish to be audio recorded, please inform the researcher. Audio recording is mandatory for the interviews. The researcher will transcribe the interview. However, neither the audio file nor the

transcription made available to any other person than the researcher and the principal investigator. The Audio recordings will be destroyed after transcribing them into text files.

5. ***Are there any potential risks in taking part?***
We collect information about yourself and your household. To guarantee appropriate data management we will fully anonymize this information and store it on an encrypted and password-protected hard drive within the University. We will apply appropriate safe-guards to protect your data.

6. ***Are there any benefits in taking part?***
You will receive any compensation for your time. But the information you will give us will support better building better smart devices to improve protection of uses' data in smart homes and specifically in context similar to the Jordanian context.

7. ***What happens to the data provided?***
The **research data** will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and the principal investigator.

**Personal/sensitive data** will be stored separately and confidentially, only accessible to the researcher.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

8. ***Will the research be published?***

The research will be published as part of the RISCS research scheme. Future research papers might be published at academic conferences.

The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

If you agree to participate in this study, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published open access.

9. ***Who is organising the research?***
This research is part of a DPhil thesis investigating privacy concerns of bystanders in smart homes.

10. ***Who has reviewed this study?***
***After the approval of CUREC***
This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: **CS_C1A_021_038)**

11. ***Who do I contact if I have a concern about the study or I wish to complain?***

If you have a concern about any aspect of this study please contact Mr. Wael Albayaydh (wael.albayaydh@cs.ox.ac.uk) or Ivan Flechais (Supervisor - ivan.flechais@cs.ox.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal

complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, **Social Sciences & Humanities Interdivisional Research Ethics Committee**; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD

***12. Further Information and Contact Details***

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

**Researcher**
Wael Albayaydh, DPhil student
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY
UK
Oxford email address: wael.albayaydh@cs.ox.ac.uk

## G.2.6 Second Study Consent Form

**Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households**
Researcher: Wael Albayaydh
Document Version: 05/10/2021

**Participant Oral Consent Form**

CUREC Approval Reference: CS_C1A_021_038

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

**Purpose of Study:**

This study aims to provide insights about smart home power dynamics, and the status of privacy protection in the smart home in Jordan. An understanding of how power dynamics inter-play between users on the smart home, how smart devices affect these dynamics, and about the privacy protection of both the primary and non-primary users in the smart homes, and whether domestic workers are affecting the privacy of the families in the mart homes and how to mitigate that effect, or how to protect both families and domestic workers from the smart devices in the smart homes that are invading their privacy.

**Consent Taking**

Record this consent process using a digital recorder (if the participant has consented to this) or by using a Record of Consent Form. PIN-protect the recorder if possible (particularly for sensitive data].

**1. Oral information giving to participants**

- ***Introduction* (*)***:* Hello, my name is Wael Albayaydh. I'm doing some research and I wondered if you'd be interested in being involved. I'm currently doing my DPhil Research at the University of Oxford in the Department of Computer Science. Can I tell you more about the study? *[Await confirmation].*
- ***Project details and aims:*** In my study, I want to investigate the Bystanders' Privacy Concerns with the Smart Home in the Middle East. I'm interested in meeting families that live in smart homes, and their domestic workers to talk about smart devices and their privacy concerns. If you choose to be a part of this project, here is what will happen:
- ***Interviews/surveys/ tasks description:*** I will have a conversation with you where I will ask a range of questions about smart devices and privacy.
- ***Data sharing/access/confidentiality:*** The data you give will form the basis of my DPhil research thesis. The research anonymized data will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts. Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

***Data storage:*** The collected data will be stored separately and confidentially on servers controlled by the university of Oxford, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit. All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

- ***Anonymity/pseudonyms/identifiable data:*** In any publications a fake name/ID number will be used (i.e. a pseudonym)/**or** your name and other identifying details will be anonymised by using a unique ID code for each participant, and we will ask the interviewees not to mention their names, address, email address, phone number, work place address, or any other information that may lead to identify them. If participants overshare information that may lead to identify them, we will remove it from the original recordings before we store them and before the transcription. We will delete all recordings after we finish the transcriptions, as we will not need them after that stage. We will make sure that the transcriptions are fully anonymized. / **or** you will be named (if you would like to be identified and if it is safe for you).
- ***Risks****:* There is no risks associated with the interviews, but to make sure that we eliminate any risks that may not be clear to us, we will anonymize the data to make sure there is no information that may lead to identifying participants personal IDs.
- ***Rights:*** You don't have to agree to take part; you can ask me any questions you want before or throughout; you can also withdraw at any stage without giving a reason before you do the interview, and you can withdraw within 4 weeks after the interview took place.
- ***Audio/video recording/photos/notes/keeping contact details:*** With your permission, I would like to make an audio recording of our discussion to make sure I'm getting an accurate record of your thoughts. I may want to re-contact you to clarify information you gave me in your interview.
- ***Publication plans:*** The project may/will be published in a(n) [thesis / dissertation/ academic journal/ academic book / academic website]. A copy of my [thesis / dissertation], will be deposited both in print and online in the University archives.[1]
- ***Complaints/concerns procedure:*** If you have any complaints or concerns please feel free to contact me in the first instance.

**Researcher:**
Wael Albayaydh,
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY

UK
Phone Number: +44 1865 283604
Oxford email address: wael.albayaydh@cs.ox.ac.uk

**Or the Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Or, the Chair, Computer Science Department Research Ethics Committee**

Email: ethics@cs.ox.ac.uk.

Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***Ethics review details:*** This research project has been reviewed and approved by an Oxford University ethics committee. Ethics Approval Reference: (CS_C1A_021_038). If, after contacting me with any concern, you're still unhappy and wish to make a formal complaint, please contact the ethics committee. Their email address ethics@cs.ox.ac.uk. Address: Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

- ***Data Protection statement****:* The University of Oxford is responsible overall for ensuring the safe and proper use of any personal information you provide, solely for research purposes. Further information about your rights to information you provide is available from the University's data protection web site (https://compliance.web.ox.ac.uk/individual-rights.
- ***Questions/concerns?*** Do you have any questions?

**2. Oral consent seeking stage, after participant has had sufficient time to think about whether s/he wants to take part. Record the participant response to below questions.**

- Do you give your permission for me to interview you and audio record you?
- Do you give permission for me to re-contact you to clarify information?
- Do you give me permission to quote you (using your pseudonym)?
- Are you happy to take part?

Ok, thanks, let's start.

## G.3 Third Study Ethics Application

### G.3.1 Third Study - Advertisement Poster

For the advertisement poster of the third study, please refer to Appendix D.1, Appendix D.2, and Appendix D.3.

### G.3.2 Third Study - Survey Question Guidelines

For the survey question guidelines of the third study, please refer to Appendix D.4.

### G.3.3 Third Study - Interview Question Guidelines

For the interviews' questions guidelines of the third study, please refer to Appendix D.5, Appendix D.6, Appendix D.7, Appendix D.8, Appendix D.9.

# G.3.4 Third Study Ethics Application

**CENTRAL UNIVERSITY**
**RESEARCH ETHICS COMMITTEE (CUREC)**

**CUREC 1A Checklist**
**for the Social Sciences and Humanities**




The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

Please refer to Where and how to apply for ethical review and the CUREC flowchart first to see if you need ethics approval.

Please complete this form using a word processor and email it, together with your supporting documents, to your Departmental Research Ethics Committee (DREC) (if applicable). If you don't have a DREC please email this form to ethics@socsci.ox.ac.uk using your official ox.ac.uk email address. Only type-written, emailed applications will be accepted.

| **SECTION A: Filter for CUREC 2 application** | | |
|---|---|---|
| This section determines whether your study raises more complex issues requiring the completion of a full application for ethical review, known as the CUREC 2 application.<br>**(Please mark 'X' in the Yes/ No column.)** | | |
| 1. Are research participants classed as people whose ability to give free and informed consent is in question? (This may include under 18s (although see competent youths), prisoners, or adults at risk.) Your attention is drawn to the University's Safeguarding Code of Practice and its implications for researchers involving children or adults at risk. This includes the need for the work to be risk assessed and for researchers to undertake related training. (**Note**: If any of your participants are aged 16 or under, answer 'Yes' here **and** also answer question 5 below.) | Yes ☐ | No ☒ |
| 2. By taking part in the research, will participants be at risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)? | Yes ☐ | No ☒ |
| 3. Does the research involve the deception of participants? | Yes ☐ | No ☒ |
| 4. Does your research raise issues relevant to the Counter-Terrorism and Security Act (the Prevent duty), which seeks to prevent people from being drawn into terrorism? Please see advice on this on our Best Practice Guidance web page. | Yes ☐ | No ☒ |
| If you answered 'No' to **all** the questions above, go to **Section B**.<br>If you answered 'Yes' to **any** question above, continue to question 5 below. | | |
| 5. Is your project covered by a CUREC Approved Procedure (formerly known as "CUREC Protocols")? | Yes ☐ | No ☒ |
| If yes, give the specific Approved Procedure number(s): | | |
| If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **stop completing this checklist and do not submit it for ethical review**. Instead, complete the CUREC 2 application form from the CUREC website, then submit that for ethical review.<br>If you answered '**Yes'** to ANY of questions 1-3, **and** answered '**Yes'** to question 5, go on to **Section B**. | | |

| **SECTION B: Contact details and project description** | |
|---|---|
| **Contact details:** | |
| 1. Principal Investigator **or** supervisor (if student research) (give title and full name) | Prof. Ivan Flechais |
| 2. Name of student (if student research) | Wael Albayaydh |
| 3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil | DPhil |
| 4. Department or Institute name | Department of Computer Science |
| 5. Address for correspondence (if different from above) | Wael Albayaydh<br>St Hilda's College, Cowley Place<br>Oxford OX4 1DY<br>UK |
| 6. University (not private) e-mail address and telephone number | wael.albayaydh@cs.ox.ac.uk |
| 7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant) | |

| **Project description:** | |
|---|---|
| 8. Title of research project | Exploring Privacy Protection Means<br>Smart Home |
| 9. List of location(s) where project will be conducted | Jordan |
| 10. If your research involves overseas fieldwork or travel and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This must be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.) Please also address any physical or psychological risks for Oxford researchers and local fieldworkers in question 16 below and discuss with your Safety Officer. | Yes ☒<br>No ☐<br>Not required in this instance ☐ |
| 11. Anticipated duration of overall research project | months or 1 years (maximum 5)<br>4 years |
| 12. Anticipated start and end dates of the part of the research project involving human participants and/or personal data | From: 01/04/22)<br>To: (30/04/22) |

| | |
|---|---|
| | Note: You will need ethics approval before you start your research. CUREC 1As may take up to **30 days** to process. Retrospective ethics approval **cannot** be granted. |
| In the case of international or collaborative research, will you submit or have you submitted this project for ethical review or consideration elsewhere (e.g. collaborator's/ local ethics committee, or other local approval)? | Yes ☐<br>No ☒<br>If 'Yes', please attach ethics or other approvals and give more details below.<br>If 'No', please explain your reasons below.<br>Please also refer to the Best Practice Guidance on Ethical Review of social-sciences based research conducted outside the UK (BPG 16), which includes an Ethics Issues Checklist for International Research (Appendix A) |
| Please supply further details in response to question 12b here.<br><br>I am not cooperating with local institutions in Jordan.<br>Reference the Best Practice Guidance 10_Version 1.0, we will follow it strictly<br>We will assure participants that the data collected will be managed with strict confidentiality, we will destroy it after we finish the analysis, we will avoid questions that might be sensitive or may create risks for both the researcher and the participants. We will inform participants that they can skip any question they do not wish to answer | |
| 13. External organisation funding the research (if applicable) | |
| 14. Brief description of research (about 150 words) in lay language.<br>a) When describing the research, include your methodology, how you are applying professional guidelines, and the use to which results/ data will be put. Please also declare any conflicts of interest here. | |
| Title: "Exploring Privacy Protection Means in the Smart Homes"<br><br>This work is the third project of my DPhil research study which aims to explore Privacy Protection Means in the Smart Home. We will conduct interviews with participants from Jordan who have relevant knowledge about privacy protection regulations such as experts in data protection regulations and policies public awareness experts, and smart device designers to explore the potential privacy protection means in the smart home, and how we can orchestrate the regulations, awareness abd the design of the devices to ensure protection of users privacy.<br>We will conduct semi-structured interviews. The interviews will be conducted online (e.g. skype, or zoom). The interviews will not start before the the participant's consent to be interviewed, to be audio recorded, and to give us his feedback.<br><br>Up to my knowledge, there is no conflict of interest associated with executing this reseach. | |
| b) Description of participants and how you will obtain informed consent to take part in the research.<br>i. Description of participants and your criteria for inclusion/ exclusion. | |
| Participants include individuals (over 18)). Children will not be included.<br><br>Interviews are conducted in Jordan, and hence participation is geographically limited. Because of the current pandemic (i.e. COVID-19), Teams/Skype/Zoom will be used to interview participants online as per their choice. | |

| ii. Your method(s) of recruitment. |
| --- |
| For the participants from private and public sectors (e.g., regulatory, labour organizations, and workers professional associations) we will contact these companies, organizations and associations directly to recruit participants after we explain the research plan and the objectives of this research. We will use snowball sampling as well. We will do the same to recruite smart devoce designers and awareness expers, and that will be by contafting their organizations, and then we will use snowball sampling to recruite more participants.<br><br>Participants may be pre-screened before they are allowed participation in the study. Pre-screening follows initial email to the participant and is done using online survey. Participants will be registered with a unique ID which only the researcher can link to a name. Information on the pre-screening data will be a subset of the demographics questionnaire survey.The survey will at no point ask to provide the email address, the IP address , or the participant's name nor will this information be recorded online by other means known to the researcher.<br><br>Independent of the recruitment, consent for participation will be sought from individuals directly at the beginning of each interview.<br><br>To thank the participants for thier participation, they will receive a simple gift equivalent to £10 in local currency). |

| | |
|---|---|
| iii. Your processes for obtaining informed consent from participants. | |
| At the beginning of each interview an oral consent wil be sought from all participants. An information sheet explaining the purpose of the study and intended usage of data (see attachement) will be presented alongside the consent form (in person or via email). The information sheet will be provided to the participants at least 24h in advance to their participation.<br>For interviews via Skype the consent form is either signed electronically (by typing initials) and emailed back to the researcher as the first step during the interview (see attached form), or by providing oral consent that the researcher will record in the beginning of each onterview. | |
| Please attach separate supporting documents (in Word), if appropriate, for your research (English language versions only). Tick those you are submitting below. If appropriate supporting documents are not submitted, you will be asked to provide these separately, which may delay the ethical review process. | |
| Recruitment and advertisement material (e.g. a poster, social media recruitment text, or brief invitation letter/ email). | ☒ |
| Information for participants to read (or hear) before they agree to take part (e.g. written information or, if applicable, an outline oral information script). | ☒ |
| A document to record informed consent. Templates for written consent forms and/ or oral information scripts (in case of an oral consent process) are available from the CUREC website. | ☒ |
| Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire). | ☒ |
| (If applicable) debriefing document after participants have taken part. | ☐ |
| Please add any further details. If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants Please answer question 15 if you cannot obtain informed consent. | |
| No further details to be added. | |
| 15. If you cannot obtain informed consent from participants according to CUREC guidelines and good practice in your discipline, please give a brief explanation and justification of this decision below. | |
| | |
| 16. What are the ethical issues connected with your research and what steps have you taken to address them? Please do not answer 'none'. We need to see that you have identified potential ethical issues with respect to your research and have taken steps to address them. If applicable, please address: | |
| a) Participant burdens and/or risks | |
| 1. Privacy issues. We ensure participants that their data will be kept secure, not shared, and all information treated as highly confidential.<br>2. Use of direct quotes; participant's data will be anonymised and only identified by a code that is known to the researcher only.<br>3. Each participant will have a unique code that is known to the research team only. | |

b) Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the University's and Social Science Division's Safety in Fieldwork guidance)

1- The research does not cover political, religious, or any kind of sensitive topics that may lead to risky consequences to the researcher's safety and privacy. The researcher will explore the use of smart devices and it is effect on privacy protection in the smart homes.

2- The research will be conducted online (e.g. Skype or Zoom), with no physical interaction with the participants, which will minimise the health & safety risks for the researcher of being physically in a risky area or environment.

3- To avoid any conflict with participants, or unwanted reactions:

- We will inform participants that they may skip any question and not to answer it, and it will be removed from the interview transcript.
- We will inform participants that they can withdraw of the study at any point in time in which case all their records will be erased.

c) Data protection/ confidentiality (also see Section 18).

Confidentiality of collected data; precautions and safeguards to protect the collected data will be taken, and data will be securely stored on the university of Oxford servers and/or the researcher PC.

Any other ethical issues. For more guidance on ethical issues, please see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources

| 17. Will your research involve discussing sensitive issues? This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/ mental health, trade union membership, sexual life or criminal activities. If you answered 'Yes', make sure you include some supporting information (as directed in **section 14b** above, showing the range of questions covering these issues. | Yes ☐ | No ☒ |
|---|---|---|

Please provide further details:

**18. Management and handling of personal and other research data**

All information provided by participants is considered research data for the purpose of this form. Any research data from which participants can be identified is known as personal data; any personal data which is sensitive is considered special category data.

Management of personal data, either directly or via a third party, must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. In answering the questions below, please also consider the points raised in the Data Protection Checklist and whether, for higher-risk data processing, a separate Data Protection Impact Assessment (DPIA) may also be required for the research. Advice on research data management and security is

| | |
|---|---|
| available from Research Data Oxford and your local IT department. Advice on data protection is available from information.compliance@admin.ox.ac.uk.<br><br>a) Please mark 'X' against the data you will collect for your research | |
| Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name) | ☒ |
| Online consent (may be anonymous) | ☒ |
| Opt-out forms | ☒ |
| Contact details for research purposes only (destroyed when no longer needed for this research) | ☒ |
| Contact details kept for future studies | ☒ |
| Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive) | ☒ |
| Video recordings | ☐ |
| Transcript of audio/ video recordings | ☒ |
| Photographs | ☐ |
| Task results (e.g. paper/ online tasks, diary completion) | ☒ |
| Questionnaire answers | ☐ |
| Field notes | ☒ |
| Other (please specify below) | ☐ |
| | |
| b) For each of the types of data selected above, state how this will be physically transferred from where it is collected to a local secure storage site (and backed up as necessary). This includes paper records and data captured electronically. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| c) How and where will each type of data be stored during the research (until the end of all participant involvement)? Describe the arrangements for ensuring confidentiality, i.e. location of storage (e.g. Nexus 365 OneDrive for Business, SharePoint), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| d) Will you use a unique participant number on research data instead of a participant name? If yes, state whether or not you will retain a list of participant names against numbers (i.e. pseudonymisation via a linkage list). Where will the list be stored, and when will it be destroyed? | |

| | | |
|---|---|---|
| We will use a unique code number for each participant instead of the participant's explicit name.<br><br>During the execution of the interviews, we will retain a list of participant names against codes. The list will be stored on Oxford Nexus 365 OneDrive. That list will be permanently destroyed as soon as it is no longer needed for the study. | | |
| e) Who will have access to the research data? | | |
| The researcher only. | | |
| f) If research data is to be shared with another organisation, how will it be transferred/ disclosed securely? | | |
| The research data will not be shared with another organization. | | |
| g) When and how will identifiable data (including audio/ video recordings & photos) be destroyed or deleted?<br>Note: Records of consent should be retained for a minimum of three years after publication or public release. Some funders may require longer periods. If you wish to retain contact details in order to re-approach participants about future studies, you must detail this in information provided to them and obtain specific consent for this. | | |
| All identifiable data will be securely stored on Oxford Nexus 365 OneDrive.<br><br>The data will be destroyed after the stated periods according to data retention policies of the university. | | |
| h) Please confirm that you will store other research data safely for at least 3 years after final publication or public release and adhere to any additional research funder policies. For more information about the University policies, please see the University's web pages on research data management. | Yes ☒ | No ☐ |
| If 'Yes', please give details of who will store the data and on storage format, location and security. Note that open science is encouraged.<br>If 'No', please provide further details below. | | |
| The data will be stored on the Open Science framework.<br><br>The stored data includes the fully pseudonymized transcripts with all other relevant information that could NOT be used to re-identify participants again | | |
| i) Does your research involve the use of secondary (i.e. previously collected) data? Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally collected for other research purposes. (If "No", please go to question 19.) | Yes ☐ | No ☒ |
| j) Do you have data access agreements for the use of this secondary data?<br>(If so, please attach these.) | Yes ☐ | No ☐ |

| | | |
|---|---|---|
| k) Is your use of this secondary data compatible with what the data subjects/ participants agreed that their data should be used for? | Yes ☐ | No ☐ |
| l) Could this data be linked back to an individual or individuals? If yes, address how securely any personally identifiable data will be transferred to you, and where and for how long it will be stored during or after the research. Who will have access to it? | Yes ☐ | No ☐ |
| | | |

| 19. Publication and dissemination of research data and outputs.<br>How will you disseminate and feedback project outcomes at the end of the research? |
|---|
| We will seek to publish the research study results in academic conferences and journals (e.g. SOUPS, CHI, CSCW, IJHCS).<br><br>The published papers will not include any kind of data that might lead to uncover participants' identities, or create any risks/threats for the participants (e.g. their privacy and safety). |

| **SECTION C: Methods and procedures to be used** | |
|---|---|
| 1. Please indicate the methods to be used: | **Mark 'X'** |
| a) Analysis of existing records | ☐ |
| b) Snowball sampling (recruiting through contacts of existing participants) | ☒ |
| c) Use of casual or local workers e.g. interpreters | ☐ |
| d) Participant observation | ☐ |
| e) Covert observation | ☐ |
| f) Observation of specific organisational practices | ☐ |
| g) Participant completes questionnaire in hard copy | ☐ |
| h) Participant completes online questionnaire or other online task | ☐ |
| i) Using social media | ☐ |
| j) Participant performs paper and pencil task | ☐ |
| k) Participant performs verbal or aural task (e.g. for linguistic study) | ☐ |
| l) Focus group | ☐ |
| m) Interview | ☒ |
| n) Audio recording of participant (you will generally need specific consent from participants for this) | ☒ |
| o) Video recording of participant (you will generally need specific consent from participants for this) | ☐ |
| p) Photography of participant (you will generally need specific consent from participants for this) | ☐ |
| q) Others (please specify below) | ☐ |

| Please ensure you have addressed any potential ethical issues related to these methods in question B14 and in your Participant Information Sheet. |
| --- |
| I have taken three training courses from the MPLS research training courses list: “Your successful DPhil”, “Research Ethics, and the “Research Integrity”<br><br>The three courses had explained in depth the research ethics management.<br><br>The first course was taken in 24-Nov-2020, and the second course was taken in 25-July-2021, and the third course was taken in September-2021. |

**SECTION D: Professional guidelines and training**

In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. This is not an exhaustive list.

| **Research specialism/ methodology** | **Association and guidance document** | **Please mark 'X'** |
|---|---|---|
| Anthropology | Association of Social Anthropologists of the UK and Commonwealth | ☐ |
| Computer Sciences | ACM Code of Ethics and Professional Conduct | ☐ |
| Criminology | British Society of Criminology | ☐ |
| Education | British Educational Research Association Ethical Guidelines for Educational Research | ☐ |
| Geography | Association of American Geographers Statement on Professional Ethics | ☐ |
| History | Oral History Society of the UK Ethical Guidelines | ☐ |
| Internet-based Research | British Psychological Society: Conducting Research on the Internet<br>Association of Internet Researchers Ethics Guide<br>ACM Code of Ethics and Professional Conduct<br>Association of Internet Researchers (AoIR)<br>Also see CUREC's Best Practice Guidance on internet-based research | ☐ |
| Law (Socio-Legal) | Socio-Legal Studies Association: Statement of Principles of Ethical Research | ☐ |
| Management | Academy of Management's Professional Code of Ethics | ☐ |
| Political Science | American Political Science Association (APSA) Guide to Professional Ethics in Political Science | ☐ |
| Politics | Political Studies Association. Guidelines for Good Professional Conduct | ☐ |
| Psychology | British Psychological Society Code of Ethics and Conduct | ☐ |
| Social Research | Social Research Association: Ethical Guidelines | ☒ |
| Sociology | The British Sociological Association: Statement of Ethical Practice | ☐ |
| Visual Research | ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research | ☐ |
| Other professional guidelines. Please specify the other guidelines used here: | | ☐ |
| | | |

Please indicate what training in research ethics (or research methodology) the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at http://researchsupport.admin.ox.ac.uk/support/training/ethics), or discussions between researchers and supervisors, if applicable.

**SECTION E: Signatures or email endorsements**

The SSH IDREC Secretariat accepts either option below. If you have a DREC, check which option it prefers.
**Option 1**: Email confirmation from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities. Pasted images of signatures cannot be accepted.
**Option 2**: Handwritten signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email to us.

Please ensure this checklist is signed by:

**For staff research**:
1. Principal Investigator
2. Head of Department (or nominee)

**For student research**:
1. Principal Investigator (project supervisor)
2. Head of Department (or nominee)
3. Student researcher

**Principal Investigator signature/ supervisor signature (if student research)**

I understand my responsibilities as Principal Investigator as outlined in the CUREC glossary and guidance on the CUREC website. I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal investigator on this project and supply the name and contact details of my successor if appropriate.

**Signature** (or email endorsement using the above declaration): _____

**Print name**: ___IVAN FLECHAIS_____ **Date**: __23-11-2022___

**Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

- consider the PI and student researcher (if applicable) to be aware of their ethical responsibilities in regard to the ethical issues associated with this research;
- am satisfied that: the proposed project design and scientific methodology are sound; the project has been subject to appropriate peer review; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the public interest.

Signed by Head of Department or nominee (example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies):

**Signature** (or email endorsement using the above declaration): _____

**Print name**: _____ **Date**: _____

**Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal investigator properly authorised by the CUREC system.

**Signature by student** (or email endorsement using the above declaration):



Wael.albayaydh@cs.ox.ac.uk

**Print** name: WAEL ALBAYAYDH_____ **Date**: _15-11-2022_____

## G.3.5 Third Study Information Sheet




**Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Researcher**
Wael Albayaydh
wael.albayaydh@cs.ox.ac.uk

**Exploring Privacy Protection Means in the Smart Home**

**PARTICIPANT INFORMATION SHEET**

Ethics Approval Reference: (CS_C1A_22_007)

1. ***What is the purpose of this study?***
   This research aims to provide insights into the privacy protection means in the smart home's context. An understanding of privacy protection means to devise new solutions to improve privacy protection.

2. ***Why have I been invited to take part?***
   You have been invited to take part in this study as we aim to include people who are above 18 years old and are involved in smart devices design. We will ask you questions about smart device design and whether you consider privacy and security aspects, in addition to your insights about what should be done to consider privacy and security concerns in future.

3. ***Do I have to take part?***
   No. You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself and your data from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision. All your data will be erased from our records. Withdrawal is possible within 4 weeks from the date your interview took place.

   You can ask me to remove any particular information from my transcript, or you can withdraw from the study entirely. If you choose to withdraw, We will delete all transcripts, recordings and other data we hold about you. For the Voucher, you may keep it in case of withdrawal after the interview has taken place.

4. ***What will happen to me if I take part in the study?***
   If you are happy to take part in the study, you will be asked a number of questions about yourself, the household you are living in, activities in the home, and smart devices you use or deal with.
   This should take approximately 45 minutes, but not longer than one hour. The study will take place online only. The oral consent includes the option to withdraw of follow up enquiries we might have. If you wish to do so, just tell the researcher during taking the oral consent. You are invited to volunteer and take part in this study. While there is no compensation for your participation, your input will contribute to a deeper understanding of privacy concerns associated with smart devices, ultimately enhancing privacy protection for users in smart homes. With your consent, the interview will be recorded on audio. If you don't wish to be audio recorded, please inform the researcher. Audio recording is mandatory for the interviews. The researcher will transcribe the interview to generate an anonymized data. However, neither the audio file

nor the transcription made available to any other person than the researcher and principal investigator. The Audio recordings will be destroyed after transcribing them into text files

5. ***Are there any potential risks in taking part?***
   We collect information about yourself and your household. To guarantee appropriate data management we will fully anonymize this information and store it on an encrypted and password-protected hard drive within the University. We will apply appropriate safe-guards to protect your data.

6. ***What happens to the data provided?***
   The **research anonymized data** will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

   If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts.

   **Personal/sensitive data** will be stored separately and confidentially, only accessible to the researcher.

   All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

   Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

7. ***Will the research be published?***

   The research will be published as part of the RISCS research scheme. Future research papers might be published at academic conferences.

   The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

   If you agree to participate in this study, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published open access.

   Please visit https://www.oerc.ox.ac.uk/

8. ***Who is organising and funding the research?***
   This research is part of a DPhil thesis investigating privacy concerns of bystanders in smart homes

9. ***Who has reviewed this study?***
   This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: CS_C1A_22_007)

10. ***Who do I contact if I have a concern about the study or I wish to complain?***

    If you have a concern about any aspect of this study please contact Wael Albayaydh (wael.albayaydh@cs.ox.ac.uk) or Ivan Flechais (Supervisor - ivan.flechais@cs.ox.ac.uk), who will do their

best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Computer Science Department Research Ethics Committee:
Email: ethics@cs.ox.ac.uk.
Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***11. Further Information and Contact Details***

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

**Researcher**
Wael Albayaydh,
University of Oxford
Department of Computer Science
Wolfson Building
Parks Road
OXFORD - OX1 3QD
United Kingdom
Oxford email address: wael.albayaydh@cs.ox.ac.uk

# G.3.6 Third Study - Consent Form

**Exploring Design Challenges of Privacy Protection with Smart Home in Jordan**
Researcher: Wael Albayaydh
Document Version: 15/12/2022

**Participant Oral Consent Form**

CUREC Approval Reference: CS_C1A_22_007

**Exploring Design Challenges of Privacy Protection with Smart Home in Jordan**

**Purpose of Study:**

This study aims to provide insights into the privacy protection means in the smart homes context. An understanding of privacy protection means to devise new solutions to improve privacy protection.

**Consent Taking**

Record this consent process using a digital recorder (if the participant has consented to this) or by using a Record of Consent Form. PIN-protect the recorder if possible (particularly for sensitive data].

**1. Oral information giving to participants**

- ***Introduction* (*)***:* Hello, my name is Wael Albayaydh. I'm doing some research and I wondered if you'd be interested in being involved. I'm currently doing my DPhil Research at the University of Oxford in the Department of Computer Science. Can I tell you more about the study? *[Await confirmation].*
- ***Project details and aims:*** In my study, I want to investigate the Bystanders' Privacy Concerns with the Smart Home in the Middle East. I'm interested in meeting families that live in smart homes, and their domestic workers to talk about smart devices and their privacy concerns. If you choose to be a part of this project, here is what will happen:
- ***Interviews/surveys/ tasks description:*** I will have a conversation with you where I will ask a range of questions about smart devices and privacy.
- ***Data sharing/access/confidentiality:*** The data you give will form the basis of my DPhil research thesis. The research anonymized data will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

  If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts. Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

***Data storage:*** The collected data will be stored separately and confidentially on servers controlled by the university of Oxford, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit. All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

- ***Anonymity/pseudonyms/identifiable data:*** In any publications a fake name/ID number will be used (i.e. a pseudonym)/**or** your name and other identifying details will be anonymised by using a unique ID code for each participant, and we will ask the interviewees not to mention their names, address, email address, phone number, work place address, or any other information that may lead to identify them. If participants overshare information that may lead to identify them, we will remove it from the original recordings before we store them and before the transcription. We will delete all recordings after we finish the transcriptions, as we will not need them after that stage. We will make sure that the transcriptions are fully anonymized. / **or** you will be named (if you would like to be identified and if it is safe for you).
- ***Risks****:* There is no risks associated with the interviews, but to make sure that we eliminate any risks that may not be clear to us, we will anonymize the data to make sure there is no information that may lead to identifying participants personal IDs.
- ***Rights:*** You don't have to agree to take part; you can ask me any questions you want before or throughout; you can also withdraw at any stage without giving a reason before you do the interview, and you can withdraw within 4 weeks after the interview took place.
- ***Audio/video recording/photos/notes/keeping contact details:*** With your permission, I would like to make an audio recording of our discussion to make sure I'm getting an accurate record of your thoughts. I may want to re-contact you to clarify information you gave me in your interview.
- ***Publication plans:*** The project may/will be published in a(n) [thesis / dissertation/ academic journal/ academic book / academic website]. A copy of my [thesis / dissertation], will be deposited both in print and online in the University archives.[1]
- ***Complaints/concerns procedure:*** If you have any complaints or concerns please feel free to contact me in the first instance.

**Researcher:**
Wael Albayaydh,
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY
UK
Phone Number: +44 1865 283604
Oxford email address: wael.albayaydh@cs.ox.ac.uk

**Or the Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Or, the Chair, Computer Science Department Research Ethics Committee**

Email: ethics@cs.ox.ac.uk.

Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***Ethics review details:*** This research project has been reviewed and approved by an Oxford University ethics committee. Ethics Approval Reference: (CS_C1A_22_007). If, after contacting me with any concern, you're still unhappy and wish to make a formal complaint, please contact the ethics committee. Their email address ethics@cs.ox.ac.uk. Address: Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

- ***Data Protection statement****:* The University of Oxford is responsible overall for ensuring the safe and proper use of any personal information you provide, solely for research purposes. Further information about your rights to information you provide is available from the University's data protection web site (https://compliance.web.ox.ac.uk/individual-rights.
- ***Questions/concerns?*** Do you have any questions?

**2. Oral consent seeking stage, after participant has had sufficient time to think about whether s/he wants to take part. Record the participant response to below questions.**

- Do you give your permission for me to interview you and audio record you?
- Do you give permission for me to re-contact you to clarify information?
- Do you give me permission to quote you (using your pseudonym)?
- Are you happy to take part?

Ok, thanks, let's start.

## G.4 Fourth Study Ethics Application

### G.4.1 Fourth Study - Advertisement Poster

For the advertisement poster of the fourth study, please refer to Appendix E.1, and Appendix E.2.

### G.4.2 Fourth Study - Survey Question Guidelines

For the survey question guidelines of the fourth study, please refer to Appendix E.3.

### G.4.3 Fourth Study - Interview Question Guidelines

For the focus group and interview guidelines of the fourth study, please refer to Appendix E.4, and Appendix E.5.

# G.4.4 Fourth Study Ethics Application

**CENTRAL UNIVERSITY**
**RESEARCH ETHICS COMMITTEE (CUREC)**

**CUREC 1A Checklist**
**for the Social Sciences and Humanities**




The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

Please refer to Where and how to apply for ethical review and the CUREC flowchart first to see if you need ethics approval.

Please complete this form using a word processor and email it, together with your supporting documents, to your Departmental Research Ethics Committee (DREC) (if applicable). If you don't have a DREC please email this form to ethics@socsci.ox.ac.uk using your official ox.ac.uk email address. Only type-written, emailed applications will be accepted.

| **SECTION A: Filter for CUREC 2 application** | | |
|---|---|---|
| This section determines whether your study raises more complex issues requiring the completion of a full application for ethical review, known as the CUREC 2 application.<br>**(Please mark 'X' in the Yes/ No column.)** | | |
| 1. Are research participants classed as people whose ability to give free and informed consent is in question? (This may include under 18s (although see competent youths), prisoners, or adults at risk.) Your attention is drawn to the University's Safeguarding Code of Practice and its implications for researchers involving children or adults at risk. This includes the need for the work to be risk assessed and for researchers to undertake related training. (**Note**: If any of your participants are aged 16 or under, answer 'Yes' here **and** also answer question 5 below.) | Yes ☐ | No ☒ |
| 2. By taking part in the research, will participants be at risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)? | Yes ☐ | No ☒ |
| 3. Does the research involve the deception of participants? | Yes ☐ | No ☒ |
| 4. Does your research raise issues relevant to the Counter-Terrorism and Security Act (the Prevent duty), which seeks to prevent people from being drawn into terrorism? Please see advice on this on our Best Practice Guidance web page. | Yes ☐ | No ☒ |
| If you answered 'No' to **all** the questions above, go to **Section B**.<br>If you answered 'Yes' to **any** question above, continue to question 5 below. | | |
| 5. Is your project covered by a CUREC Approved Procedure (formerly known as "CUREC Protocols")? | Yes ☐ | No ☒ |
| If yes, give the specific Approved Procedure number(s): | | |
| If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **stop completing this checklist and do not submit it for ethical review**. Instead, complete the CUREC 2 application form from the CUREC website, then submit that for ethical review.<br>If you answered '**Yes'** to ANY of questions 1-3, **and** answered '**Yes'** to question 5, go on to **Section B**. | | |

| **SECTION B: Contact details and project description** | |
|---|---|
| **Contact details:** | |
| 1. Principal Investigator **or** supervisor (if student research) (give title and full name) | Prof. Ivan Flechais |
| 2. Name of student (if student research) | Wael Albayaydh |
| 3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil | DPhil |
| 4. Department or Institute name | Department of Computer Science |
| 5. Address for correspondence (if different from above) | Wael Albayaydh<br>St Hilda's College, Cowley Place<br>Oxford OX4 1DY<br>UK |
| 6. University (not private) e-mail address and telephone number | wael.albayaydh@cs.ox.ac.uk |
| 7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant) | |

| **Project description:** | |
|---|---|
| 8. Title of research project | Enhancing Bystander Privacy Protection: A Mobile App approach for Jordanian Smart Homes |
| 9. List of location(s) where project will be conducted | Jordan |
| 10. If your research involves overseas fieldwork or travel and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This must be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.) Please also address any physical or psychological risks for Oxford researchers and local fieldworkers in question 16 below and discuss with your Safety Officer. | Yes ☒<br>No ☐<br>Not required in this instance ☒<br><br>There are no risks as we will discuss how to develop a mobile application for smart home devices, and all focus groups will be conducted online [Zoom] |
| 11. Anticipated duration of overall research project | months or 1 years (maximum 5)<br><br>4 years |
| 12. Anticipated start and end dates of the part of the research project involving human participants and/or personal data | From: 15/04/23)<br>To: (30/10/23) |

| | |
|---|---|
| | Note: You will need ethics approval before you start your research. CUREC 1 As may take up to **30 days** to process. Retrospective ethics approval **cannot** be granted. |
| In the case of international or collaborative research, will you submit or have you submitted this project for ethical review or consideration elsewhere (e.g. collaborator's/ local ethics committee, or other local approval)? | Yes ☐<br>No ☒<br>If 'Yes', please attach ethics or other approvals and give more details below.<br>If 'No', please explain your reasons below.<br>Please also refer to the Best Practice Guidance on Ethical Review of social-sciences based research conducted outside the UK (BPG 16), which includes an Ethics Issues Checklist for International Research (Appendix A) |
| Please supply further details in response to question 12b here.<br><br>I am not cooperating with local institutions in Jordan.<br>Reference the Best Practice Guidance 10_Version 1.0, we will follow it strictly.<br>We will assure participants that the data collected will be managed with strict confidentiality, we will destroy audio recordings after we finish the transcribing of them, we will avoid questions that might be sensitive or may create risks for both the researcher and the participants. We will inform participants that they can skip any question they do not wish to answer | |
| 13. External organisation funding the research (if applicable) | |
| 14. Brief description of research (about 150 words) in lay language.<br>a) When describing the research, include your methodology, how you are applying professional guidelines, and the use to which results/ data will be put. Please also declare any conflicts of interest here. | |
| Title: "Focus Group Study to Collect Stakeholders Insights on Developing Mobile Application to Support Bystanders' Privacy Protection in the Smart Home"<br><br>This work is the fourth project of my DPhil research study which aims to explore how mobile application can support privacy protection of bystanders in the smart home. We will conduct online (e.g. skype, or zoom) focus group study with participants who have relevant expereince.<br><br>The interviews will not start before the the participant's consent to participate, to be audio recorded, and to give her/his feedback.<br><br>Up to my knowledge, there is no conflict of interest associated with executing this reseach. | |
| b) Description of participants and how you will obtain informed consent to take part in the research. | |
| i. Description of participants and your criteria for inclusion/ exclusion. | |
| Participants include individuals (over 18)). Children will not be included.<br><br>This study is conducted in Jordan, and hence participation is geographically limited for some particioants (households, domestic workers, and policymakers). Teams/Skype/Zoom will be used to interview participants online as per their choice. | |
| ii. Your method(s) of recruitment. | |

We will advertise the study and we will contact companies, organizations and associations directly to recruit households, domestic workerrs, policy makers, designbers, and mbile app developers. After we explain the research plan and the objectives of this research. We will use snowball sampling as well.

Participants may be pre-screened before they are allowed participation in the study. Pre-screening follows initial email to the participant and is done using online survey. Participants will be registered with a unique ID which only the researcher can link to a name. Information on the pre-screening data will be a subset of the demographics questionnaire survey.The survey will at no at any point ask to provide the email address, the IP address , or the participant's name nor will this information be recorded online by other means known to the researcher. Instead the survey will ask paricipants to privide the researcher on how he can contact them.

Independent of the recruitment, consent for participation will be sought from individuals before the beginning of session.

There will be no compensation for participating in this study, and we will thank participanst for vlunteering in the study.

| iii. Your processes for obtaining informed consent from participants. | |
|---|---|
| Before the beginning of each session an oral consent wil be sought from all participants. An information sheet explaining the purpose of the study and intended usage of data (see attachement) will be presented alongside the consent form (in person or via an mean as per the particiopant preference). The information sheet will be provided to the participants at least 24h in advance to their participation.<br>The oral consent will be recorded by the researcher before the beginning of each session. | |
| Please attach separate supporting documents (in Word), if appropriate, for your research (English language versions only). Tick those you are submitting below. If appropriate supporting documents are not submitted, you will be asked to provide these separately, which may delay the ethical review process. | |
| Recruitment and advertisement material (e.g. a poster, social media recruitment text, or brief invitation letter/ email). | ☒ |
| Information for participants to read (or hear) before they agree to take part (e.g. written information or, if applicable, an outline oral information script). | ☒ |
| A document to record informed consent. Templates for written consent forms and/ or oral information scripts (in case of an oral consent process) are available from the CUREC website. | ☒ |
| Questions to be asked of participants (e.g. focus group, interview questions, or a preliminary scope of questions, or a sample questionnaire). | ☒ |
| (If applicable) debriefing document after participants have taken part. | ☐ |
| Please add any further details. If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants Please answer question 15 if you cannot obtain informed consent. | |
| No further details to be added. | |
| 15. If you cannot obtain informed consent from participants according to CUREC guidelines and good practice in your discipline, please give a brief explanation and justification of this decision below. | |
| | |
| 16. What are the ethical issues connected with your research and what steps have you taken to address them? Please do not answer 'none'. We need to see that you have identified potential ethical issues with respect to your research and have taken steps to address them. If applicable, please address: | |
| a) Participant burdens and/or risks | |
| 1. Privacy issues. We ensure participants that their data will be kept secure, not shared, and all information treated as highly confidential.<br>2. Use of direct quotes; participant's data will be anonymised and only identified by a code that is known to the researcher only.<br>3. Each participant will have a unique code that is known to the research team only. | |

b) Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the University's and Social Science Division's Safety in Fieldwork guidance)

1- The research does not cover political, religious, or any kind of sensitive topics that may lead to risky consequences to the researcher's safety and privacy. The researcher will explore the use of mobile application to support privacy protection in the smart homes.

2- The research will be conducted online (e.g. Skype or Zoom), with no physical interaction with the participants, which will minimise the health & safety risks for the researcher of being physically in a risky area or environment.

3- To avoid any conflict with participants, or unwanted reactions:

- We will inform participants that they may skip any question and not to answer it, and it will be removed from the session transcript.
- We will inform participants that they can withdraw of the study at any point in time in which case all their records will be erased.

c) Data protection/ confidentiality (also see Section 18).

Confidentiality of collected data; precautions and safeguards to protect the collected data will be taken, and data will be securely stored on the university of Oxford servers and/or the researcher PC.

Any other ethical issues. For more guidance on ethical issues, please see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources

| | | |
|---|---|---|
| 17. Will your research involve discussing sensitive issues? This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/ mental health, trade union membership, sexual life or criminal activities. If you answered 'Yes', make sure you include some supporting information (as directed in **section 14b** above, showing the range of questions covering these issues. | Yes ☐ | No ☒ |

Please provide further details:

**18. Management and handling of personal and other research data**

All information provided by participants is considered research data for the purpose of this form. Any research data from which participants can be identified is known as personal data; any personal data which is sensitive is considered special category data.

Management of personal data, either directly or via a third party, must comply with the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, as set out in the University's Guidance on Data Protection and Research. In answering the questions below, please also consider the points raised in the Data Protection Checklist and whether, for higher-risk data processing, a separate Data Protection Impact Assessment (DPIA) may also be required for the research. Advice on research data management and security is

| | |
|---|---|
| available from Research Data Oxford and your local IT department. Advice on data protection is available from information.compliance@admin.ox.ac.uk.<br><br>a) Please mark 'X' against the data you will collect for your research | |
| Consent records (written consent forms, audio-recorded consent, assent forms (for research involving minors) including participant name) | ☒ |
| Online consent (may be anonymous) | ☒ |
| Opt-out forms | ☒ |
| Contact details for research purposes only (destroyed when no longer needed for this research) | ☒ |
| Contact details kept for future studies | ☒ |
| Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive) | ☒ |
| Video recordings | ☐ |
| Transcript of audio/ video recordings | ☒ |
| Photographs | ☐ |
| Task results (e.g. paper/ online tasks, diary completion) | ☒ |
| Questionnaire answers | ☐ |
| Field notes | ☒ |
| Other (please specify below) | ☐ |
| | |
| b) For each of the types of data selected above, state how this will be physically transferred from where it is collected to a local secure storage site (and backed up as necessary). This includes paper records and data captured electronically. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| c) How and where will each type of data be stored during the research (until the end of all participant involvement)? Describe the arrangements for ensuring confidentiality, i.e. location of storage (e.g. Nexus 365 OneDrive for Business, SharePoint), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives. | |
| All data gathered as part of this research will be securely stored backed up on Oxford Nexus 365 OneDrive. The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption to protect the data.<br><br>Personal data will be destroyed as soon as it is no longer needed for the study. | |
| d) Will you use a unique participant number on research data instead of a participant name? If yes, state whether or not you will retain a list of participant names against numbers (i.e. pseudonymisation via a linkage list). Where will the list be stored, and when will it be destroyed? | |

| | | |
|---|---|---|
| We will use a unique code number for each participant instead of the participant's explicit name.<br><br>During the execution of the sessions, we will retain a list of participant names against codes. The list will be stored on Oxford Nexus 365 OneDrive. That list will be permanently destroyed as soon as it is no longer needed for the study. | | |
| e) Who will have access to the research data? | | |
| The researcher only. | | |
| f) If research data is to be shared with another organisation, how will it be transferred/ disclosed securely? | | |
| The research data will not be shared with another organization. | | |
| g) When and how will identifiable data (including audio/ video recordings & photos) be destroyed or deleted?<br>Note: Records of consent should be retained for a minimum of three years after publication or public release. Some funders may require longer periods. If you wish to retain contact details in order to re-approach participants about future studies, you must detail this in information provided to them and obtain specific consent for this. | | |
| All identifiable data will be securely stored on Oxford Nexus 365 OneDrive.<br><br>The data will be destroyed after the stated periods according to data retention policies of the university. | | |
| h) Please confirm that you will store other research data safely for at least 3 years after final publication or public release and adhere to any additional research funder policies. For more information about the University policies, please see the University's web pages on research data management. | Yes ☒ | No ☐ |
| If 'Yes', please give details of who will store the data and on storage format, location and security. Note that open science is encouraged.<br>If 'No', please provide further details below. | | |
| The data will be stored on the Open Science framework. https://osf.io<br><br>The stored data includes the fully pseudonymized transcripts with all other relevant information that could NOT be used to re-identify participants again | | |
| i) Does your research involve the use of secondary (i.e. previously collected) data? Common sources of secondary data include censuses, information collected by government departments, organisational records and data that was originally collected for other research purposes. (If "No", please go to question 19.) | Yes ☐ | No ☒ |
| j) Do you have data access agreements for the use of this secondary data?<br>(If so, please attach these.) | Yes ☐ | No ☐ |

| | | |
|---|---|---|
| k) Is your use of this secondary data compatible with what the data subjects/ participants agreed that their data should be used for? | Yes ☐ | No ☐ |
| l) Could this data be linked back to an individual or individuals? If yes, address how securely any personally identifiable data will be transferred to you, and where and for how long it will be stored during or after the research. Who will have access to it? | Yes ☐ | No ☐ |
| | | |

| 19. Publication and dissemination of research data and outputs.<br>How will you disseminate and feedback project outcomes at the end of the research? |
|---|
| We will seek to publish the research study results in academic conferences and journals (e.g. SOUPS, CHI, CSCW, IJHCS).<br><br>The published papers will not include any kind of data that might lead to uncover participants' identities, or create any risks/threats for the participants (e.g. their privacy and safety). |

| **SECTION C: Methods and procedures to be used** | |
|---|---|
| 1. Please indicate the methods to be used: | **Mark 'X'** |
| a) Analysis of existing records | ☐ |
| b) Snowball sampling (recruiting through contacts of existing participants) | ☒ |
| c) Use of casual or local workers e.g. interpreters | ☐ |
| d) Participant observation | ☐ |
| e) Covert observation | ☐ |
| f) Observation of specific organisational practices | ☐ |
| g) Participant completes questionnaire in hard copy | ☐ |
| h) Participant completes online questionnaire or other online task | ☐ |
| i) Using social media | ☐ |
| j) Participant performs paper and pencil task | ☐ |
| k) Participant performs verbal or aural task (e.g. for linguistic study) | ☐ |
| l) Focus group | ☒ |
| m) Interview | ☐ |
| n) Audio recording of participant (you will generally need specific consent from participants for this) | ☒ |
| o) Video recording of participant (you will generally need specific consent from participants for this) | ☐ |
| p) Photography of participant (you will generally need specific consent from participants for this) | ☐ |
| q) Others (please specify below) | ☐ |

| Please ensure you have addressed any potential ethical issues related to these methods in question B14 and in your Participant Information Sheet. |
| --- |
| I have taken three training courses from the MPLS research training courses list: “Your successful DPhil”, “Research Ethics, and the “Research Integrity”<br><br>The three courses had explained in depth the research ethics management.<br><br>The first course was taken in 24-Nov-2020, and the second course was taken in 25-July-2021, and the third course was taken in September-2021. |

**SECTION D: Professional guidelines and training**

In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. This is not an exhaustive list.

| **Research specialism/ methodology** | **Association and guidance document** | **Please mark 'X'** |
|---|---|---|
| Anthropology | Association of Social Anthropologists of the UK and Commonwealth | ☐ |
| Computer Sciences | ACM Code of Ethics and Professional Conduct | ☐ |
| Criminology | British Society of Criminology | ☐ |
| Education | British Educational Research Association Ethical Guidelines for Educational Research | ☐ |
| Geography | Association of American Geographers Statement on Professional Ethics | ☐ |
| History | Oral History Society of the UK Ethical Guidelines | ☐ |
| Internet-based Research | British Psychological Society: Conducting Research on the Internet<br>Association of Internet Researchers Ethics Guide<br>ACM Code of Ethics and Professional Conduct<br>Association of Internet Researchers (AoIR)<br>Also see CUREC's Best Practice Guidance on internet-based research | ☐ |
| Law (Socio-Legal) | Socio-Legal Studies Association: Statement of Principles of Ethical Research | ☐ |
| Management | Academy of Management's Professional Code of Ethics | ☐ |
| Political Science | American Political Science Association (APSA) Guide to Professional Ethics in Political Science | ☐ |
| Politics | Political Studies Association. Guidelines for Good Professional Conduct | ☐ |
| Psychology | British Psychological Society Code of Ethics and Conduct | ☐ |
| Social Research | Social Research Association: Ethical Guidelines | ☒ |
| Sociology | The British Sociological Association: Statement of Ethical Practice | ☐ |
| Visual Research | ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research | ☐ |
| Other professional guidelines. Please specify the other guidelines used here: | | ☐ |

Please indicate what training in research ethics (or research methodology) the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at http://researchsupport.admin.ox.ac.uk/support/training/ethics), or discussions between researchers and supervisors, if applicable.

**SECTION E: Signatures or email endorsements**

The SSH IDREC Secretariat accepts either option below. If you have a DREC, check which option it prefers.
**Option 1**: Email confirmation from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities. Pasted images of signatures cannot be accepted.
**Option 2**: Handwritten signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email to us.

Please ensure this checklist is signed by:

**For staff research**:
1. Principal Investigator
2. Head of Department (or nominee)

**For student research**:
1. Principal Investigator (project supervisor)
2. Head of Department (or nominee)
3. Student researcher

**Principal Investigator signature/ supervisor signature (if student research)**

I understand my responsibilities as Principal Investigator as outlined in the CUREC glossary and guidance on the CUREC website. I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal investigator on this project and supply the name and contact details of my successor if appropriate.

**Signature** (or email endorsement using the above declaration): _____

**Print name**: ____IVAN FLECHAIS_____ **Date**: _____17-01-2023_____

**Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

- consider the PI and student researcher (if applicable) to be aware of their ethical responsibilities in regard to the ethical issues associated with this research;
- am satisfied that: the proposed project design and scientific methodology are sound; the project has been subject to appropriate peer review; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the public interest.

Signed by Head of Department or nominee (example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies):

**Signature** (or email endorsement using the above declaration): _____

**Print name**: _____ **Date**: _____

**Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal investigator properly authorised by the CUREC system.

**Signature by student** (or email endorsement using the above declaration):



Wael.albayaydh@cs.ox.ac.uk

**Print** name: WAEL ALBAYAYDH_____ **Date**: _09-01-2023_____

## G.4.5 Fourth Study Information Sheet




**Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Researcher**
Wael Albayaydh
wael.albayaydh@cs.ox.ac.uk

**Focus Group and Interview Study – Develop Mobile App to Support Bystanders' Privacy Protection in The Smart Home**

**PARTICIPANT INFORMATION SHEET**

Ethics Approval Reference: [CS_C1A_23_012]

1. ***What is the purpose of this study?***
   This research study aims to gather your insights on how to design a mobile app that can support privacy protection for bystanders in smart homes in Jordan. Your participation in this study is greatly appreciated and will be invaluable in helping us to develop a mobile app that meets the needs and expectations of smart home users, families, policy makers, and designers.

   As you may be aware, smart home devices have become increasingly popular in recent years, providing users with convenience, comfort, and security. However, the use of these devices also raises concerns about privacy protection for bystanders who may be unknowingly monitored or recorded. This is particularly important in the case of passive family members, domestic workers, and guests who may not have provided their consent for monitoring. In order to address these concerns and provide a solution that meets the needs of all stakeholders, we are conducting this focus group study to gather your insights and requirements for a mobile app that supports privacy protection for bystanders in the smart home.

   Your input will be crucial in helping us to develop a mobile app that is effective, user-friendly, and meets the needs of all stakeholders.

2. ***Why have I been invited to take part?***
   You have been invited to take part in this study as we aim to include people who are above 18 years old and are engaged with smart devices, whether they are users, domestic workers (bystanders to the devices), recruiters of domestic workers, policy makers, designers, or mobile application developers. During this focus group and interviews, we will be asking you a series of questions and discussing your thoughts and experiences related to smart home devices and privacy protection. Your opinions and perspectives are important to us, and we encourage you to share your thoughts openly and honestly.

3. ***Do I have to take part?***
   No. You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself and your data from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision. All your data will be erased from our records. Withdrawal is possible within 4 weeks from the date the focus group study took place.

You can ask the researcher to remove any particular information from my transcript, or you can withdraw from the study entirely. If you choose to withdraw, we will delete all transcripts, recordings and other data we hold about you.

4. ***What will happen to me if I take part in the study?***
If you are happy to take part in the study, you will be asked a number of questions about yourself, your experience with smart home devices that you use or deal with, and your insights about how a mobile application could support privacy protection in the smart home. The focus group should take approximately 90 minutes, but not longer than two hours. If you participate in the Interviews, they are expected to take less than 45 minutes. Both the focus groups, and the interviews will take place online only. The oral consent includes the option to withdraw of follow up enquiries we might have. If you wish to do so, just tell the researcher during taking the oral consent. You are invited to volunteer and take part in this study. While there is no compensation for your participation, your input will contribute to a deeper understanding of privacy concerns associated with smart devices, ultimately enhancing privacy protection for users in smart homes.

With your consent, the study will be recorded on audio. If you don't wish to be audio recorded, please inform the researcher. Audio recording is mandatory for this study. The researcher will transcribe the recorded study to generate an anonymized data. However, neither the audio file nor the transcription made available to any other person than the researcher and principal investigator. The Audio recordings will be destroyed after transcribing them into text files.

5. ***Are there any potential risks in taking part?*** share
To guarantee appropriate data management we will fully anonymize this information and store it on an encrypted and password-protected hard drive within the University. We will apply appropriate safe-guards to protect your data.

6. ***What happens to the data provided?***
The **research anonymized data** will be stored confidentially using an encrypted hard drive and kept locked away in the University. The **anonymized data** will be stored on Open Science framework " https://osf.io/". Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator. If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts.

**Personal/sensitive data** will be stored separately and confidentially, only accessible to the researcher.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research. Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit.

7. ***Will the research be published?***

The research will be published as part of the RISCS research scheme. Future research papers might be published at academic conferences.

The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford

postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

If you agree to participate in this focus group study, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published open access.

Please visit https://www.oerc.ox.ac.uk/

8. ***Who is organising and funding the research?***
This research is part of a DPhil thesis investigating privacy concerns of bystanders in smart homes

9. ***Who has reviewed this study?***
This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: [CS_C1A_23_012].

10. ***Who do I contact if I have a concern about the study or I wish to complain?***

If you have a concern about any aspect of this study please contact Wael Albayaydh (wael.albayaydh@cs.ox.ac.uk) or Ivan Flechais (Supervisor - ivan.flechais@cs.ox.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Computer Science Department Research Ethics Committee:
Email: ethics@cs.ox.ac.uk.
Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

11. ***Further Information and Contact Details***

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

**Researcher**
Wael Albayaydh,
University of Oxford
Department of Computer Science
Wolfson Building
Parks Road
OXFORD - OX1 3QD
United Kingdom
Oxford email address: wael.albayaydh@cs.ox.ac.uk

# G.4.6 Fourth Study - Consent Form

**Focus Group and Interview Study – Develop Mobile App to Support Bystanders' Privacy Protection in The Smart Home**
Researcher: Wael Albayaydh
Document Version: 21/05/2023

**Participant Oral Consent Form**

CUREC Approval Reference: CS_C1A_23_012

**Focus Group and Interview Study – Develop Mobile App to Support Bystanders' Privacy Protection in The Smart Home**

**Purpose of Study:**

This research study aims to gather your insights on how to design a mobile app that can support privacy protection for bystanders in smart homes in Jordan. Your participation in this study is greatly appreciated and will be invaluable in helping us to develop a mobile app that meets the needs and expectations of smart home users, families, policy makers, and designers.

**Consent Taking**

Record this consent process using a digital recorder (if the participant has consented to this) or by using a Record of Consent Form. PIN-protect the recorder if possible (particularly for sensitive data].

**1. Oral information giving to participants**

- ***Introduction* (*)***:* Hello, my name is Wael Albayaydh. I'm doing some research and I wondered if you'd be interested in being involved. I'm currently doing my DPhil Research at the University of Oxford in the Department of Computer Science. Can I tell you more about the study? *[Await confirmation].*
- ***Project details and aims:*** In my study, I want to investigate the Bystanders' Privacy Concerns with the Smart Home in the Middle East. I'm interested in meeting families that live in smart homes, and their domestic workers to talk about smart devices and their privacy concerns. If you choose to be a part of this project, here is what will happen:
- ***Interviews/surveys/ tasks description:*** I will have a conversation with you where I will ask a range of questions about smart devices and privacy.
- ***Data sharing/access/confidentiality:*** The data you give will form the basis of my DPhil research thesis. The research anonymized data will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

  If we decide to make the data available for other researchers, we will review it to make sure that we redact any inadvertent "oversharing" from the transcripts. Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher. This data may

also be confidentially shared with University authorities in the event of academic or financial audit.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

***Data storage:*** The collected data will be stored separately and confidentially on servers controlled by the university of Oxford, only accessible to the researcher. This data may also be confidentially shared with University authorities in the event of academic or financial audit. All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

- ***Anonymity/pseudonyms/identifiable data:*** In any publications a fake name/ID number will be used (i.e. a pseudonym)/**or** your name and other identifying details will be anonymised by using a unique ID code for each participant, and we will ask the interviewees not to mention their names, address, email address, phone number, work place address, or any other information that may lead to identify them. If participants overshare information that may lead to identify them, we will remove it from the original recordings before we store them and before the transcription. We will delete all recordings after we finish the transcriptions, as we will not need them after that stage. We will make sure that the transcriptions are fully anonymized. / **or** you will be named (if you would like to be identified and if it is safe for you).
- ***Risks****:* There is no risks associated with the interviews, but to make sure that we eliminate any risks that may not be clear to us, we will anonymize the data to make sure there is no information that may lead to identifying participants personal IDs.
- ***Rights:*** You don't have to agree to take part; you can ask me any questions you want before or throughout; you can also withdraw at any stage without giving a reason before you do the interview, and you can withdraw within 4 weeks after the interview took place.
- ***Audio/video recording/photos/notes/keeping contact details:*** With your permission, I would like to make an audio recording of our discussion to make sure I'm getting an accurate record of your thoughts. I may want to re-contact you to clarify information you gave me in your interview.
- ***Publication plans:*** The project may/will be published in a(n) [thesis / dissertation/ academic journal/ academic book / academic website]. A copy of my [thesis / dissertation], will be deposited both in print and online in the University archives.[1]
- ***Complaints/concerns procedure:*** If you have any complaints or concerns please feel free to contact me in the first instance.

**Researcher:**
Wael Albayaydh,
University of Oxford
St Hilda's College, Cowley Place
Oxford OX4 1DY
UK
Phone Number: +44 1865 283604
Oxford email address: wael.albayaydh@cs.ox.ac.uk

**Or the Principal Investigator**
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

**Or, the Chair, Computer Science Department Research Ethics Committee**

Email: ethics@cs.ox.ac.uk.

Address:
Wolfson Building,
Parks Road, Oxford
OX1 3QD, UK

***Ethics review details:*** This research project has been reviewed and approved by an Oxford University ethics committee. Ethics Approval Reference: (CS_C1A_23_012). If, after contacting me with any concern, you're still unhappy and wish to make a formal complaint, please contact the ethics committee. Their email address ethics@cs.ox.ac.uk. Address: Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

- ***Data Protection statement****:* The University of Oxford is responsible overall for ensuring the safe and proper use of any personal information you provide, solely for research purposes. Further information about your rights to information you provide is available from the University's data protection web site (https://compliance.web.ox.ac.uk/individual-rights.
- ***Questions/concerns?*** Do you have any questions?

**2. Oral consent seeking stage, after participant has had sufficient time to think about whether s/he wants to take part. Record the participant response to below questions.**

- Do you give your permission for me to interview you and audio record you?
- Do you give permission for me to re-contact you to clarify information?
- Do you give me permission to quote you (using your pseudonym)?
- Are you happy to take part?

Ok, thanks, let's start.

# References


[1] Yaxing Yao et al. “Privacy Perceptions and Designs of Bystanders in Smart Homes”. en. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (May 2019), pp. 1–24. URL: https://dl.acm.org/doi/10.1145/3359161 (visited on 06/30/2022).

[2] Julia Bernd et al. “Smart Home Bystanders: Further Complexifying a Complex Context, CI Symposium, August 19–20, 2019, Berkeley, CA, USA”. en. In: (2019), p. 6.

[3] Razvan Nicolescu et al. *State of the Art in IoT - Beyond Economic Value. IoT UK: UX and service design for connected. DOI: 10.13140/RG.2.2.24165.45289.* Jan. 2018.

[4] Smart Home. *Homepage banner*. en. Jan. 2017. URL: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (visited on 04/08/2022).

[5] Danny Briere and Pat Hurley. *Smart Homes For Dummies® Amazon.com link for wide world of wireless products, and secure and protect your investment with an integrated security system*. English. Foster City, CA: John Wiley & Sons, May 1999.

[6] ICS. *ISO 9241-210:2019 Ergonomics of human-system interaction Part 210: Human-centred design for interactive systems*. en. 2019. URL: https://www.iso.org/standard/77520.html (visited on 03/06/2022).

[7] Julia Bernd et al. “Balancing Power Dynamics in Smart Homes: Nannies’ Perspectives on How Cameras Reflect and Affect Relationships”. en. In: (2022), p. 21.

[8] Fukiko IKEHATA. *<Special Feature "Toward New Studies on Islamic Moderate Trends">Aspiring to be a Leader of Moderation: A Study on Jordan’s Islamic Policy*. en. Mar. 2017. URL: https://doi.org/10.14989/225232 (visited on 07/01/2022).

[9] Wael Albayaydh and Ivan Flechais. “Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households”. en. In: 2023, pp. 4643–4659. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/albayaydh (visited on 08/24/2022).

[10] Wael S Albayaydh and Ivan Flechais. “Exploring Bystanders’ Privacy Concerns with Smart Homes in Jordan”. en. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–24. URL: https://dl.acm.org/doi/10.1145/3491102.3502097 (visited on 06/26/2022).

[11] Wael Albayaydh and Ivan Flechais. “"Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan”. en. In: *Proc. ACM Hum.-Comput. Interact., Vol. 1, No. CSCW* 1.Proc. ACM Hum.-Comput. Interact., Vol. 1, No. CSCW (2023). URL: https://dl.acm.org/doi/pdf/10.1145/3637353.

[12] Wael Albayaydh and Ivan Flechais. “Co-Designing a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape”. en. In: *USENIX Security* (2024).

[13] Britannica-Jordan. *Jordan | History, Population, Flag, Map, King, & Facts | Britannica*. 2020. URL: https://www.britannica.com/place/Jordan (visited on 10/28/2022).

[14] population Worldmeter. *Jordan Population (2022) - Worldometer*. 2020. URL: https://www.worldometers.info/world-population/jordan-population/ (visited on 10/28/2022).

[15] WsW. *Jordan Demographics Profile*. en. 2021. URL: https://www.indexmundi.com/jordan/demographics_profile.html (visited on 11/06/2022).

[16] Britannica. *Arab | Description, History, & Facts | Britannica*. en. 2020. URL: https://www.britannica.com/topic/Arab (visited on 09/06/2021).

[17] Britannica. *Bedouin | Definition, People, Customs, & Facts | Britannica*. 2022. URL: https://www.britannica.com/topic/Bedouin (visited on 10/22/2022).

[18] Britannica. *Arab-Israeli wars | History, Conflict, Causes, Summary, & Facts | Britannica*. 2020. URL: https://www.britannica.com/event/Arab-Israeli-wars (visited on 10/22/2022).

[19] Karasapan. *Syrian refugees in Jordan: A decade and counting*. en-US. 2022. URL: https://www.brookings.edu/articles/syrian-refugees-in-jordan-a-decade-and-counting/ (visited on 01/06/2022).

[20] Britannica-Cherkes. *Circassian | History & Description | Britannica*. 2020. URL: https://www.britannica.com/topic/Circassian (visited on 10/22/2022).

[21] Khlaif Gharaybeh. “General Socio-Demographic Characteristics of the Jordanian Society: A Study in Social Geography”. en. In: (2014), p. 10.

[22] Dr. Mohammad Husni Abumelhim. “Contextualizing Efforts at Increasing Socioeconomic Participation in the Context of Jordan”. en. In: *American International Journal of Social Science* 7.4 (2018). URL: http://www.aijssnet.com/journal/index/600 (visited on 10/24/2022).

[23] Diab M. Al-Badayneh. “Violence Against Women in Jordan”. en. In: *Journal of Family Violence* 27.5 (July 2012), pp. 369–379. URL: http://link.springer.com/10.1007/s10896-012-9429-1 (visited on 10/24/2022).

[24] Dallos. *Identity and opportunity: Asymmetrical household integration among the Lanoh, newly sedentary hunter-gatherers and forest collectors of Peninsular Malaysia*. 2003. URL: https://elibrary.ru/item.asp?id=8849614 (visited on 10/24/2022).

[25] Ranjan Ray. "Poverty and expenditure pattern of households in Pakistan and South Africa: a comparative study". en. In: *Journal of International Development* 12.2 (Mar. 2000), pp. 241–256. URL: https://onlinelibrary.wiley.com/doi/10.1002/(SICI)1099-1328(200003)12:2%3C241::AID-JID654%3E3.0.CO;2-G (visited on 11/16/2021).

[26] Jeffrey H. Cohen. "Migration, Remittances, and Household Strategies". en. In: *Annual Review of Anthropology* 40.1 (Oct. 2011), pp. 103–114. URL: https://www.annualreviews.org/doi/10.1146/annurev-anthro-081309-145851 (visited on 11/26/2021).

[27] Frederic S Lee. "Modeling the Economy as a Whole: An Integrative Approach". en. In: (2011).

[28] Mohammed M. Al-Garni. *The impact of family structure and family function factors on the deviant behaviors of high school students in Makkah City, Saudi Arabia*. en. 2000. URL: https://www.semanticscholar.org/paper/The-impact-of-family-structure-and-family-function-Al-Garni/2fdce6be6e4dec6e73e07a1b3070ee73c23ebb30 (visited on 11/06/2022).

[29] coe. *Jordan Cultural Routes of the Council of Europe - Cultural Routes - publi.coe.int*. en-GB. 2010. URL: https://www.coe.int/en/web/cultural-routes/jordan (visited on 02/12/2022).

[30] Yoav Alon. "THE TRIBAL SYSTEM IN THE FACE OF THE STATE-FORMATION PROCESS: MANDATORY TRANSJORDAN, 1921–46". en. In: *International Journal of Middle East Studies* 37.2 (May 2005), pp. 213–240. URL: http://www.journals.cambridge.org/abstract_S0020743805372047 (visited on 10/11/2022).

[31] Dale F. Eickelman. "Tribal «Belonging» Today Implications and Transformations". ar. In: *Omran For social sciences* 5.19 (2017), pp. 57–68. URL: https://omran.dohainstitute.org/en/issue019/Pages/art02.aspx (visited on 05/14/2022).

[32] Jessica Watkins. "SEEKING JUSTICE: TRIBAL DISPUTE RESOLUTION AND SOCIETAL TRANSFORMATION IN JORDAN". en. In: *International Journal of Middle East Studies* 46.1 (Feb. 2014), pp. 31–49. URL: https://www.cambridge.org/core/product/identifier/S002074381300127X/type/journal_article (visited on 10/11/2022).

[33] Richard T. Antoun. "CIVIL SOCIETY, TRIBAL PROCESS, AND CHANGE IN JORDAN: AN ANTHROPOLOGICAL VIEW". en. In: *International Journal of Middle East Studies* 32.4 (Nov. 2000), pp. 441–463. URL: https://www.cambridge.org/core/product/identifier/S0020743800021164/type/journal_article (visited on 10/11/2022).

[34] Mona AlMunajjed. *Women in Saudi Arabia today*. en. New York: St. Martin's Press, 1997.

[35] UN-Women. *Gender Discrimination in Jordan | UN Women – Jordan*. 2019. URL: https://jordan.unwomen.org/en/digital-library/publications/2019/irckhf (visited on 10/27/2022).

[36] UNDP, ed. *The next frontier: human development and the Anthropocene*. en. Human development report 2020. New York, NY: United Nations Development Programme, 2020.

[37] Muntaha Gharaibeh and Arwa Oweis. "Why Do Jordanian Women Stay in an Abusive Relationship: Implications for Health and Social Well-Being". en. In: *Journal of Nursing Scholarship* 41.4 (Dec. 2009), pp. 376–384. URL: https://onlinelibrary.wiley.com/doi/10.1111/j.1547-5069.2009.01305.x (visited on 07/09/2022).

[38] Gilles Privat. "A system-architecture viewpoint on smart networked devices". en. In: *Microelectronic Engineering* 54.1-2 (Dec. 2000), pp. 193–197. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167931700800702 (visited on 05/07/2022).

[39] Ebtihal Mahadeen. *Women and the Media in Jordan: Gender, Power, Resistance*. en. Gender, Sexualities and Culture in Asia. Singapore: Springer Singapore, 2022. URL: https://link.springer.com/10.1007/978-981-16-9344-1 (visited on 10/10/2022).

[40] Mary Kawar. *Gender and generation in household labor supply in Jordan*. en. Tech. rep. Population Council, 2000. URL: https://knowledgecommons.popcouncil.org/departments_sbsr-pgy/1526 (visited on 09/06/2022).

[41] Muhammad M. Haj-Yahia. "Can people's patriarchal ideology predict their beliefs about wife abuse? The case of Jordanian men". en. In: 33.5 (2005). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jcop.20068, pp. 545–567. (Visited on 05/07/2021).

[42] G. Jäschke. "George A. Lipsky : Saudi Arabia, its people, its society, its culture. New Haven: HRAF Press 1959. XI, 367 S. $ 7.00. (= Survey of World Cultures, Ed. Thomas Fitzsimmons, 4)". en. In: *Die Welt des Islams* 6.3 (Jan. 1961). Publisher: Brill Section: Die Welt des Islams, pp. 296–298. URL: https://brill.com/view/journals/wdi/6/3/article-p296_33.xml (visited on 09/06/2022).

[43] Judy Brink. "Saddeka Arebi, Women and Words in Saudi Arabia: The Politics of Literary Discourse (New York: Columbia University Press, 1994). Pp. 369." en. In: *International Journal of Middle East Studies* 27.3 (Aug. 1995). Publisher: Cambridge University Press, pp. 390–391. URL: https://www.cambridge.org/core/journals/international-journal-of-middle-east-studies/article/abs/saddeka-arebi-women-and-words-in-saudi-arabia-the-politics-of-literary-discourse-new-york-columbia-university-press-1994-pp-369/EC905FD4D53F498F866AAF776CBD0871 (visited on 03/16/2021).

[44] Wonders. *Jordan culture and traditions - Wonders Travel and Tourism*. 2020. URL: https://jordan-travel.com/jordan-culture-and-traditions/ (visited on 10/22/2022).

[45] Nathan Malkin et al. “"What Can't Data Be Used For?": Privacy Expectations about Smart TVs in the U.S.” en. In: *Proceedings 3rd European Workshop on Usable Security*. London, England: Internet Society, 2018. URL: https://www.ndss-symposium.org/wp-content/uploads/2018/06/eurousec2018_16_Malkin_paper.pdf (visited on 08/22/2022).

[46] jordanjo. *Culture of Jordan - history, people, traditions, women, beliefs, food, customs, family, social*. 2019. URL: https://www.everyculture.com/Ja-Ma/Jordan.html (visited on 10/22/2022).

[47] John S Badeau. “ISLAM AND THE MODERN MIDDLE EAST”. en. In: *FOREIGN AFFAIRS* (1959), p. 15.

[48] Norah Abokhodair et al. “Privacy and Social Media Use in the Arabian Gulf: Saudi Arabian & Qatari Traditional Values in the Digital World”. en. In: (2017). Publisher: The Journal of Web Science. URL: https://webscience-journal.net/webscience/article/view/38 (visited on 10/11/2022).

[49] ILO. *Jordan - Regulation No 90/2009 Of Domestic Workers, Cooks, Gardeners And Similar Categories.* 2009. URL: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=85397 (visited on 10/24/2022).

[50] Bunewsservic. *Abuse against migrant domestic workers in Jordan heightened during pandemic – Boston University News Service*. 2021. URL: https://bunewsservice.com/abuse-against-migrant-domestic-workers-in-jordan-heightened-during-pandemic/ (visited on 10/24/2022).

[51] Tamkeen. *Tamkeen for Legal Aid and Human Rights is an independent Jordanian non-governmental civil society organization*. en. 2019. URL: https://tamkeen-jo.org/en/publications (visited on 07/03/2022).

[52] ILO. *Jordan: Regulatory framework governing migrant workers.. Private sector workers vs domestic workers.* 2022. URL: https://www.ilo.org/beirut/projects/fairway/WCMS_776521/lang--en/index.html (visited on 10/24/2022).

[53] ILO. *Employers' perspectives towards domestic workers in Jordan: a qualitative study on attitudes, working conditions and the employment relationship*. 2015. URL: https://www.ilo.org/beirut/publications/WCMS_429584/lang--en/index.html (visited on 10/28/2022).

[54] Alan F Westin. “Privacy And Freedom”. en. In: (1968). URL: https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.

[55] Jan Holvast. “History of Privacy.” en. In: (2007). URL: https://link.springer.com/content/pdf/10.1007/978-3-642-03315-5_2.pdf.

[56] Daniel J Solove. “A Brief History of Information Privacy Law”. en. In: (2006). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271.

[57] E. L. Godkin. *Libel and Its Legal Remedy*. en. Dec. 1880. URL: https://www.theatlantic.com/magazine/archive/1880/12/libel-and-its-legal-remedy/632214/ (visited on 03/06/2023).

[58] Samuel Warren and Louis Brandeis. "The Right to Privacy". en. In: *Killing the Messenger*. Section: Killing the Messenger. Columbia University Press, May 2019, pp. 1–21. URL: https://www.degruyter.com/document/doi/10.7312/gold91730-002/html (visited on 09/06/2022).

[59] Richard A. Posner. *The Economics of Justice*. en. Google-Books-ID: CKEN0F07ChUC. Harvard University Press, Aug. 1983.

[60] bigelow. *What is Data Privacy? - Definition from TechTarget.com*. en. 2015. URL: https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy (visited on 03/06/2023).

[61] Alan F. Westin. "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I–The Current Impact of Surveillance on Privacy". en. In: *Columbia Law Review* 66.6 (June 1966), p. 1003. URL: https://www.jstor.org/stable/1120997?origin=crossref (visited on 09/06/2023).

[62] Irwin Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. en. Google-Books-ID: GLBPAAAAMAAJ. Brooks/Cole Publishing Company, 1975.

[63] Helen Nissenbaum. "A Contextual Approach to Privacy Online, Information Law Institute at New York University." en. In: *Daedalus* 140.4 (Oct. 2011), pp. 32–48. URL: https://direct.mit.edu/daed/article/140/4/32-48/26914 (visited on 08/22/2022).

[64] Ari Ezra Waldman. "Privacy as Trust: Sharing Personal Information in a Networked World". en. In: *UNIVERSITY OF MIAMI LAW REVIEW* 69 (2015). URL: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=3054&context=umlr.

[65] M.G. Michael and Katina Michael. "Uberveillance: Microchipping People and the Assault on Privacy". In: *Faculty of Informatics - Papers* 53 (Jan. 2009).

[66] A. Barth et al. "Privacy and contextual integrity: framework and applications". In: *2006 IEEE Symposium on Security and Privacy (S&P'06)*. ISSN: 2375-1207. May 2006, 15 pp.–198.

[67] ICO UK. *Data protection by design and default*. en. Publisher: ICO. Oct. 2022. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (visited on 04/06/2021).

[68] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Jan. 2009. URL: https://www.degruyter.com/document/doi/10.1515/9780804772891/html (visited on 08/22/2022).

[69] Igor Bilogrevic and Martin Ortlieb. “"If You Put All The Pieces Together...": Attitudes Towards Data Combination and Sharing Across Services and Companies”. en. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. San Jose California USA: ACM, May 2016, pp. 5215–5227. URL: https://dl.acm.org/doi/10.1145/2858036.2858432 (visited on 04/13/2022).

[70] Pardis Emami Naeini et al. “The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios”. en. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), pp. 1–26. URL: https://dl.acm.org/doi/10.1145/3274317 (visited on 04/13/2022).

[71] Pedro Giovanni Leon et al. “What matters to users?: factors that affect users’ willingness to share information with online advertisers”. en. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. Newcastle United Kingdom: ACM, July 2013, pp. 1–12. URL: https://dl.acm.org/doi/10.1145/2501604.2501611 (visited on 04/13/2022).

[72] Jialiu Lin et al. “Expectation and purpose: understanding users’ mental models of mobile app privacy through crowdsourcing”. en. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. Pittsburgh Pennsylvania: ACM, Sept. 2012, pp. 501–510. URL: https://dl.acm.org/doi/10.1145/2370216.2370290 (visited on 04/13/2022).

[73] Irina Shklovski et al. “Leakiness and creepiness in app space: perceptions of privacy and mobile app use”. en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Toronto Ontario Canada: ACM, Apr. 2014, pp. 2347–2356. URL: https://dl.acm.org/doi/10.1145/2556288.2557421 (visited on 04/13/2022).

[74] Blase Ur et al. “Smart, useful, scary, creepy: perceptions of online behavioral advertising”. en. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Washington, D.C.: ACM, July 2012, pp. 1–15. URL: https://dl.acm.org/doi/10.1145/2335356.2335362 (visited on 04/13/2022).

[75] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. “The Economics of Privacy”. en. In: *Journal of Economic Literature* 54.2 (June 2016), pp. 442–492. URL: https://pubs.aeaweb.org/doi/10.1257/jel.54.2.442 (visited on 04/13/2022).

[76] Spyros Kokolakis. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon | Elsevier Enhanced Reader*. en. 2017. (Visited on 02/03/2023).

[77] H. Jeff Smith, Tamara Dinev, and Heng Xu. “Information Privacy Research: An Interdisciplinary Review”. In: *MIS Quarterly* 35.4 (2011). Publisher: Management Information Systems Research Center, University of Minnesota, pp. 989–1015. URL: https://www.jstor.org/stable/41409970 (visited on 03/06/2022).

[78] Andy Crabtree, Peter Tolmie, and Will Knight. “Repacking ‘Privacy’ for a Networked World”. en. In: *Computer Supported Cooperative Work (CSCW)* 26.4-6 (Dec. 2017), pp. 453–488. URL: http://link.springer.com/10.1007/s10606-017-9276-y (visited on 11/26/2023).

[79] Paul Dourish and Genevieve Bell. “Divining a Digital Future”. en. In: (2011).

[80] Andy Crabtree and Richard Mortier. “Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control”. en. In: *SSRN Electronic Journal* (2016). URL: https://www.ssrn.com/abstract=2874312 (visited on 11/26/2023).

[81] Timo Jakobi et al. “Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility”. en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2.4 (Dec. 2018), pp. 1–28. URL: https://dl.acm.org/doi/10.1145/3287049 (visited on 11/26/2022).

[82] Peter Tolmie et al. “Making the home network at home: Digital housekeeping”. en. In: *ECSCW 2007*. Ed. by Liam J. Bannon et al. London: Springer London, 2007, pp. 331–350. URL: http://link.springer.com/10.1007/978-1-84800-031-5_18 (visited on 11/26/2023).

[83] Patrick Gage Kelley et al. “A "nutrition label" for privacy”. en. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View California USA: ACM, July 2009, pp. 1–12. URL: https://dl.acm.org/doi/10.1145/1572532.1572538 (visited on 01/06/2022).

[84] Pardis Emami-Naeini et al. “Exploring How Privacy and Security Factor into IoT Device Purchase Behavior”. en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Glasgow Scotland Uk: ACM, May 2019, pp. 1–12. URL: https://dl.acm.org/doi/10.1145/3290605.3300764 (visited on 07/06/2022).

[85] Decew. *DeCew, 1997 - Security Constructs*. 2007. URL: https://verdi.cs.ucl.ac.uk/constructDB/publications/decew-pursuit-1997.html (visited on 07/12/2021).

[86] Kieron O’Hara. “The Seven Veils of Privacy”. In: *IEEE Internet Computing* 20.2 (Mar. 2016). Conference Name: IEEE Internet Computing, pp. 86–91. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7436680.

[87] Priscilla M. Regan. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, 1995. URL: https://www.jstor.org/stable/10.5149/9780807864050_regan (visited on 02/10/2022).

[88] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius. “The European Union general data protection regulation: what it is and what it means”. en. In: 28.1 (Jan. 2019), pp. 65–98. URL: https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501 (visited on 07/01/2022).

[89] Yaxing Yao et al. “Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes”. en. In: Glasgow Scotland Uk: ACM, May 2019, pp. 1–12. URL: https://dl.acm.org/doi/10.1145/3290605.3300428 (visited on 04/27/2021).

[90] Noah Apthorpe et al. "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity". en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2.2 (July 2018), pp. 1–23. URL: https://dl.acm.org/doi/10.1145/3214262 (visited on 07/01/2022).

[91] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. "Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers". en. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), pp. 1–31. URL: https://dl.acm.org/doi/10.1145/3274371 (visited on 07/01/2022).

[92] Bert-Jaap Koops et al., eds. *Responsible Innovation 2*. en. Cham: Springer International Publishing, 2015. URL: http://link.springer.com/10.1007/978-3-319-17308-5 (visited on 09/10/2022).

[93] Jeroen van den hoven et al. *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*. Jan. 2014. 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.

[94] Karl Manheim and Lyric Kaplan. "Artificial Intelligence: Risks to Privacy and Democracy". en. In: 21 (2019).

[95] Tianqing Zhu and Philip S. Yu. "Applying Differential Privacy Mechanism in Artificial Intelligence". en. In: *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. Dallas, TX, USA: IEEE, July 2019, pp. 1601–1609. URL: https://ieeexplore.ieee.org/document/8885331/ (visited on 08/28/2022).

[96] Van Der B. J.J. Vlist et al. "Design semantics of connections in a smart home environment". English. In: *Creation and Design* 13.2 (2011), pp. 18–24. URL: https://research.tue.nl/en/publications/design-semantics-of-connections-in-a-smart-home-environment-2 (visited on 08/28/2022).

[97] Marc L. Resnick and Raquel Montania. "Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store". en. In: *International Journal of Human-Computer Interaction* 16.2 (Oct. 2003), pp. 211–234. URL: http://www.tandfonline.com/doi/abs/10.1207/S15327590IJHC1602_05 (visited on 02/12/2021).

[98] Mihai Nadin. "Semiotic Engineering – An Opportunity or an Opportunity Missed?" en. In: *Conversations Around Semiotic Engineering*. Ed. by Simone Diniz Junqueira Barbosa and Karin Breitman. Cham: Springer International Publishing, 2017, pp. 41–63. URL: http://link.springer.com/10.1007/978-3-319-56291-9_6 (visited on 08/28/2022).

[99] Bruno A. Chagas, David F. Redmiles, and Clarisse S. de Souza. "Observed Appropriation of IoT Technology: A Semiotic Account". en. In: *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*. Belém Brazil: ACM, Oct. 2018, pp. 1–10. URL: https://dl.acm.org/doi/10.1145/3274192.3274225 (visited on 07/02/2022).

[100] Open Data. *DATAPROTECT 97*. 2012. URL: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (visited on 01/06/2023).

[101] Lee A. Bygrave. "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements". en. In: *Oslo Law Review* 4.2 (Aug. 2017), pp. 105–120. URL: http://www.idunn.no/doi/10.18261/issn.2387-3299-2017-02-03 (visited on 09/06/2021).

[102] Ann Cavoukian. "Privacy by Design The 7 Foundational Principles. Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Ontario, Canada. Creation of a Global Privacy Standard." en. In: (2006). URL: https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf.

[103] Peter Carey. *Data Protection: A Practical Guide to UK and EU law*. English. 5th edition. Oxford, United Kingdom: Oxford University Press, May 2018. URL: https://www.amazon.co.uk/Data-Protection-Practical-Guide-law/dp/0198815417.

[104] Ann Cavoukian. "Privacy by Design in law, policy and practice : Privacy by Design". en. In: (2011). Publisher: desLibris. URL: https://policycommons.net/artifacts/1222006/privacy-by-design-in-law-policy-and-practice/1775082/ (visited on 09/04/2022).

[105] Jun Zhao et al. "'I make up a silly name': Understanding Children's Perception of Privacy Risks Online". en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Glasgow Scotland Uk: ACM, May 2019, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3290605.3300336 (visited on 03/11/2022).

[106] Priya Kumar et al. "Co-designing online privacy-related games and stories with children". en. In: *Proceedings of the 17th ACM Conference on Interaction Design and Children*. Trondheim Norway: ACM, June 2018, pp. 67–79. URL: https://dl.acm.org/doi/10.1145/3202185.3202735 (visited on 02/14/2022).

[107] Brenna McNally et al. "Co-designing mobile online safety applications with children: 2018 CHI Conference on Human Factors in Computing Systems, CHI 2018". In: *CHI 2018 - Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. Conference on Human Factors in Computing Systems - Proceedings (Apr. 2018). Publisher: Association for Computing Machinery. URL: http://www.scopus.com/inward/record.url?scp=85046950628&partnerID=8YFLogxK (visited on 01/26/2022).

[108] Ge wang. "'Treat me as your friend, not a number in your database': Co-designing with Children to Cope with Datafication Online". en. In: *ACM Computing Surveys* (Feb. 2023), p. 1122445.1122456. URL: https://ora.ox.ac.uk/objects/uuid:361767de-511d-4174-a548-97b1fc44d754/download_file?file_format=application%2Fpdf&safe_filename=Wang_et_al_2023_Treat_me_as.pdf&type_of_work=Conference+item (visited on 03/16/2021).

[109] Ge Wang et al. "Informing Age-Appropriate AI: Examining Principles and Practices of AI for Children". en. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–29. URL: https://dl.acm.org/doi/10.1145/3491102.3502057 (visited on 06/14/2022).

[110] Leon Cruickshank, Gemma Coupe, and Dee Hennessy. "Co-Design: Fundamental Issues and Guidelines for Designers: Beyond the Castle Case Study". en. In: *Swedish Design Research Journal* 10 (Dec. 2013), pp. 48–57. URL: https://svid.ep.liu.se/article/view/514 (visited on 03/23/2021).

[111] Atta Badii et al. "Holistic Privacy Impact Assessment Framework for Video Privacy Filtering Technologies". en. In: *Signal & Image Processing : An International Journal* 4.6 (Dec. 2013), pp. 13–32. URL: http://www.aircconline.com/sipij/V4N6/4613sipij02.pdf (visited on 05/23/2022).

[112] Chelsea-Joy Wardle et al. "Exploring Co-design with Breastfeeding Mothers". en. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Montreal QC Canada: ACM, Apr. 2018, pp. 1–12. URL: https://dl.acm.org/doi/10.1145/3173574.3174056 (visited on 05/26/2022).

[113] Tuck-Voon How et al. "Envisioning future cognitive telerehabilitation technologies: a co-design process with clinicians". en. In: *Disability and Rehabilitation: Assistive Technology* 12.3 (Apr. 2017), pp. 244–261. URL: https://www.tandfonline.com/doi/full/10.3109/17483107.2015.1129457 (visited on 08/14/2022).

[114] Emily McReynolds et al. "Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 5197–5207. URL: https://dl.acm.org/doi/10.1145/3025453.3025735 (visited on 08/23/2022).

[115] Max Van Kleek et al. "Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 5208–5220. URL: https://dl.acm.org/doi/10.1145/3025453.3025556 (visited on 03/23/2022).

[116] Noah Apthorpe et al. *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*. en. arXiv:1708.05044 [cs]. Aug. 2017. URL: http://arxiv.org/abs/1708.05044 (visited on 01/30/2023).

[117] Trisha Datta, Noah Apthorpe, and Nick Feamster. "A Developer-Friendly Library for Smart Home IoT Privacy-Preserving Traffic Obfuscation". en. In: *Proceedings of the 2018 Workshop on IoT Security and Privacy*. Budapest Hungary: ACM, Aug. 2018, pp. 43–48. URL: https://dl.acm.org/doi/10.1145/3229565.3229567 (visited on 06/17/2022).

[118] Kenji Yoshigoe et al. “Overcoming invasion of privacy in smart home environment with synthetic packet injection”. In: *2015 TRON Symposium (TRONSHOW)*. Dec. 2015, pp. 1–7.

[119] Junjue Wang et al. “Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework”. en. In: *ACM Transactions on Multimedia Computing, Communications, and Applications* 14.3s (June 2018), pp. 1–24. URL: https://dl.acm.org/doi/10.1145/3209659 (visited on 01/17/2022).

[120] Simon Moncrieff, Svetha Venkatesh, and Geoff West. “Dynamic Privacy in a Smart House Environment”. In: *2007 IEEE International Conference on Multimedia and Expo*. ISSN: 1945-788X. July 2007, pp. 2034–2037.

[121] Abdullahi Arabo, Ian Brown, and Fadi El-Mousa. “Privacy in the Age of Mobility and Smart Devices in Smart Homes. DOI: 10.1109/SocialCom-PASSAT.2012.108. 978-0-7695-4848-7/12 $26.00 © 2012 IEEE DOI 10.1109/SocialCom-PASSAT.2012.108”. In: (Sept. 2012). URL: https://www.researchgate.net/profile/Abdullahi-Arabo/publication/254934189_Privacy_in_the_Age_of_Mobility_and_Smart_Devices_in_Smart_Homes/links/5641b2b908aec448fa61bdff/Privacy-in-the-Age-of-Mobility-and-Smart-Devices-in-Smart-Homes.pdf.

[122] Antorweep Chakravorty, Tomasz Wlodarczyk, and Chunming Rong. “Privacy Preserving Data Analytics for Smart Homes”. In: *2013 IEEE Security and Privacy Workshops*. May 2013, pp. 23–27.

[123] Anupam Das et al. “Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice”. en. In: *IEEE Pervasive Computing* 17.3 (July 2018), pp. 35–46. URL: https://ieeexplore.ieee.org/document/8490188/ (visited on 10/02/2022).

[124] Huichen Lin and Neil W. Bergmann. “IoT Privacy and Security Challenges for Smart Home Environments”. en. In: *Information* 7.3 (Sept. 2016). Number: 3 Publisher: Multidisciplinary Digital Publishing Institute, p. 44. URL: https://www.mdpi.com/2078-2489/7/3/44 (visited on 02/17/2021).

[125] Jodi Forlizzi and Carl DiSalvo. “Service Robots in the Domestic Environment: A Study of the Roomba Vacuum in the Home”. en. In: (2006).

[126] Allison Woodruff et al. “Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences”. en. In: (2014).

[127] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. “"I don’t own the data": End User Perceptions of Smart Home Device Data Practices and Risks”. en. In: (2019).

[128] Nina Gerber et al. “FoxIT: enhancing mobile users’ privacy behavior by increasing knowledge and awareness”. en. In: *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. Orlando Florida USA: ACM, Dec. 2018, pp. 53–63. URL: https://dl.acm.org/doi/10.1145/3167996.3167999 (visited on 11/26/2022).

[129] William Seymour et al. "Informing the Design of Privacy-Empowering Tools for the Connected Home". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3313831.3376264 (visited on 03/24/2021).

[130] Lauren E. Willis. "Deception by Design". eng. In: *Harvard Journal of Law & Technology (Harvard JOLT)* 34.1 (2020), pp. 115–190. URL: https://heinonline.org/HOL/P?h=hein.journals/hjlt34&i=121 (visited on 02/03/2024).

[131] Arunesh Mathur et al. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites". en. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019), pp. 1–32. URL: https://dl.acm.org/doi/10.1145/3359183 (visited on 10/20/2022).

[132] Tziporah Stern and Nanda Kumar. "Improving privacy settings control in online social networks with a wheel interface". en. In: *Journal of the Association for Information Science and Technology* 65.3 (2014). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.22994, pp. 524–538. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.22994 (visited on 11/20/2021).

[133] Nicholas Vollmer. *Recital 32 EU General Data Protection Regulation (EU-GDPR)*. en. text. Publisher: SecureDataService. Apr. 2023. URL: https://www.privacy-regulation.eu/en/recital-32-GDPR.htm (visited on 01/02/2021).

[134] Nikhil Dhingra et al. "The default pull: An experimental demonstration of subtle default effects on preferences". en. In: *Judgment and Decision Making* 7.1 (Jan. 2012), pp. 69–76. URL: https://www.cambridge.org/core/product/identifier/S1930297500001844/type/journal_article (visited on 10/06/2021).

[135] Florian M Farke et al. "Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity". en. In: (2021).

[136] Silas Hsu et al. "Awareness, Navigation, and Use of Feed Control Settings Online". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3313831.3376583 (visited on 01/02/2022).

[137] Hana Habib and Lorrie Faith Cranor. "Evaluating the Usability of Privacy Choice Mechanisms". en. In: (2022).

[138] Alessandro Acquisti et al. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online". en. In: *ACM Computing Surveys* 50.3 (May 2018), pp. 1–41. URL: https://dl.acm.org/doi/10.1145/3054926 (visited on 01/02/2022).

[139] Heather Richter Lipford et al. "Understanding Privacy Settings in Facebook with an Audience View". en. In: (2008).

[140] Lynn Tsai et al. "TurtleGuard: Helping Android Users Apply Contextual Privacy Preferences". en. In: (2017).

[141] Sarah Pearman, Ellie Young, and Lorrie Faith Cranor. "User-friendly yet rarely read: A case study on the redesign of an online HIPAA authorization". en. In: *Proceedings on Privacy Enhancing Technologies* 2022.3 (July 2022), pp. 558–581. URL: https://petsymposium.org/popets/2022/popets-2022-0086.php (visited on 10/20/2022).

[142] Dr. Kenneth A. Kovach et al. "The Balance Between Employee Privacy And Employer Interests". en. In: *Business and Society Review* 105.2 (2000). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/0045-3609.00082, pp. 289–298. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/0045-3609.00082 (visited on 01/06/2022).

[143] Ilias Leontiadis et al. "Don't kill my ads!: balancing privacy in an ad-supported mobile application market". en. In: *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications - HotMobile '12*. San Diego, California: ACM Press, 2012, p. 1. URL: http://dl.acm.org/citation.cfm?doid=2162081.2162084 (visited on 11/20/2022).

[144] George Chalhoub and Ivan Flechais. "Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives". en. In: *Proceedings of the ACM on Human-Computer Interaction* 6.CSCW2 (Nov. 2022), pp. 1–36. URL: https://dl.acm.org/doi/10.1145/3555537 (visited on 02/01/2021).

[145] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. "Designing Effective Privacy Notices and Controls". In: *IEEE Internet Computing* 21.3 (May 2017). Conference Name: IEEE Internet Computing, pp. 70–77. URL: https://ieeexplore.ieee.org/abstract/document/7927931?casa_token=QILmM26QqLIAAAAA:4O9OImZkp4Nw0NazpSE1yUbVMgttbmqs7Gej-r7lEJWtIKQeGTEF-7SrHhC71eE4hyKYSgZL (visited on 02/12/2023).

[146] Mohammad Alafeef, Dalbir Singh -, and Kamsuriah Ahmad -. "Influence of Demographic Factors on the Adoption Level of Mobile Banking Applications in Jordan". In: *Journal of Convergence Information Technology* 6.12 (Dec. 2011), pp. 107–113. URL: http://www.aicit.org/jcit/global/paper_detail.html?jname=JCIT&q=909 (visited on 11/22/2022).

[147] Shaheen. *Clients Acceptance towards Mobile Banking Application in Jordan Based on TAM Mode*. 2021. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9464557 (visited on 06/23/2023).

[148] Sulieman Al-Hawary and Ahmad Obiadat. "Impact of Mobile Marketing on Customer Loyalty in Jordan". en. In: *International Journal of Web Applications* 11.4 (Dec. 2019), p. 136. URL: http://www.dline.info/ijwa/fulltext/v11n4/ijwav11n4_3.pdf (visited on 04/23/2023).

[149] Giovanni Iachello and Jason Hong. "End-User Privacy in Human-Computer Interaction". en. In: *Foundations and Trends® in Human-Computer Interaction* 1.1 (2007), pp. 1–137. URL: http://www.nowpublishers.com/article/Details/HCI-004 (visited on 05/09/2022).

[150] William Gaver et al. "Realizing a video environment: EuroPARC's RAVE system". en. In: *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '92*. Monterey, California, United States: ACM Press, 1992, pp. 27–35. URL: http://portal.acm.org/citation.cfm?doid=142750.142754 (visited on 04/09/2022).

[151] Michael J. Muller et al. "Privacy, anonymity and interpersonal competition issues identified during participatory design of project management groupware!" en. In: *ACM SIGCHI Bulletin* 23.1 (Jan. 1991), pp. 82–87. URL: https://dl.acm.org/doi/10.1145/122672.122693 (visited on 09/02/2022).

[152] Marc Langheinrich, Barry Brumitt, and Steven Shafer, eds. *Ubicomp 2001: ubiquitous computing: International Conference, Atlanta, Georgia, USA, September 30-October 2, 2001: proceedings*. en. Lecture notes in computer science 2201. Meeting Name: Ubicomp 2001. Berlin : New York: Springer, 2001.

[153] Alan D. Smith and Felix Offodile. "Information management of automatic data capture: an overview of technical developments". en. In: *Information Management & Computer Security* 10.3 (Aug. 2002), pp. 109–118. URL: https://www.emerald.com/insight/content/doi/10.1108/09685220210431863/full/html (visited on 07/05/2022).

[154] Donald A. Norman. *The Design of Everyday Things, revised and expanded edition*. English. 2nd revised and expanded ed edition. Cambridge, MA London: MIT Press, Dec. 2013. URL: https://www.amazon.co.uk/Design-Everyday-Things-MIT-Press/dp/0262525674.

[155] CARROLL. *Artifacts as psychological theories: the case of human-computer interaction: Behaviour & Information Technology: Vol 8, No 4*. 1989. URL: https://www.tandfonline.com/doi/abs/10.1080/01449298908914556 (visited on 10/25/2022).

[156] Paul Dourish and Ken Anderson. "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena". en. In: *Human-Computer Interaction* 21.3 (Sept. 2006), pp. 319–342. URL: http://www.tandfonline.com/doi/abs/10.1207/s15327051hci2103_2 (visited on 09/06/2021).

[157] Dix. *Human-computer Interaction - Alan Dix, Janet Finlay, Gregory D. Abowd, Russell Beale - Google Books*. 2019. URL: https://books.google.co.uk/books?hl=en&lr=&id=IuQxui8GHDcC&oi=fnd&pg=PR14&dq=Abowd+++human&ots=I57ezOEVZH&sig=StEktmxylyruJu1BkydX_tKCNJ8&redir_esc=y#v=onepage&q=Abowd%20%20%20human&f=false (visited on 10/25/2022).

[158] Donald Norman. "The Invisible Computer : Why Good Products Can Fail, the Personal Computer Is So Complex, and Information Appliances Are the Solution / D.A. Norman." In: (Jan. 1998).

[159] Karen Renaud, Basie Von Solms, and Rossouw Von Solms. "How does intellectual capital align with cyber security?" en. In: *Journal of Intellectual Capital* 20.5 (Sept. 2019). Publisher: Emerald Publishing Limited, pp. 621–641. URL: https://www.emerald.com/insight/content/doi/10.1108/JIC-04-2019-0079/full/html (visited on 09/02/2022).

[160] John Karat and IBM T J Watson. "User centered design". en. In: (1996). URL: https://dl.acm.org/doi/pdf/10.1145/234813.234814.

[161] Yee. *Aligning security and usability | IEEE Journals & Magazine | IEEE Xplore*. 2004. URL: https://ieeexplore.ieee.org/abstract/document/1341409 (visited on 10/25/2022).

[162] Chunlei Yang, Guiyun Tian, and Steve Ward. "Security systems of point-of-sales devices". en. In: *The International Journal of Advanced Manufacturing Technology* 34.7-8 (Sept. 2007), pp. 799–815. URL: http://link.springer.com/10.1007/s00170-006-0638-8 (visited on 08/05/2022).

[163] Lorrie Faith Cranor and Simson Garfinkel. *Security and Usability: Designing Secure Systems that People Can Use*. en. Google-Books-ID: wDVhy9EyEAEC. "O'Reilly Media, Inc.", Aug. 2005.

[164] Batya Friedman and Colby College. "Trust and Accountability: Preserving Human Values in Interactibnal Experience". en. In: (1998), p. 1.

[165] C. Geoffrey Weirich and Daniel P. Hart. "Protecting Trade Secrets and Confidential Information in Georgia". eng. In: *Mercer Law Review* 60.2 (2008), pp. 533–562. URL: https://heinonline.org/HOL/P?h=hein.journals/mercer60&i=539 (visited on 10/11/2022).

[166] olson. *A study of preferences for sharing and privacy | CHI '05 Extended Abstracts on Human Factors in Computing Systems*. 2005. URL: https://dl.acm.org/doi/abs/10.1145/1056808.1057073 (visited on 10/25/2022).

[167] M Angela Sasse and Ivan Flechais. "Why Do We Need It? How Do We Get It?" en. In: (2005). URL: https://discovery.ucl.ac.uk/id/eprint/20345/2/cransimpsonbook.pdf.

[168] inglesant. *The true cost of unusable password policies | Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2010. URL: https://dl.acm.org/doi/abs/10.1145/1753326.1753384 (visited on 10/25/2022).

[169] Kim Zetter. "WIKILEAKS FILES SHOW THE CIA REPURPOSING HACKING CODE TO SAVE TIME, NOT TO FRAME RUSSIA". en. In: (2017), p. 7.

[170] hunt. *Troy Hunt: What do Sony and Yahoo! have in common? Passwords!* 2012. URL: https://www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/ (visited on 10/25/2022).

[171] Schneier. *Secrets and Lies: Digital Security in a Networked World - Bruce Schneier - Google Books*. 2015. URL: https://books.google.co.uk/books?hl=en&lr=&id=OT6kBgAAQBAJ&oi=fnd&pg=PR9&dq=Schneier,+B.+(1996).+Applied+Cryptography.+New+York,+John+Wiley+%26+Sons.&ots=N5wZWHo-7O&sig=GXOtkW7weODbcWDl06z-t79i6kw&redir_esc=y#v=onepage&q&f=false (visited on 10/25/2022).

[172] Mark S Ackerman and Scott D Mainwaring. "Privacy Issues and Human-Computer Interaction". en. In: (2005). URL: http://scott.mainzone.com/pubs/05-privacy-issues-and-hci.pdf.

[173] Sommerville. *Software Documentation*. 2001. URL: http://www.literateprogramming.com/documentation.pdf (visited on 07/06/2022).

[174] williamson. *Calculativeness, Trust, and Economic Organization | The Journal of Law and Economics: Vol 36, No 1, Part 2*. 1993. URL: https://www.journals.uchicago.edu/doi/abs/10.1086/467284 (visited on 10/25/2022).

[175] Supriya Singh and Claudia Slegers. "Trust and Electronic Money. Centre for International Research on Communication and Information Technologies. Policy Research Paper no 42". en. In: (1997), p. 46.

[176] agre. *Technology and Privacy: The New Landscape - Google Books*. 1998. URL: https://books.google.co.uk/books?hl=en&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PP11&dq=Agre,+P.+(1998).+Introduction.+Technology+and+Privacy:+The+New+Landscape.+P.+Agre+and+M.+Rotenberg.+Cambridge,+Mass,+The+MIT+Press:+1-28.&ots=1YZkyd_sLp&sig=rCqHz90bZrVeIqiZqI9wA16GmzY&redir_esc=y#v=onepage&q&f=false (visited on 10/25/2022).

[177] Leysia Palen and Paul Dourish. "Unpacking "Privacy" for a Networked World. Ft. Lauderdale, Florida, USA. Privacy and Trust". en. In: *NEW HORIZONS* 5 (2003), p. 8. URL: https://dl.acm.org/doi/pdf/10.1145/642611.642635.

[178] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. "Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance," en. In: (2019), p. 14.

[179] Bart P. Knijnenburg et al., eds. *Modern Socio-Technical Perspectives on Privacy*. en. Cham: Springer International Publishing, 2022. URL: https://link.springer.com/10.1007/978-3-030-82786-1 (visited on 02/24/2023).

[180] Daricia Wilkinson et al. "Moving Beyond a "one-size fits all": Exploring Individual Differences in Privacy". en. In: *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. Montreal QC Canada: ACM, Apr. 2018, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3170427.3170617 (visited on 02/12/2022).

[181] Yao Li et al. "Cross-Cultural Privacy Prediction". en. In: *Proceedings on Privacy Enhancing Technologies* 2017.2 (Apr. 2017), pp. 113–132. URL: https://petsymposium.org/popets/2017/popets-2017-0019.php (visited on 04/08/2021).

[182] Geert H. Hofstede, Gert Jan Hofstede, and Michael Minkov. *Cultures and organizations: software of the mind: intercultural cooperation and its importance for survival*. en. 3rd ed. New York: McGraw-Hill, 2010.

[183] Syed Ishtiaque Ahmed et al. "Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh". en. In: *Proceedings of the ACM on Human-Computer Interaction* 1.CSCW (Dec. 2017), pp. 1–20. URL: https://dl.acm.org/doi/10.1145/3134652 (visited on 07/01/2022).

[184] Maryam Mustafa et al. "IslamicHCI: Designing with and within Muslim Populations". en. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3334480.3375151 (visited on 07/01/2022).

[185] Michael Lipka. *Muslims and Islam: Key findings in the U.S. and around the world*. en-US. 2017. URL: https://www.pewresearch.org/fact-tank/2017/08/09/muslims-and-islam-key-findings-in-the-u-s-and-around-the-world/ (visited on 02/01/2022).

[186] Muhammad Aslam Hayat. "Privacy and Islam: From the Quran to data protection in Pakistan". en. In: *Information & Communications Technology Law* 16.2 (June 2007), pp. 137–148. URL: http://www.tandfonline.com/doi/abs/10.1080/13600830701532043 (visited on 03/10/2022).

[187] Norita Md. Norwawi et al. "Promoting Islamic Ethics on Privacy in Digital Social Network for User Data Protection and Trust". en. In: *Ulūm Islāmiyyah Journal* 13 (2014), pp. 115–127. URL: http://Platform.almanhal.com/CrossRef/Preview/?ID=2-67320 (visited on 03/10/2022).

[188] Eric Zeng, Shrirang Mare, and Franziska Roesner. "End User Security & Privacy Concerns with Smart Homes". en. In: (Feb. 2017), p. 17. URL: https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf.

[189] Bako Ali and Ali Ismail Awad. "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes". en. In: *Sensors* 18.3 (Mar. 2018). Number: 3 Publisher: Multidisciplinary Digital Publishing Institute, p. 817. URL: https://www.mdpi.com/1424-8220/18/3/817 (visited on 02/01/2023).

[190] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. "Smart homes and their users: a systematic analysis and key challenges". en. In: *Personal and Ubiquitous Computing* 19.2 (Feb. 2015), pp. 463–476. URL: http://link.springer.com/10.1007/s00779-014-0813-0 (visited on 08/21/2022).

[191] Wilson. *Benefits and risks of smart home technologies | Elsevier Enhanced Reader*. en. 2017. URL: https://www.sciencedirect.com/science/article/pii/S030142151630711X (visited on 08/21/2022).

[192] Tousif Ahmed et al. "Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments". In: *IEEE Internet Computing* (2017). Conference Name: IEEE Internet Computing, pp. 1–1.

[193] Denys Brand et al. "A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities". en. In: *Behavior Analysis in Practice* 13.1 (Mar. 2020), pp. 11–21. URL: http://link.springer.com/10.1007/s40617-018-00329-y (visited on 02/11/2022).

[194] N Abdi, K M Ramokapane, and J M Such. "More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants". en. In: (2019).

[195] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. "Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks". en. In: Honolulu HI USA: ACM, Apr. 2020, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3313831.3376529 (visited on 08/21/2022).

[196] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. "Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things". In: *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. Calgary, AB: IEEE, Aug. 2017, pp. 181–18109. URL: https://ieeexplore.ieee.org/document/8476932/ (visited on 08/21/2022).

[197] Peter Worthy, Ben Matthews, and Stephen Viller. "Trust Me: Doubts and Concerns Living with the Internet of Things". en. In: Brisbane QLD Australia: ACM, June 2016, pp. 427–434. URL: https://dl.acm.org/doi/10.1145/2901790.2901890 (visited on 07/01/2022).

[198] Jenifer Sunrise Winter. "Citizen Perspectives on the Customization/Privacy Paradox Related to Smart Meter Implementation". en. In: *International Journal of Technoethics (IJT)* 6.1 (2015). Publisher: IGI Global, pp. 45–59. URL: https://www.igi-global.com/gateway/article/www.igi-global.com/gateway/article/124867 (visited on 02/10/2022).

[199] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. "Exploring Consumers' Attitudes of Smart TV Related Privacy Risks". en. In: ed. by Theo Tryfonas. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 656–674.

[200] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. "Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats". en. In: (2018), p. 4.

[201] J. SathishKumar and Dhiren R. Patel. "A Survey on Internet of Things: Security and Privacy Issues". en. In: *International Journal of Computer Applications* 90.11 (Mar. 2014), pp. 20–26. URL: http://research.ijcaonline.org/volume90/number11/pxc3894454.pdf (visited on 02/12/2022).

[202] Pardis Emami Naeini. *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 (visited on 10/26/2022).

[203] Timo Jakobi et al. "The Catch(es) with Smart Home: Experiences of a Living Lab Field Study". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 1620–1633. URL: https://dl.acm.org/doi/10.1145/3025453.3025799 (visited on 02/03/2022).

[204] M. Mikusz et al. "Raising Awareness of IoT Sensor Deployments". en. In: (Jan. 2018). Publisher: IET Digital Library, 9 (8 pp.)–9 (8 pp.) URL: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0009 (visited on 02/04/2022).

[205] Sabrina Karwatzki, Manuel Trenz, and Daniel Veit. "The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services". en. In: *Information Systems Journal* 32.6 (2022). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/isj.12386, pp. 1126–1157. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12386 (visited on 03/06/2022).

[206] Yaxing Yao et al. "Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 6777–6788. URL: https://dl.acm.org/doi/10.1145/3025453.3025907 (visited on 08/22/2022).

[207] Roberto Hoyle et al. "Privacy behaviors of lifeloggers using wearable cameras". en. In: Seattle Washington: ACM, Sept. 2014, pp. 571–582. URL: https://dl.acm.org/doi/10.1145/2632048.2632079 (visited on 02/10/2022).

[208] Haojian Jin et al. "Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, Apr. 2022, pp. 1–19. URL: https://doi.org/10.1145/3491102.3517602 (visited on 08/22/2022).

[209] Yaxing Yao et al. "Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 6789–6793. URL: https://dl.acm.org/doi/10.1145/3025453.3026049 (visited on 08/22/2022).

[210] Christine Geeng and Franziska Roesner. "Who's In Control?: Interactions In Multi-User Smart Homes". en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Glasgow Scotland Uk: ACM, May 2019, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3290605.3300498 (visited on 07/01/2022).

[211] Eric Zeng and Franziska Roesner. "Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study". en. In: (2017), p. 19. URL: https://www.usenix.org/system/files/sec19-zeng.pdf.

[212] Radhika Garg and Christopher Moreno. "Understanding Motivators, Constraints, and Practices of Sharing Internet of Things". en. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.2 (June 2019), pp. 1–21. URL: https://dl.acm.org/doi/10.1145/3328915 (visited on 02/01/2022).

[213] Yu Zhai et al. "A Survey Study of the Usefulness and Concerns about Smart Home Applications from the Human Perspective". en. In: *Open Journal of Social Sciences* 02.11 (2014), pp. 119–126. URL: http://www.scirp.org/journal/doi.aspx?DOI=10.4236/jss.2014.211017 (visited on 02/12/2021).

[214] Blase Ur, Jaeyeon Jung, and Stuart Schechter. "Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance". en. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. Seattle Washington: ACM, Sept. 2014, pp. 129–139. URL: https://dl.acm.org/doi/10.1145/2632048.2632107 (visited on 08/23/2022).

[215] Sarah Mennicken, David Kim, and Elaine May Huang. "Integrating the Smart Home into the Digital Calendar". en. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. San Jose California USA: ACM, May 2016, pp. 5958–5969. URL: https://dl.acm.org/doi/10.1145/2858036.2858168 (visited on 04/11/2021).

[216] Camille Cobb et al. "How Risky Are Real Users' IFTTT Applets?. USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9–11, 2020, Virtual Conference." en. In: (2020), p. 26. URL: https://www.usenix.org/system/files/soups2020-cobb.pdf.

[217] Noah Apthorpe et al. "You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships". en. In: *ACM Transactions on Internet of Things* (June 2022), p. 3539737. URL: https://dl.acm.org/doi/10.1145/3539737 (visited on 08/22/2022).

[218] Radhika Garg and Hua Cui. "Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies". en. In: *ACM Transactions on Computer-Human Interaction* 29.2 (Apr. 2022), pp. 1–30. URL: https://dl.acm.org/doi/10.1145/3485058 (visited on 08/22/2022).

[219] Vinay Koshy et al. ""We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes". en. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Yokohama Japan: ACM, May 2021, pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3411764.3445598 (visited on 08/23/2022).

[220] Martin J Kraemer, Ivan Flechais, and Helena Webb. "Exploring Communal Technology Use in the Home". en. In: Nottingham United Kingdom: ACM, Nov. 2019, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3363384.3363389 (visited on 07/01/2022).

[221] James Pierce, Richmond Y. Wong, and Nick Merrill. "Sensor Illumination: Exploring Design Qualities and Ethical Implications of Smart Cameras and Image/Video Analytics". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–19. URL: https://dl.acm.org/doi/10.1145/3313831.3376347 (visited on 08/23/2022).

[222] Franziska Roesner et al. "Augmented reality: hard problems of law and policy". en. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. Seattle Washington: ACM, Sept. 2014, pp. 1283–1288. URL: https://dl.acm.org/doi/10.1145/2638728.2641709 (visited on 07/01/2022).

[223] Rajib Dey et al. "Exploring Smart Home Device Use by Airbnb Hosts". en. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3334480.3382900 (visited on 08/23/2022).

[224] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. "Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts". en. In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (Apr. 2020), pp. 436–458. URL: https://petsymposium.org/popets/2020/popets-2020-0035.php (visited on 08/23/2022).

[225] Yunpeng Song et al. "I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3313831.3376585 (visited on 08/23/2022).

[226] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. "Owning and Sharing: Privacy Perceptions of Smart Speaker Users". en. In: *Proceedings of the ACM on Human-Computer Interaction* 5.CSCW1 (Apr. 2021), pp. 1–29. URL: https://dl.acm.org/doi/10.1145/3449119 (visited on 08/23/2022).

[227] Camille Cobb et al. ""I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users". en. In: *Proceedings on Privacy Enhancing Technologies* 2021.4 (Oct. 2021), pp. 54–75. URL: https://petsymposium.org/popets/2021/popets-2021-0060.php (visited on 01/03/2022).

[228] Karola Marky et al. ""You just can't know about everything": Privacy Perceptions of Smart Home Visitors". en. In: Essen Germany: ACM, Nov. 2020, pp. 83–95. URL: https://dl.acm.org/doi/10.1145/3428361.3428464 (visited on 11/22/2021).

[229] Mary Madden. "Opinion | The Devastating Consequences of Being Poor in the Digital Age". en-US. In: *The New York Times* (Apr. 2019). URL: https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html (visited on 02/11/2021).

[230] Oriana McDonough. "A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices". en. In: (2019).

[231] Karola Marky et al. ""I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments". en. In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. Tallinn Estonia: ACM, Oct. 2020, pp. 1–11. URL: https://dl.acm.org/doi/10.1145/3419249.3420164 (visited on 02/09/2021).

[232] Imtiaz Ahmad et al. "Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy". en. In: *Proceedings of the ACM on Human-Computer Interaction* 4.CSCW2 (Oct. 2020), pp. 1–28. URL: https://dl.acm.org/doi/10.1145/3415187 (visited on 11/22/2021).

[233] Mark Johnson et al. "Beyond the 'All Seeing Eye': Filipino Migrant Domestic Workers' Contestation of Care and Control in Hong Kong". en. In: *Ethnos* 85.2 (Mar. 2020), pp. 276–292. URL: https://www.tandfonline.com/doi/full/10.1080/00141844.2018.1545794 (visited on 08/23/2022).

[234] George Chalhoub and Ivan Flechais. ""Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users". en. In: *HCI for Cybersecurity, Privacy and Trust*. Ed. by Abbas Moallem. Vol. 12210. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 305–325. URL: http://link.springer.com/10.1007/978-3-030-50309-3_21 (visited on 12/01/2021).

[235] Deborah Lupton. "Self-tracking cultures: towards a sociology of personal informatics". en. In: Sydney New South Wales Australia: ACM, Dec. 2014, pp. 77–86. URL: https://dl.acm.org/doi/10.1145/2686612.2686623 (visited on 08/23/2022).

[236] Andrew Baerg1. "Big Data, Sport, and the Digital Divide: Theorizing How Athletes Might Respond to Big Data Monitoring". en. In: *Journal of Sport and Social Issues* 41.1 (Feb. 2017), pp. 3–20. URL: http://journals.sagepub.com/doi/10.1177/0193723516673409 (visited on 08/23/2022).

[237] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. "Facebook and privacy: it's complicated". en. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Washington, D.C.: ACM, July 2012, pp. 1–15. URL: https://dl.acm.org/doi/10.1145/2335356.2335369 (visited on 04/12/2022).

[238] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. "A study of privacy settings errors in an online social network". en. In: *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. Lugano, Switzerland: IEEE, Mar. 2012, pp. 340–345. URL: http://ieeexplore.ieee.org/document/6197507/ (visited on 07/03/2021).

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

[240] Alisa Frik et al. "Privacy and Security Threat Models and Mitigation Strategies of Older Adults. ISBN 978-1-939133-05-2, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11–13, 2019, Santa Clara, CA, USA." en. In: (2019).

[241] Alessandro Montanari et al. "Understanding the Privacy Design Space for Personal Connected Objects". en. In: July 2016. URL: https://scienceopen.com/document?vid=0bc0297a-df89-46b2-a5ca-ab6428ca3c78 (visited on 08/21/2022).

[242] Eun Kyoung Choe et al. "Investigating receptiveness to sensing and inference in the home using sensor proxies". en. In: Pittsburgh, Pennsylvania: ACM Press, 2012, p. 61. URL: http://dl.acm.org/citation.cfm?doid=2370216.2370226 (visited on 08/21/2022).

[243] John Vines et al. "Making family care work: dependence, privacy and remote home monitoring telecare systems". en. In: *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. Zurich Switzerland: ACM, Sept. 2013, pp. 607–616. URL: https://dl.acm.org/doi/10.1145/2493432.2493469 (visited on 02/11/2021).

[244] Loni Hagen. "Overcoming the Privacy Challenges of Wearable Devices: A Study on the Role of Digital Literacy". en. In: *Proceedings of the 18th Annual International Conference on Digital Government Research*. Staten Island NY USA: ACM, June 2017, pp. 598–599. URL: https://dl.acm.org/doi/10.1145/3085228.3085254 (visited on 08/23/2022).

[245] Scott R Peppet. "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent". en. In: *Texas Law Review* 93 (2014).

[246] Gianmarco Baldini et al. "Ethical Design in the Internet of Things". en. In: *Science and Engineering Ethics* 24.3 (June 2018), pp. 905–925. URL: http://link.springer.com/10.1007/s11948-016-9754-5 (visited on 07/01/2022).

[247] David Eckhoff and Isabel Wagner. "Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions". In: 20.1 (2018). Conference Name: IEEE Communications Surveys & Tutorials, pp. 489–516.

[248] Martin Krämer. "Disentangling Privacy in Smart Homes. Privacy. Computer Science Department, University of Oxford". en. In: (2019). URL: https://www.martin-kraemer.net/presentations/2018-10-cdt-showcase.pdf.

[249] Times Newyork. *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse (Published 2018)*. en. Section: Technology. June 2018. URL: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (visited on 02/10/2022).

[250] Roxanne Leitão. "Digital Technologies and their Role in Intimate Partner Violence". en. In: *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. Montreal QC Canada: ACM, Apr. 2018, pp. 1–6. URL: https://dl.acm.org/doi/10.1145/3170427.3180305 (visited on 02/11/2023).

[251] Marion Koelle, Matthias Kranz, and Andreas Möller. "Don't look at me that way!: Understanding User Attitudes Towards Data Glasses Usage". en. In: Copenhagen Denmark: ACM, Aug. 2015, pp. 362–372. URL: https://dl.acm.org/doi/10.1145/2785830.2785842 (visited on 02/10/2022).

[252] Sarah Pidcock et al. "NotiSense: An Urban Sensing Notification System To Improve Bystander Privacy". en. In: (2011), p. 5.

[253] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. "Security and Privacy Approaches in Mixed Reality: A Literature Survey". en. In: *ACM Computing Surveys* 52.6 (Nov. 2020), pp. 1–37. URL: https://dl.acm.org/doi/10.1145/3359626 (visited on 02/10/2022).

[254] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. "In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies". en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Toronto Ontario Canada: ACM, Apr. 2014, pp. 2377–2386. URL: https://dl.acm.org/doi/10.1145/2556288.2557352 (visited on 02/10/2022).

[255] Blaine A. Price et al. "Logging you, Logging me: A Replicable Study of Privacy and Sharing Behaviour in Groups of Visual Lifeloggers". en. In: 1.2 (June 2017), pp. 1–18. URL: https://dl.acm.org/doi/10.1145/3090087 (visited on 02/10/2022).

[256] Jennifer King. "Privacy, Disclosure, and Social Exchange Theory". English. ISBN: 9780438324954. Ph.D. United States – California: University of California, Berkeley, 2016. URL: https://www.proquest.com/docview/2102068508/abstract/63AF5B95B75D443DPQ/1 (visited on 08/22/2022).

[257] Peter J. Burke, ed. *Contemporary social psychological theories . Center for Internet and Society, Stanford Law School Andreas Katsanevas, Department of Communication, Stanford University*. en. Stanford, Calif: Stanford Social Sciences, 2006. URL: https://privaci.info/symposium2/papers_and_slides/King_Katsanevas.pdf.

[258] Sebastian Benthall and Bruce D Haynes. "Contexts are Political: Field Theory and Privacy. Association for Computing Machinery. ACM." en. In: (2019), p. 3. URL: https://privaci.info/symposium2/papers_and_slides/cifieldtheory.pdf.

[259] Martin J Kraemer, William Seymour, and Ivan Flechais. "Responsibility and Privacy: Caring for a Dependent in a Digital Age". en. In: (2019), p. 6.

[260] Lev Manovich. "Trending: The Promises and the Challenges of Big Social Data". en. In: *Debates in the Digital Humanities*. Ed. by Matthew K. Gold. University of Minnesota Press, Jan. 2012, pp. 460–475. URL: https://academic.oup.com/minnesota-scholarship-online/book/29340/chapter/243999993 (visited on 08/23/2022).

[261] Mark Andrejevic. "Big Data, Big Questions| The Big Data Divide. International Journal of Communication". en. In: (2014), p. 17. URL: https://ijoc.org/index.php/ijoc/article/view/2161.

[262] danah boyd danah and Kate Crawford. "CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon". en. In: *Information, Communication & Society* 15.5 (June 2012), pp. 662–679. URL: http://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878 (visited on 08/23/2022).

[263] Lee Rainie, Janna Anderson, and Elon University's. "Digital Life in 2025 The Future of Privacy. 202.419.4500 www.pewresearch.org". en. In: (2014), p. 77. URL: https://cryptome.org/2014/12/future-of-privacy.pdf.

[264] Laura Robinson and Brian K. Gran. "No Kid Is an Island: Privacy Scarcities and Digital Inequalities". en. In: *American Behavioral Scientist* 62.10 (Sept. 2018), pp. 1413–1430. URL: http://journals.sagepub.com/doi/10.1177/0002764218787014 (visited on 08/23/2022).

[265] Joseph Turow et al. "Divided We Feel: Partisan Politics Drive American's Emotions Regarding Surveillance of Low-Incom. e Populations. University of Pennsylvania". en. In: (2018), p. 33. URL: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1563&context=asc_papers.

[266] Myria Watkins Allen et al. "Workplace Surveillance and Managing Privacy Boundaries". en. In: 21.2 (July 2017), pp. 172–200. URL: http://journals.sagepub.com/doi/10.1177/0893318907306033 (visited on 08/23/2022).

[267] Kirstie Ball. "Workplace surveillance: an overview. Kirstie Ball (2010) Workplace surveillance: an overview, Labor History." en. In: *Labor History* 51.1 (Feb. 2010), pp. 87–106. (Visited on 08/23/2022).

[268] Samantha Lee and Brian H. Kleiner. "Electronic surveillance in the workplace". en. In: *Management Research News* 26.2/3/4 (Mar. 2003). Publisher: MCB UP Ltd, pp. 72–81. URL: https://www.emerald.com/insight/content/doi/10.1108/01409170310784014/full/html (visited on 08/23/2022).

[269] Clara Berridge, Jodi Halpern, and Karen Levy. "Cameras on beds: The ethics of surveillance in nursing home rooms". en. In: *AJOB Empirical Bioethics* 10.1 (Jan. 2019), pp. 55–62. URL: https://www.tandfonline.com/doi/full/10.1080/23294515.2019.1568320 (visited on 08/23/2022).

[270] Karen Levy, Lauren Kilgour, and Clara Berridge. "REGULATING PRIVACY IN PUBLIC/PRIVATE SPACE: THE CASE OF NURSING HOME MONITORING LAWS". en. In: 26 (2022), p. 43.

[271] Luke Stark and Karen Levy. "The surveillant consumer". en. In: *Media, Culture & Society* 40.8 (Nov. 2018), pp. 1202–1220. URL: http://journals.sagepub.com/doi/10.1177/0163443718781985 (visited on 08/23/2022).

[272] Stephen Neville. "Eavesmining: A Critical Audit of the Amazon Echo and Alexa Conditions of Use". en. In: *Surveillance & Society* 18.3 (Aug. 2020), pp. 343–356. URL: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13426 (visited on 09/06/2021).

[273] Mary Madden et al. "PRIVACY, POVERTY, AND BIG DATA: A MATRIX OF VULNERABILITIES FOR POOR AMERICANS". en. In: 95 (2017), p. 75. URL: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview.

[274] Diana Freed et al. ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology". en. In: Montreal QC Canada: ACM, Apr. 2018, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3173574.3174241 (visited on 08/24/2022).

[275] Tom Feltwell et al. "Broadening Exposure to Socio-Political Opinions via a Pushy Smart Home Device". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3313831.3376774 (visited on 03/06/2022).

[276] Jiahong Chen et al. "Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption". en. In: *International Data Privacy Law* 10.4 (2020). URL: https://academic.oup.com/idpl/article/10/4/279/5900395.

[277] William Seymour et al. "Strangers in the Room: Unpacking Perceptions of 'Smartness' and Related Ethical Concerns in the Home". en. In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. arXiv:2005.00284 [cs]. July 2020, pp. 841–854. URL: http://arxiv.org/abs/2005.00284 (visited on 09/06/2022).

[278] Mirzel Avdic et al. "Machine Body Language: Expressing a Smart Speaker's Activity with Intelligible Physical Motion". en. In: *Designing Interactive Systems Conference 2021*. Virtual Event USA: ACM, June 2021, pp. 1403–1418. URL: https://dl.acm.org/doi/10.1145/3461778.3462031 (visited on 01/15/2023).

[279] Neelima Sailaja et al. "The Living Room of the Future". en. In: *Proceedings of the 2019 ACM International Conference on Interactive Experiences for TV and Online Video*. Salford (Manchester) United Kingdom: ACM, June 2019, pp. 95–107. URL: https://dl.acm.org/doi/10.1145/3317697.3323360 (visited on 03/06/2022).

[280] Ann DeSmet et al. "Determinants of Self-Reported Bystander Behavior in Cyberbullying Incidents Amongst Adolescents". en. In: *Cyberpsychology, Behavior, and Social Networking* 17.4 (Apr. 2014), pp. 207–215. URL: http://www.liebertpub.com/doi/10.1089/cyber.2013.0027 (visited on 04/09/2022).

[281] Albert Bandura. "Social Cognitive Theory: An Agentic Perspective". In: *Annual Review of Psychology* 52.1 (2001). _eprint: https://doi.org/10.1146/annurev.psych.52.1.1, pp. 1–26. URL: https://doi.org/10.1146/annurev.psych.52.1.1 (visited on 01/06/2021).

[282] Albert Bandura. "Toward a Psychology of Human Agency: Pathways and Reflections". In: *Perspectives on Psychological Science* 13.2 (Mar. 2018). Publisher: SAGE Publications Inc, pp. 130–136. URL: https://doi.org/10.1177/1745691617699280 (visited on 03/06/2022).

[283] Roxanne Leitão. "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse". en. In: San Diego CA USA: ACM, June 2019, pp. 527–539. URL: https://dl.acm.org/doi/10.1145/3322276.3322366 (visited on 08/23/2022).

[284] Isabel Lopez-Neira et al. "'Internet of Things': How Abuse is Getting Smarter". en. In: *SSRN Electronic Journal* (2019). URL: https://www.ssrn.com/abstract=3350615 (visited on 08/23/2022).

[285] Ignacio Rodríguez-Rodríguez et al. "Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm". en. In: *Symmetry* 12.1 (Dec. 2019), p. 37. URL: https://www.mdpi.com/2073-8994/12/1/37 (visited on 08/23/2022).

[286] Simon Parkin et al. "Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse". en. In: *Proceedings of the New Security Paradigms Workshop*. San Carlos Costa Rica: ACM, Sept. 2019, pp. 1–15. URL: https://dl.acm.org/doi/10.1145/3368860.3368861 (visited on 08/23/2022).

[287] Kaiwen Sun et al. "Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies". en. In: *Proceedings of the ACM on Human-Computer Interaction* 5.CSCW2 (Oct. 2021), pp. 1–41. URL: https://dl.acm.org/doi/10.1145/3479858 (visited on 08/23/2022).

[288] Noah Apthorpe, Sarah Varghese, and Nick Feamster. "Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA". en. In: (Aug. 2017), p. 18.

[289] William Balmford, Larissa Hjorth, and Ingrid Richardson. "Supervised Play: Intimate Surveillance and Children's Mobile Media Usage". In: *The Routledge Companion to Digital Media and Children*. Num Pages: 10. Routledge, 2020.

[290] Tama Leaver. "Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online". en. In: *Social Media + Society* 3.2 (Apr. 2017), p. 205630511770719. URL: http://journals.sagepub.com/doi/10.1177/2056305117707192 (visited on 08/23/2022).

[291] Tian Liu et al. "Detecting Wireless Spy Cameras Via Stimulating and Probing". en. In: Munich Germany: ACM, June 2018, pp. 243–255. URL: https://dl.acm.org/doi/10.1145/3210240.3210332 (visited on 08/23/2022).

[292] Shwetak N. Patel, Jay W. Summet, and Khai N. Truong. "BlindSpot: Creating Capture-Resistant Spaces". en. In: *Protecting Privacy in Video Surveillance*. Ed. by Andrew Senior. London: Springer London, 2009, pp. 185–201. URL: http://link.springer.com/10.1007/978-1-84882-301-3_11 (visited on 08/24/2022).

[293] Anadi Chaman et al. "Ghostbuster: Detecting the Presence of Hidden Eavesdroppers". en. In: *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. New Delhi India: ACM, Oct. 2018, pp. 337–351. URL: https://dl.acm.org/doi/10.1145/3241539.3241580 (visited on 08/23/2022).

[294] Khai N. Truong et al. "Preventing Camera Recording by Designing a Capture-Resistant Environment". en. In: *UbiComp 2005: Ubiquitous Computing*. Ed. by David Hutchison et al. Vol. 3660. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 73–86. URL: http://link.springer.com/10.1007/11551201_5 (visited on 08/23/2022).

[295] Serge Egelman, Raghudeep Kannavara, and Richard Chow. "Is This Thing On?: Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms". en. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Seoul Republic of Korea: ACM, Apr. 2015, pp. 1669–1678. URL: https://dl.acm.org/doi/10.1145/2702123.2702251 (visited on 08/23/2022).

[296] Rebecca S. Portnoff et al. "Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights". en. In: Seoul Republic of Korea: ACM, Apr. 2015, pp. 1649–1658. URL: https://dl.acm.org/doi/10.1145/2702123.2702164 (visited on 08/23/2022).

[297] Parth Kirankumar Thakkar et al. ""It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes". en. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3491102.3502137 (visited on 08/23/2022).

[298] James Pierce et al. "Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras". en. In: *Designing Interactive Systems Conference*. Virtual Event Australia: ACM, June 2022, pp. 26–40. URL: https://dl.acm.org/doi/10.1145/3532106.3535195 (visited on 08/23/2022).

[299] Jeremy Schiff et al. "Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns". en. In: *Protecting Privacy in Video Surveillance*. Ed. by Andrew Senior. London: Springer London, 2009, pp. 65–89. URL: http://link.springer.com/10.1007/978-1-84882-301-3_5 (visited on 08/24/2022).

[300] Paarijaat Aditya et al. "I-Pic: A Platform for Privacy-Compliant Image Capture". en. In: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. Singapore Singapore: ACM, June 2016, pp. 235–248. URL: https://dl.acm.org/doi/10.1145/2906388.2906412 (visited on 08/23/2022).

[301] Till Ballendat, Nicolai Marquardt, and Saul Greenberg. "Proxemic interaction: designing for a proximity and orientation-aware environment". en. In: *ACM International Conference on Interactive Tabletops and Surfaces - ITS '10*. Saarbrücken, Germany: ACM Press, 2010, p. 121. URL: http://portal.acm.org/citation.cfm?doid=1936652.1936676 (visited on 08/24/2022).

[302] Carman Neustaedter and Saul Greenberg. "The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness". In: *UbiComp 2003: Ubiquitous Computing*. Ed. by Gerhard Goos et al. Vol. 2864. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 297–314. URL:

http://link.springer.com/10.1007/978-3-540-39653-6_24 (visited on 08/23/2022).

[303] Alfredo J. Perez, Sherali Zeadally, and Scott Griffith. "Bystanders' Privacy. 1520-9202/17/$33.00 © 2017 IEEE Published by the IEEE Computer Society computer.org/ITPro". In: *IT Professional* 19.3 (2017). Conference Name: IT Professional, pp. 61–65.

[304] Serena Zheng et al. "User Perceptions of Smart Home IoT Privacy". en. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), pp. 1–20. URL: https://dl.acm.org/doi/10.1145/3274469 (visited on 07/01/2022).

[305] Marion Koelle, Katrin Wolf, and Susanne Boll. "Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras". en. In: Stockholm Sweden: ACM, Mar. 2018, pp. 177–187. URL: https://dl.acm.org/doi/10.1145/3173225.3173234 (visited on 08/23/2022).

[306] Neilly H. Tan et al. "Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras". en. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–25. URL: https://dl.acm.org/doi/10.1145/3491102.3517617 (visited on 08/21/2022).

[307] Ray Jureidini. "Migrant Workers and Xenophobia in the Middle East". en. In: *Racism and Public Policy*. Ed. by Yusuf Bangura and Rodolfo Stavenhagen. London: Palgrave Macmillan UK, 2005, pp. 48–71. URL: http://link.springer.com/10.1057/9780230554986_3 (visited on 10/11/2022).

[308] Jenny K. Rodriguez and Maranda Ridgway. "Contextualizing privilege and disadvantage: Lessons from women expatriates in the Middle East". en. In: *Organization* 26.3 (May 2019), pp. 391–409. URL: http://journals.sagepub.com/doi/10.1177/1350508418812580 (visited on 10/09/2022).

[309] Elizabeth Frantz. "OF MAIDS AND MADAMS: Sri Lankan Domestic Workers and Their Employers in Jordan". en. In: *Critical Asian Studies* 40.4 (Dec. 2008), pp. 609–638. URL: http://www.tandfonline.com/doi/abs/10.1080/14672710802505323 (visited on 10/11/2022).

[310] Daphné Caillol. "The spatial dimension of agency: the everyday urban practices of Filipina domestic workers in Amman, Jordan". en. In: *Gender, Place & Culture* 25.5 (May 2018), pp. 645–665. URL: https://www.tandfonline.com/doi/full/10.1080/0966369X.2018.1472555 (visited on 10/19/2022).

[311] George Sami Naufal and Froilan Malit Jr. "Exploitation and the Decision to Migrate: The Role of Abuse and Unfavorable Working Conditions in Filipina Domestic Workers' Desire to Return Abroad". en. In: *SSRN Electronic Journal* (2018). URL: https://www.ssrn.com/abstract=3217495 (visited on 10/19/2022).

[312] Dr Amal Yousef Tal. "Female Migrant Domestic Workers, a Forgotten Segment of Forced Labor: Evidence from Jordan. Journal of Resources Development and Management www.iiste.org ISSN 2422-8397 An International Peer-reviewed Journal Vol.7". en. In: (2015), p. 6.

[313] Claudio Badii et al. "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects". In: *IEEE Access* 8 (2020). Conference Name: IEEE Access, pp. 23601–23623.

[314] Ilaria Torre et al. "A framework for personal data protection in the IoT". In: *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. Dec. 2016, pp. 384–391.

[315] Vijayaraghavan Varadharajan and Shruti Bansal. "Data Security and Privacy in the Internet of Things (IoT) Environment". en. In: *Connectivity Frameworks for Smart Devices* (2016). Publisher: Springer, Cham, pp. 261–281. URL: https://link.springer.com/chapter/10.1007/978-3-319-33124-9_11 (visited on 08/18/2022).

[316] Charith Perera et al. "Big Data Privacy in the Internet of Things Era". In: *IT Professional* 17.3 (May 2015). Conference Name: IT Professional, pp. 32–39.

[317] Abhik Chaudhuri. "Internet of things data protection and privacy in the era of the General Data Protection Regulation". In: *Journal of Data Protection & Privacy* 1.1 (Dec. 2016), pp. 64–75.

[318] Jahanzeb Shahid et al. "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)". en. In: *Applied Sciences* 12.4 (Feb. 2022), p. 1927. URL: https://www.mdpi.com/2076-3417/12/4/1927 (visited on 02/18/2022).

[319] Daniel Bastos et al. *GDPR Privacy Implications for the Internet of Things*. Dec. 2018.

[320] Irene Ioannidou and Nicolas Sklavos. "On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications". en. In: *Cryptography* 5.4 (Oct. 2021), p. 29. URL: https://www.mdpi.com/2410-387X/5/4/29 (visited on 11/18/2022).

[321] Masoud Barati et al. "GDPR Compliance Verification in Internet of Things". In: *IEEE Access* 8 (2020). Conference Name: IEEE Access, pp. 119697–119709.

[322] Bambang Pratama and Rachelia Jasmine. "Smart Home Appliances Regulation and Principles". en. In: *Proceedings of the 4th International Conference on Indonesian Legal Studies, ICILS 2021, June 8-9 2021, Semarang, Indonesia*. Semarang, Indonesia: EAI, 2022. URL: http://eudl.eu/doi/10.4108/eai.8-6-2021.2314344 (visited on 02/18/2022).

[323] B K Sovacool, D D Furszyfer Del Rio, and S Griffiths. "Policy mixes for more sustainable smart home technologies". en. In: *Environmental Research Letters* 16.5 (May 2021), p. 054073. URL: https://iopscience.iop.org/article/10.1088/1748-9326/abe90a (visited on 03/09/2022).

[324] Stephen Cousins. "The dark side of smart homes: What can they do with our data?" In: *Construction Research and Innovation* 9.1 (Jan. 2018). Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/20450249.2018.1440962, pp. 13–16. URL: https://doi.org/10.1080/20450249.2018.1440962 (visited on 02/18/2022).

[325] Colin J. Bennett. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. en. Google-Books-ID: D17pcdORb9UC. Cornell University Press, 1992.

[326] Thomas mname Hoppner and Anastasia mname Gubanova. "Regulatory Challenges of the Internet of Things". en. In: *SSRN Electronic Journal* (2015). URL: https://www.ssrn.com/abstract=3097113 (visited on 02/18/2023).

[327] FILIPPO PIEROZZI. *Data Power Europe GDPR Jurisdictional Reach and the bid for an international unilateral standard*. it. Dec. 2018. URL: https://dta.santannapisa.it/theses/available/etd-11192018-110828/unrestricted/Pierozzi_Filippo.pdf (visited on 02/23/2023).

[328] CNIL. *GDPR developer's guide | CNIL*. 2022. URL: https://www.cnil.fr/en/gdpr-developers-guide (visited on 02/24/2023).

[329] Colin J. Bennett. "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?" en. In: *Information Polity* 23.2 (June 2018). Ed. by Soon Ae Chun, Nabil R. Adam, and Beth Noveck, pp. 239–246. URL: https://www.medra.org/servlet/aliasResolver?alias=iospress&doi=10.3233/IP-180002 (visited on 02/24/2023).

[330] Skyflow. *How to Achieve Global Data Privacy Compliance in 2023 - Skyflow*. 2023. URL: https://www.skyflow.com/post/how-to-achieve-global-data-privacy-compliance (visited on 01/04/2024).

[331] Michele E Gilman. "Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice. University of Baltimore". en. In: (2020), p. 78. URL: https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=2111&context=all_fac.

[332] Victor Dahl and Marco Österlin. "Impact of GDPR on Data Sharing Behavior of Smart Home users:" en. In: (2020). URL: http://mau.diva-portal.org/smash/get/diva2:1480209/FULLTEXT01.pdf.

[333] Eoghan Furey and Juanita Blue. "Can I Trust Her? Intelligent Personal Assistants and GDPR". In: *2019 International Symposium on Networks, Computers and Communications (ISNCC)*. June 2019, pp. 1–6.

[334] Dean Ivancevic and David Randall. "Privacy and security of IoT. A smart home perspective. Faculty of Technology SE-391 82 Kalmar | SE-351 95 Växjö". en. In: (2020). URL: http://lnu.diva-portal.org/smash/get/diva2:1504361/FULLTEXT01.pdf.

[335] Lachlan Urquhart and Jiahong Chen. "On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity". en. In: (2020).

[336] Sahar Allegue, Mouna Rhahla, and Takoua Abdellatif. "Toward GDPR Compliance in IoT Systems". en. In: *Service-Oriented Computing – ICSOC 2019 Workshops*. Ed. by Sami Yangui et al. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 130–141.

[337] Daniel Anderson. "The GDPR and its impact on the Web". en. In: (2020). Medium: PDF Publisher: Chair of Network Architectures and Services, Department of Computer Science, Technical University of Munich. URL: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_01.pdf (visited on 02/13/2021).

[338] Dominique Machuletz and Rainer Böhme. "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR". en. In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (Apr. 2020), pp. 481–498. URL: https://petsymposium.org/popets/2020/popets-2020-0037.php (visited on 07/06/2021).

[339] Christoph Bösch et al. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns". en. In: *Proceedings on Privacy Enhancing Technologies* 2016.4 (Oct. 2016), pp. 237–254. URL: https://petsymposium.org/popets/2016/popets-2016-0038.php (visited on 07/04/2022).

[340] Gregory Conti and Edward Sobiesk. "Malicious interface design: exploiting the user". en. In: *Proceedings of the 19th international conference on World wide web*. Raleigh North Carolina USA: ACM, Apr. 2010, pp. 271–280. URL: https://dl.acm.org/doi/10.1145/1772690.1772719 (visited on 05/07/2021).

[341] Colin M. Gray et al. "The Dark (Patterns) Side of UX Design". en. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Montreal QC Canada: ACM, Apr. 2018, pp. 1–14. URL: https://dl.acm.org/doi/10.1145/3173574.3174108 (visited on 06/09/2022).

[342] Forbruker. *DECEIVED BY DESIGN*. 2018. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (visited on 08/04/2022).

[343] EDPS. *EDPS Opinion*. en. Jan. 2023. URL: https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf (visited on 05/07/2022).

[344] Natasha Singer. "When Websites Won't Take No for an Answer". en-US. In: *The New York Times* (May 2016). URL: https://www.nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html (visited on 07/09/2022).

[345] JAMES VINCENT. *California bans 'dark patterns' that trick users into giving away their personal data - The Verge*. Mar. 2021. URL: https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data (visited on 02/13/2022).

[346] Midas Nouwens et al. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". en. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu HI USA: ACM, Apr. 2020, pp. 1–13. URL: https://dl.acm.org/doi/10.1145/3313831.3376321 (visited on 02/13/2022).

[347] Michael Hintze. "Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR". en. In: *SSRN Electronic Journal* (2018). URL: https://www.ssrn.com/abstract=3192721 (visited on 04/14/2024).

[348] Goran Vojković, Melita Milenković, and Tihomir Katulić. "IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law". en. In: *Business Systems Research : International journal of the Society for Advancing Innovation and Research in Economy* 11.3 (Nov. 2020). Number: 3, pp. 167–185. URL: https://hrcak.srce.hr/ojs/index.php/bsr/article/view/12916 (visited on 04/14/2023).

[349] Michelle Goddard. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact". In: *International Journal of Market Research* 59.6 (Nov. 2017). Publisher: SAGE Publications, pp. 703–705. URL: https://doi.org/10.2501/IJMR-2017-050 (visited on 02/04/2022).

[350] Phuong le Pham. *The applicability of the GDPR to the Internet of Things*. en. Text. Publisher: Henry Stewart Publications. 2019. URL: https://www.ingentaconnect.com/content/hsp/jdpp/2019/00000002/00000003/art00008 (visited on 01/21/2022).

[351] Bea. *Why isn't household production included in GDP? | U.S. Bureau of Economic Analysis (BEA)*. 2018. URL: https://www.bea.gov/help/faq/1297 (visited on 03/05/2022).

[352] Intersoft-consulting. *Recital 18 - Not Applicable to Personal or Household Activities*. en-US. 2020. URL: https://gdpr-info.eu/recitals/no-18/ (visited on 03/05/2022).

[353] Stanislaw Piasecki. *Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons*. en. ISSN: 1360-0834. 2023. URL: https://www.tandfonline.com/doi/epdf/10.1080/13600834.2023.2231326?needAccess=true (visited on 04/14/2024).

[354] Michael L. Rustad. "How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices". eng. In: *Suffolk University Law Review* 52.2 (2019), pp. 227–272. URL: https://heinonline.org/HOL/P?h=hein.journals/sufflr52&i=260 (visited on 04/14/2024).

[355] Nadine Guhr et al. "Privacy concerns in the smart home context". en. In: *SN Applied Sciences* 2.2 (Feb. 2020), p. 247. URL: http://link.springer.com/10.1007/s42452-020-2025-8 (visited on 04/14/2024).

[356] Data Law Jordan. *Jordan issues first personal data protection law : Clyde & Co*. en. 2023. URL: https://www.clydeco.com:443/insights/2023/10/jordan-issues-first-personal-data-protection-law (visited on 11/14/2023).

[357] Marwa Fatafta and Dima Samaro. *Exposed and exploited: data protection in the Middle East and North Africa*. en. Report. Access Now, Jan. 2021. URL: https://apo.org.au/sites/default/files/resource-files/2021-01/apo-nid310911.pdf (visited on 02/18/2023).

[358] Dolores Cullen. "Data Protection: The New IP Frontier — An Overview of Existing Laws and Regulations". In: *Journal of Generic Medicines* 5.1 (Oct. 2007). Publisher: SAGE Publications, pp. 9–25. URL: https://doi.org/10.1057/palgrave.jgm.4950087 (visited on 02/18/2023).

[359] Samah A Massadeh. "Cloud Computing in Higher Education in Jordan. World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 3, No. 2, 38-43, 2013". en. In: (2013). URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=772ad5b3d92ea5340bb693e985a02ffbd1d6c7b1.

[360] Alaeldin Alkhasawneh. "The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do We Need to Comply with the GDPR?" eng. In: *Journal of Legal, Ethical and Regulatory Issues* 23.2 (2020), pp. 1–19. URL: https://heinonline.org/HOL/P?h=hein.journals/jnlolletl23&i=334 (visited on 09/06/2022).

[361] Reema A Karasneh et al. "Patient Data Sharing and Confidentiality Practices of Researchers in Jordan". In: *Risk Management and Healthcare Policy* 12 (Dec. 2019). Publisher: Dove Medical Press _eprint: https://www.tandfonline.com/doi/pdf/10.2147/RMHP.S227759, pp. 255–263. URL: https://www.tandfonline.com/doi/abs/10.2147/RMHP.S227759 (visited on 02/18/2023).

[362] Raed S A Faqir. "Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010". en. In: 7.1 (2013), p. 10.

[363] Dataguidance. *Jordan | DataGuidance*. 2020. URL: https://www.dataguidance.com/jurisdiction/jordan (visited on 12/01/2021).

[364] Sawsan Abo Alsondos. *Will the New Jordanian Law Protect Personal Data?* en-US. Section: News. Feb. 2022. URL: https://smex.org/will-the-new-jordanian-law-protect-personal-data/ (visited on 06/27/2022).

[365] Jordan MODEE. *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 (visited on 02/10/2022).

[366] Ashraf Alrai. *Study on the New Personal Data Protection Law*. ar. Section: -. Mar. 2024. URL: https://alghad.com/story/1657926 (visited on 03/23/2024).

[367] kuwait. *Law in Kuwait - DLA Piper Global Data Protection Laws of the World.* 2023. URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=KW (visited on 02/24/2023).

[368] iraq. *Iraq | DataGuidance*. 2023. URL: https://www.dataguidance.com/jurisdiction/iraq (visited on 02/24/2023).

[369] kuwait. "Privacy Laws & Business International Report 175". In: (2022). URL: https://accesspartnership.com/wp-content/uploads/2022/04/Kuwait-2.pdf.

[370] Egypt. *Data Protection Guide Egypt*. 2022. URL: https://www.multilaw.com/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Egypt.aspx (visited on 02/24/2023).

[371] MAGNiTT. *The world's most valuable resource is no longer oil, but data | MAGNiTT*. Sept. 2017. URL: https://magnitt.com/news/world%E2%80%99s-most-valuable-resource-no-longer-oil-data-21035 (visited on 02/12/2023).

[372] Marc van Lieshout. "The Value of Personal Data". en. In: *Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Springer, Cham, 2015, pp. 26–38. URL: https://link.springer.com/chapter/10.1007/978-3-319-18621-4_3 (visited on 03/06/2023).

[373] Columbia Law Review. *PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY*. en. 2014. URL: https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/ (visited on 03/06/2022).

[374] Philippe Petit. "Unlocking the Value of Personal Data: From Collection to Usage". en. In: (2013). URL: https://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

[375] Kenneth C Laudon. "Markets and privacy. Communication of the ACM September 1996/Vol. 39, No. 9". en. In: *COMMUNICATIONS OF THE ACM* 39.9 (1996). URL: https://dl.acm.org/doi/pdf/10.1145/234215.234476.

[376] Nicole Lindsey. *Personal Data Marketplaces Might Not Be the Best Solution for Data Privacy*. en-US. Apr. 2019. URL: https://www.cpomagazine.com/data-privacy/personal-data-marketplaces-might-not-be-the-best-solution-for-data-privacy/ (visited on 03/06/2021).

[377] Sarah Spiekermann et al. "The challenges of personal data markets and privacy". en. In: *Electronic Markets* 25.2 (June 2015), pp. 161–167. URL: http://link.springer.com/10.1007/s12525-015-0191-0 (visited on 01/06/2022).

[378] Ivan Stepanov. "Introducing a property right over data in the EU: the data producer's right – an evaluation". In: *International Review of Law, Computers & Technology* 34.1 (Jan. 2020). Publisher: Routledge _eprint: https://doi.org/10.1080/13600869.2019.1631621, pp. 65–86. URL: https://doi.org/10.1080/13600869.2019.1631621 (visited on 03/06/2023).

[379] Jeffrey Ritter and Anna Mayer. "REGULATING DATA AS PROPERTY". en. In: *TECHNOLOGY REVIEW* 16.1 (2017). URL: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1320&context=dltr.

[380] Mark MacCarthy. *Privacy Is Not A Property Right In Personal Information*. en. Section: Policy. 2018. URL: https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/ (visited on 03/06/2023).

[381] Cameron F. Kerry and John B. Morris. *Why data ownership is the wrong approach to protecting privacy*. en-US. June 2019. URL: https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/ (visited on 03/06/2023).

[382] OECD. *ACM: Digital Library: Communications of the ACM*. 2014. URL: https://dl.acm.org/doi/fullHtml/10.1145/2580944 (visited on 03/06/2023).

[383] Alessandro Acquisti, Leslie K. John, and George Loewenstein. "What Is Privacy Worth?" en. In: *The Journal of Legal Studies* 42.2 (June 2013), pp. 249–274. URL: https://www.journals.uchicago.edu/doi/10.1086/671754 (visited on 03/06/2021).

[384] Sören Preibusch. "The value of privacy in Web search". en. In: (2013). URL: https://econinfosec.org/archive/weis2013/papers/PreibuschWEIS2013.pdf.

[385] Tsogzolmaa Saizmaa and Hee-Cheol Kim. "A Holistic Understanding of HCI Perspectives on Smart Home". In: *2008 Fourth International Conference on Networked Computing and Advanced Information Management*. Vol. 2. Sept. 2008, pp. 59–65.

[386] Kujala. *User involvement: A review of the benefits and challenges*. en. 2010. URL: https://www.tandfonline.com/doi/epdf/10.1080/01449290301782?needAccess=true&role=button (visited on 03/09/2023).

[387] Silvia Ceccacci et al. "An user-centered approach to design smart systems for people with dementia". en. In: *2017 IEEE 7th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*. Berlin: IEEE, Sept. 2017, pp. 273–278. URL: http://ieeexplore.ieee.org/document/8210650/ (visited on 04/14/2024).

[388] H. J. Cha and M. L. Ahn. "Design and development of a smart-tool prototype to promote differentiated instruction: a user-centered design approach". EN. In: *Interactive Learning Environments* (Aug. 2020). Publisher: Routledge. URL: https://www.tandfonline.com/doi/full/10.1080/10494820.2018.1552871 (visited on 04/14/2024).

[389] Joseph Check. *Research Methods in Education*. 2011. URL: https://books.google.com/books/about/Research_Methods_in_Education.html?id=nSWYAAAAQBAJ (visited on 12/30/2021).

[390] Julie Ponto. "Understanding and Evaluating Survey Research". en. In: *Journal of the Advanced Practitioner in Oncology* 6.2 (Apr. 2015). Publisher: Harborside Press, p. 168. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4601897/ (visited on 10/21/2023).

[391] K. Kelley. "Good practice in the conduct and reporting of survey research". en. In: *International Journal for Quality in Health Care* 15.3 (May 2003), pp. 261–266. URL: https://academic.oup.com/intqhc/article-lookup/doi/10.1093/intqhc/mzg031 (visited on 12/30/2022).

[392] D.B Bromley. *The case-study method in psychology and related disciplines | WorldCat.org*. en. 1986. URL: https://search.worldcat.org/title/12235475 (visited on 12/30/2023).

[393] George R. Milne, Lauren I. Labrecque, and Cory Cromer. "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices". en. In: *Journal of Consumer Affairs* 43.3 (Sept. 2009). Publisher: John Wiley & Sons, Ltd, pp. 449–473. URL: https://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2009.01148.x (visited on 12/30/2022).

[394] Conklin Wm. Arthur. *Computer security behaviors of home PC users: A diffusion of innovation approach - ProQuest*. en. 2006. URL: https://www.proquest.com/docview/304915755/abstract/58E88C6108EE442APQ/1 (visited on 12/30/2023).

[395] Marilyn L. Taylor. *Unraveling the Mysteries of Case Study Research*. 2017. URL: https://books.google.com/books/about/Unraveling_the_Mysteries_of_Case_Study_R.html?id=a2EsDwAAQBAJ (visited on 12/30/2023).

[396] Geoff Rolls. *Classic case studies in psychology*. en. Fourth edition. Abingdon: Routledge, 2020.

[397] Robert K. Yin. *Case study research and applications*. Vol. 6. Sage Thousand Oaks, CA, 2018. URL: https://www.academia.edu/download/106905310/Artikel_Yustinus_Calvin_Gai_Mali.pdf (visited on 12/30/2023).

[398] Izak Benbasat. *The Case Research Strategy in Studies of Information Systems on JSTOR*. en. 1987. URL: https://www.jstor.org/stable/248684 (visited on 12/30/2021).

[399] Gideon Sjoberg, Anthony M. Orum, and Joe R. Feagin. *A Case for the Case Study*. English. The University of North Carolina Press, 2020. URL: https://muse.jhu.edu/book/77227 (visited on 12/30/2023).

[400] Norbert Nthala. "Home Data Security Decisions". en. In: (2019). URL: https:%20//ora.ox.ac.uk/objects/uuid:72401f07-d923-4448-af20-f99ecb677e3a (visited on 01/22/2021).

[401] Alan McIntosh. *Tools and Skills*. en-US. Pages: 1-112. Elsevier, Jan. 2017. URL: https://www.sciencedirect.com/science/article/pii/B9780128017128000019 (visited on 12/30/2023).

[402] Ben Shneiderman et al. *Designing the User Interface: Strategies for Effective Human-Computer Interaction, 6th Edition*. en. Pearson, 2016. URL: https://nsuworks.nova.edu/gscis_facbooks/18 (visited on 11/25/2022).

[403] Jonathan Lazar. *Research Methods in Human-Computer Interaction*. 2017. URL: https://books.google.com/books/about/Research_Methods_in_Human_Computer_Inter.html?id=hbkxDQAAQBAJ (visited on 03/14/2021).

[404] dictionary. *ETHNOGRAPHY Definition & Usage Examples | Dictionary.com*. 2021. URL: https://www.dictionary.com/browse/ethnography (visited on 12/30/2023).

[405] Mayukh Dewan. "Understanding Ethnography: An 'Exotic' Ethnographer's Perspective". en. In: *Asian Qualitative Research in Tourism*. ISSN: 2509-4211. Springer, Singapore, 2018, pp. 185–203. URL: https://link.springer.com/chapter/10.1007/978-981-10-7491-2_10 (visited on 12/30/2023).

[406] Scott Reeves, Ayelet Kuper, and Brian David Hodges. "Qualitative research methodologies: ethnography". en. In: *BMJ* 337 (Aug. 2008). Publisher: British Medical Journal Publishing Group Section: Practice. URL: https://www.bmj.com/content/337/bmj.a1020 (visited on 12/30/2023).

[407] Mike Allen. *The SAGE Encyclopedia of Communication Research Methods*. en. Google-Books-ID: 4GFCDgAAQBAJ. SAGE Publications, Apr. 2017.

[408] World Leaders in Research-Based User Experience. *Diary Studies: Understanding Long-Term User Behavior and Experiences*. en. 2016. URL: https://www.nngroup.com/articles/diary-studies/ (visited on 12/30/2022).

[409] Eiji Hayashi and Jason Hong. "A diary study of password usage in daily life". en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Vancouver BC Canada: ACM, May 2011, pp. 2627–2630. URL: https://dl.acm.org/doi/10.1145/1978942.1979326 (visited on 12/30/2022).

[410] Anselm Strauss and Juliet M. Corbin. *Grounded Theory in Practice*. en. Google-Books-ID: TtRMolAapBYC. SAGE, Mar. 1997.

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

[412] Johnny Saldana. "The Coding Manual for Qualitative Researchers". en. In: *The Coding Manual for Qualitative Researchers* (2021). Publisher: SAGE Publications Ltd, pp. 1–440. URL: https://www.torrossa.com/en/resources/an/5018667 (visited on 03/06/2023).

[413] Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. "Research on Interviewing Techniques". In: *Sociological Methodology* 12 (1981). Publisher: [American Sociological Association, Wiley, Sage Publications, Inc.], pp. 389–437. URL: https://www.jstor.org/stable/270748 (visited on 03/04/2023).

[414] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. en. Google-Books-ID: hZ6kBQAAQBAJ. SAGE Publications, Nov. 2014.

[415] Anne Adams and Martina Angela Sasse. "Users are not the enemy". en. In: *Communications of the ACM* 42.12 (Dec. 1999), pp. 40–46. URL: https://dl.acm.org/doi/10.1145/322796.322806 (visited on 09/08/2022).

[416] Corrine Glesne. "Becoming Qualitative Researchers: An Introduction, 5th Edition." en. In: *Pearson* (2016). ISBN: 9780133859393 Publisher: Pearson. One Lake Street, Upper Saddle River, New Jersey 07458. Tel: 800-848-9500; Web site: http://www.pearsoned.com/. URL: https://eric.ed.gov/?id=ED594812 (visited on 07/06/2021).

[417] David L. Morgan. *Focus Groups as Qualitative Research*. en. Google-Books-ID: LxF5CgAAQBAJ. SAGE Publications, Oct. 1996. URL: https://books.google.co.uk/books?hl=en&lr=&id=LxF5CgAAQBAJ&oi=fnd&pg=PT6&dq=Morgan,+1996).+%22Qualitative+research&ots=3uRnuUZVI1&sig=_Md1GmdyrgtFr_xKzU4SVjcsHfo#v=onepage&q=Morgan%2C%201996).%20%22Qualitative%20research&f=false.

[418] Diane Walker and Florence Myrick. "Grounded Theory: An Exploration of Process and Procedure". In: *Qualitative Health Research* 16.4 (Apr. 2006). Publisher: SAGE Publications Inc, pp. 547–559. URL: https://doi.org/10.1177/1049732305285972 (visited on 03/09/2023).

[419] Greg Guest, Arwen Bunce, and Laura Johnson. "How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability". In: *Field Methods* 18.1 (Feb. 2006). Publisher: SAGE Publications Inc, pp. 59–82. URL: https://doi.org/10.1177/1525822X05279903 (visited on 02/10/2023).

[420] Dave S. Collingridge and Edwin E. Gantt. "The Quality of Qualitative Research". In: *American Journal of Medical Quality* 23.5 (Sept. 2008). Publisher: SAGE Publications Inc, pp. 389–395. URL: https://doi.org/10.1177/1062860608320646 (visited on 02/10/2023).

[421] Virginia Braun and Victoria Clarke. "Thematic analysis". In: *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*. APA handbooks in psychology®. Washington, DC, US: American Psychological Association, 2012, pp. 57–71.

[422] Virginia Braun and Victoria Clarke. "Using thematic analysis in psychology". In: *Qualitative Research in Psychology* 3.2 (Jan. 2006). Publisher: Routledge _eprint: https://www.tandfonline.com/doi/pdf/10.1191/1478088706qp063oa, pp. 77–101. URL: https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa (visited on 04/03/2021).

[423] fca. "System Development". en. In: (2007). URL: https://www.fca.gov/template-fca/download/ITManual/itsystemsdevelopment.pdf (visited on 01/22/2021).

[424] Jay F. Nunamaker Jr, Minder Chen, and Titus D. M. Purdin. "Systems Development in Information Systems Research". EN. In: *Journal of Management Information Systems* (Dec. 1990). Publisher: Routledge. URL: https://www.tandfonline.com/doi/abs/10.1080/07421222.1990.11517898 (visited on 12/30/2023).

[425] Gillham. *Research Interviewing: The Range Of Techniques: A Practical Guide - Gillham, Bill - Google Books*. 2005. URL: https://books.google.co.uk/books?hl=en&lr=&id=fU_oAAAAQBAJ&oi=fnd&pg=PP1&dq=Gillham,+B.+(2005).+Research+interviewing:+the+range+of+techniques.+Maidenhead+%3B+New+York,+Open+University+Press.&ots=

BSxkeZFWkb&sig=V1AaotUttvv9kn9f7Ss_H1y3FTY#v=onepage&q&f=false (visited on 03/06/2023).

[426] Paul J. Lavrakas. *Encyclopedia of Survey Research Methods*. en. Google-Books-ID: Rhp1AwAAQBAJ. SAGE Publications, Sept. 2008. URL: https://books.google.co.uk/books?hl=en&lr=&id=Rhp1AwAAQBAJ&oi=fnd&pg=PP1&dq=Dialsingh,+I.+(2008).+Face-to-Face+Interviewing.+Encyclopedia+of+Survey+Research+Methods.+P.+Lavrakas,+SAGE.&ots=NUM3zYnLA9&sig=sKHgynEeUKRq1CZAl3kV8qxO4wY#v=onepage&q&f=false.

[427] Annie Irvine. "Realities Toolkit # Using phone interviews". en. In: (2010). URL: https://www.researchgate.net/publication/279372560_Using_phone_interviews.

[428] Kathy Charmaz. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. en. Google-Books-ID: 2ThdBAAAQBAJ. SAGE, Jan. 2006.

[429] Rubin. *SAGE Research Methods - Qualitative Interviewing (2nd ed.): The Art of Hearing Data*. 2005. URL: https://methods.sagepub.com/book/qualitative-interviewing (visited on 03/06/2023).

[430] Evelyn Folch-Lyon and John F. Trost. "Conducting Focus Group Sessions". In: *Studies in Family Planning* 12.12 (1981). Publisher: [Population Council, Wiley], pp. 443–449. URL: https://www.jstor.org/stable/1965656 (visited on 01/06/2024).

[431] Rosaline Barbour and Jenny Kitzinger. *Developing Focus Group Research: Politics, Theory and Practice*. en. Google-Books-ID: sDZbOLOQB9sC. SAGE, Dec. 1998.

[432] Michael Bloor et al. *Focus Groups in Social Research*. 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom: SAGE Publications Ltd, 2001. URL: https://methods.sagepub.com/book/focus-groups-in-social-research (visited on 03/06/2023).

[433] David L. Morgan, Richard A. Krueger, and Alice U. Scannell. *Planning Focus Groups*. en. Google-Books-ID: 6P7mdhtuzBEC. SAGE, 1998.

[434] Claudia Puchta and Jonathan Potter. *Focus Group Practice*. en. SAGE Publications Ltd, 2004. URL: https://methods.sagepub.com/book/focus-group-practice (visited on 02/03/2024).

[435] Jenny Kitzinger. "Qualitative Research: Introducing focus groups". en. In: *BMJ* 311.7000 (July 1995). Publisher: British Medical Journal Publishing Group Section: Education and debate, pp. 299–302. URL: https://www.bmj.com/content/311/7000/299 (visited on 03/06/2023).

[436] Martin Nils Amsteus. "The Validity of Divergent Grounded Theory Method". In: *International Journal of Qualitative Methods* 13.1 (Feb. 2014). Publisher: SAGE Publications Inc, pp. 71–87. URL: https://doi.org/10.1177/160940691401300133 (visited on 03/09/2023).

[437] Karsten Jonsen and Karen A. Jehn. "Using triangulation to validate themes in qualitative studies". en. In: 4.2 (Aug. 2009), pp. 123–150. URL: https://www.emerald.com/insight/content/doi/10.1108/17465640910978391/full/html (visited on 03/10/2022).

[438] Marry L. McHugh. "Interrater reliability: the kappa statistic". en. In: *Biochemia Medica* (2012), pp. 276–282. URL: http://www.biochemia-medica.com/en/journal/22/3/10.11613/BM.2012.031 (visited on 01/04/2023).

[439] Valentin Rousson, Theo Gasser, and Burkhardt Seifert. "Assessing intrarater, interrater and test–retest reliability of continuous measurements". en. In: *Statistics in Medicine* 21.22 (2002). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sim.1253, pp. 3431–3446. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/sim.1253 (visited on 04/09/2024).

[440] Rebecca S. Natow. "The use of triangulation in qualitative studies employing elite interviews". In: *Qualitative Research* 20.2 (Apr. 2020). Publisher: SAGE Publications, pp. 160–173. URL: https://doi.org/10.1177/1468794119830077 (visited on 04/09/2024).

[441] Violeta Lopez and Dean Whitehead. "Sampling data and data collection in qualitative research". en. In: (2012).

[442] Nancy Carter et al. "The Use of Triangulation in Qualitative Research". en. In: *Oncology Nursing Forum* 41.5 (Sept. 2014), pp. 545–547. URL: http://onf.ons.org/onf/41/5/use-triangulation-qualitative-research (visited on 01/21/2024).

[443] Leo A. Goodman. "Snowball Sampling". In: *The Annals of Mathematical Statistics* 32.1 (1961). Publisher: Institute of Mathematical Statistics, pp. 148–170. URL: https://www.jstor.org/stable/2237615 (visited on 02/10/2022).

[444] Christian Kraft. *User Experience Innovation: User Centered Design that Works*. en. Google-Books-ID: j7MnPwGrtqEC. Apress, June 2012.

[445] Rowland Atkinson and John Flint. "Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies". en. In: (2001). URL: https://sru.soc.surrey.ac.uk/SRU33.html.

[446] Warren D. TenHouten. "Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-reach Populations". en. In: *Bulletin of Sociological Methodology/Bulletin de Méthodologie Sociologique* 134.1 (Apr. 2017), pp. 58–61. URL: http://journals.sagepub.com/doi/10.1177/0759106317693790 (visited on 02/03/2023).

[447] Georgia Robins Sadler et al. "Research Article: Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy". en. In: *Nursing & Health Sciences* 12.3 (2010). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1442-2018.2010.00541.x, pp. 369–374. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1442-2018.2010.00541.x (visited on 02/10/2023).

[448] Jean Faugier and Mary Sargeant. "Sampling hard to reach populations". en. In: *Journal of Advanced Nursing* 26.4 (1997). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1046/j.1365-2648.1997.00371.x, pp. 790–797. URL: https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2648.1997.00371.x (visited on 02/10/2023).

[449] Guha. *Cooperative Inquiry revisited: Reflections of the past and guidelines for the future of intergenerational co-design | Elsevier Enhanced Reader*. 2013. (Visited on 03/23/2023).

[450] Elizabeth B.-N. Sanders and Pieter Jan Stappers. "Co-creation and the new landscapes of design". en. In: *CoDesign* 4.1 (Mar. 2008), pp. 5–18. URL: http://www.tandfonline.com/doi/abs/10.1080/15710880701875068 (visited on 03/23/2023).

[451] Mojtaba Vaismoradi, Hannele Turunen, and Terese Bondas. "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study". en. In: *Nursing & Health Sciences* 15.3 (Sept. 2013). Publisher: John Wiley & Sons, Ltd, pp. 398–405. URL: https://onlinelibrary.wiley.com/doi/10.1111/nhs.12048 (visited on 05/28/2023).

[452] Brad Wuetherick. "Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory". en. In: *Canadian Journal of University Continuing Education* 36.2 (Dec. 2010). Number: 2. URL: https://journals.library.ualberta.ca/cjuce-rcepu/index.php/cjuce-rcepu/article/view/9688 (visited on 03/06/2023).

[453] Chola Chhetri and Vivian Genaro Motti. "Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective". en. In: *Information in Contemporary Society*. Ed. by Natalie Greene Taylor et al. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 91–101.

[454] James W. Moore. "What Is the Sense of Agency and Why Does it Matter?" en. In: *Frontiers in Psychology* 7 (Aug. 2016). URL: http://journal.frontiersin.org/Article/10.3389/fpsyg.2016.01272/abstract (visited on 03/06/2023).

[455] Syed Ishtiaque Ahmed et al. "Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh". en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 906–918. URL: https://dl.acm.org/doi/10.1145/3025453.3025961 (visited on 11/27/2021).

[456] Labour Law Jordan. *Jordan's New Labour Law Amendments Impact the Employment Relationship*. en-US. 2019. URL: https://ogletree.com/international-employment-update/articles/november-2019/jordan/2019-10-28/jordans-new-labour-law-amendments-impact-the-employment-relationship/ (visited on 03/06/2023).

[457] Stuart E Dreyfus. *A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition*. en. Tech. rep. Section: Technical Reports. Feb. 1980. URL: https://apps.dtic.mil/sti/citations/ADA084551 (visited on 02/10/2023).

[458] Eddie Keane. "The GDPR and Employee's Privacy: Much Ado but Nothing New". en. In: *King's Law Journal* 29.3 (Sept. 2018), pp. 354–363. URL: https://www.tandfonline.com/doi/full/10.1080/09615768.2018.1555065 (visited on 02/10/2023).

[459] Winfried Veil. "The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law". en. In: (Dec. 2018). URL: https://papers.ssrn.com/abstract=3305056 (visited on 02/10/2023).

[460] Nicola Dell et al. ""Yours is better!": participant response bias in HCI". en. In: Austin Texas USA: ACM, May 2012, pp. 1321–1330. URL: https://dl.acm.org/doi/10.1145/2207676.2208589 (visited on 02/01/2023).

[461] Caitlin Wilson, Gillian Janes, and Julia Williams. "Identity, positionality and reflexivity: relevance and application to research paramedics". In: *British Paramedic Journal* 7.2 (Sept. 2022), pp. 43–49. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9662153/ (visited on 01/04/2023).

[462] B. K. Koskei and C. Simiyu. "Role of Interviews, Observation, Pitfalls and Ethical Issues in Qualitative Research Methods". In: *Journal of Educational Policy and Entrepreneurial Research* (Oct. 2015). URL: https://www.semanticscholar.org/paper/Role-of-Interviews%2C-Observation%2C-Pitfalls-and-in-Koskei-Simiyu/19036cfb1bf7ebab3ce2048bd18e53db7e76c2df (visited on 02/10/2023).

[463] Victor Jupp. *The SAGE Dictionary of Social Research Methods*. 1 Oliver's Yard, 55 City Road, London England EC1Y 1SP United Kingdom: SAGE Publications, Ltd, 2006. URL: https://methods.sagepub.com/reference/the-sage-dictionary-of-social-research-methods (visited on 02/10/2023).

[464] Trueman. *Structured Interviews - History Learning Site*. 2015. URL: https://www.historylearningsite.co.uk/sociology/research-methods-in-sociology/structured-interviews/ (visited on 02/12/2023).

[465] Anna Gorbacheva and Andrey Pestunov. "On freedom and slavery when using a smart device". en. In: *AI & SOCIETY* (Dec. 2022), s00146–022–01606–9. URL: https://link.springer.com/10.1007/s00146-022-01606-9 (visited on 02/06/2023).

[466] John Hagan, John Simpson, and A. R. Gillis. "Class in the Household: A Power-Control Theory of Gender and Delinquency". en. In: *American Journal of Sociology* (Jan. 1987). Publisher: University of Chicago Press. URL: https://www.journals.uchicago.edu/doi/10.1086/228583 (visited on 01/30/2023).

[467] L McGinn Kathleen and Ch2 Eunsil. *Gender, social class, and women's employment | Elsevier Enhanced Reader*. en. 2017. (Visited on 01/30/2023).

[468] Valentine M. Moghadam. "Patriarchy in Transition: Women and the Changing Family in the Middle East". en. In: *Journal of Comparative Family Studies* (Mar. 2019). Publisher: University of Toronto Press. URL: https://www.utpjournals.press/doi/10.3138/jcfs.35.2.137 (visited on 01/30/2023).

[469] Ebba Ourfali. "Comparison between Western and Middle Eastern Cultures: Research on Why American Expatriates Struggle in the Middle East". en. In: 13 (2015).

[470] Mohamed Benaida and M Arif. *Differences Between Arab World Culture and British Culture Based on Hofstede Dimensions and Their Impact on Web Design*. Apr. 2013.

[471] Peter Schaar. "Privacy by Design." en. In: *Identity in the Information Society* 3.2 (Aug. 2010), pp. 267–274. URL: http://link.springer.com/10.1007/s12394-010-0055-x (visited on 07/02/2022).

[472] Barrett Ens et al. "Candid Interaction: Revealing Hidden Mobile and Wearable Computing Activities". en. In: Charlotte NC USA: ACM, Nov. 2015, pp. 467–476. URL: https://dl.acm.org/doi/10.1145/2807442.2807449 (visited on 02/03/2023).

[473] Daqing Zhang, Tao Gu, and Xiaohang Wang. "Enabling Context-aware Smart Home with Semantic Web Technologies". en. In: (2005).

[474] Alexa Terms of Use Amazon Help & Customer Service. *Alexa Terms of Use - Amazon Customer Service*. Dec. 2021. URL: https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740 (visited on 02/11/2023).

[475] William Jang, Adil Chhabra, and Aarathi Prasad. "Enabling Multi-user Controls in Smart Home Devices". en. In: Dallas Texas USA: ACM, Nov. 2017, pp. 49–54. URL: https://dl.acm.org/doi/10.1145/3139937.3139941 (visited on 02/11/2022).

[476] Jaap-Henk Hoepman. "Privacy Design Strategies". en. In: ed. by Nora Cuppens-Boulahia et al. Vol. 428. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 446–459. URL: http://link.springer.com/10.1007/978-3-642-55415-5_38 (visited on 05/01/2023).

[477] Deepak Dhungana et al. "Aspern smart ICT: Data analytics and privacy challenges in a smart city". In: Dec. 2015, pp. 447–452.

[478] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. "On Privacy and Security Challenges in Smart Connected Homes". In: *2016 European Intelligence and Security Informatics Conference (EISIC)*. Aug. 2016, pp. 172–175.

[479] William Enck et al. "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones". en. In: *ACM Transactions on Computer Systems* 32.2 (June 2014), pp. 1–29. URL: https://dl.acm.org/doi/10.1145/2619091 (visited on 01/07/2022).

[480] Seda Gurses, Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design. K.U. Leuven/IBBT, ESAT/SCD-COSIC". en. In: (2007). URL: https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf (visited on 08/01/2022).

[481] Cynthia Dwork et al. "On the complexity of differentially private data release: efficient algorithms and hardness results". en. In: Bethesda MD USA: ACM, May 2009, pp. 381–390. URL: https://dl.acm.org/doi/10.1145/1536414.1536467 (visited on 05/01/2023).

[482] Sharan B. Merriam. *Qualitative Research and Case Study Applications in Education. Revised and Expanded from "Case Study Research in Education.".* en. 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. URL: https://eric.ed.gov/?id=ED415771 (visited on 03/06/2023).

[483] Alan Calder. *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 (visited on 02/10/2023).

[484] Data Bridge. *Middle East and Africa Smart Home Market Size, Scope, Growth, Analysis, & Forecast Trends By 2029*. Apr. 2022. URL: https://www.databridgemarketresearch.com/reports/middle-east-and-africa-smart-home-market (visited on 02/12/2023).

[485] Kathy Baxter, Catherine Courage, and Kelly Caine. *Understanding Your Users: A Practical Guide to User Research Methods*. en. Morgan Kaufmann, May 2015.

[486] Peter Birmingham. *Using Research Instruments : A Guide for Researchers. ISBN 0-203-42299-6 Master e-book ISBN*. en. Routledge, Dec. 2003. URL: https://www.taylorfrancis.com/books/mono/10.4324/9780203422991/using-research-instruments-peter-birmingham-david-wilkinson (visited on 02/10/2023).

[487] Christopher Harrold. *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 (visited on 02/12/2023).

[488] J. McCann, R. Hurford, and A. Martin. "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)*. ISSN: 2376-8541. Oct. 2005, pp. 70–77. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1550788.

[489] Alexey Pelykh. *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/ (visited on 02/12/2021).

[490] Michael Luchs and K. Scott Swan. "Perspective: The Emergence of Product Design as a Field of Marketing Inquiry*". en. In: *Journal of Product Innovation Management* 28.3 (2011). _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1540-5885.2011.00801.x, pp. 327–345. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-5885.2011.00801.x (visited on 03/06/2023).

[491] Anne Britt Torkildsby. "Critical Design in Universal Design Settings: Pedagogy turned upside down". en. In: (2018). URL: https://files.eric.ed.gov/fulltext/EJ1184352.pdf.

[492] ANIND K. DEY. "Context-Aware Computing". In: *Ubiquitous Computing Fundamentals*. Num Pages: 32. Chapman and Hall/CRC, 2009. URL: https://www.taylorfrancis.com/chapters/edit/10.1201/9781420093612-12/context-aware-computing-anind-dey.

[493] Anind K Dey et al. "An Architecture To Support Context-Aware Applications". en. In: (1999). URL: http://www.danielsalber.com/publications/gvu_99-23.pdf.

[494] Robert Sommer. *Design Awareness. ISBN-10 : 0030802989 ISBN-13 : 978-0030802980*. English. San Francisco: Rinehart Press, Jan. 1972. URL: https://www.amazon.com/Design-Awareness-R-Sommer/dp/0030802989.

[495] Dennis D. Hirsch. "The Glass House Effect: Big Data, the New Oil, and the Power of Analogy". In: *Maine Law Review* 66 (2013), p. 373. URL: https://heinonline.org/HOL/Page?handle=hein.journals/maine66&id=391&div=&collection=.

[496] Alessandro Acquisti. "Privacy in electronic commerce and the economics of immediate gratification". en. In: *Proceedings of the 5th ACM conference on Electronic commerce*. New York NY USA: ACM, May 2004, pp. 21–29. URL: https://dl.acm.org/doi/10.1145/988772.988777 (visited on 03/06/2022).

[497] Carrie Gates and Peter Matthews. "Data Is the New Currency". en. In: *Proceedings of the 2014 New Security Paradigms Workshop*. Victoria British Columbia Canada: ACM, Sept. 2014, pp. 105–116. URL: https://dl.acm.org/doi/10.1145/2683467.2683477 (visited on 02/13/2023).

[498] Charith Perera et al. "Designing privacy-aware internet of things applications". en. In: *Information Sciences* 512 (Feb. 2020), pp. 238–257. URL: https://linkinghub.elsevier.com/retrieve/pii/S0020025519309120 (visited on 02/11/2022).

[499] Jonathan Charity Talwana and Huang Jian Hua. "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)*. Dec. 2016, pp. 240–245.

[500] Rajendra Kumar Pandey and Mohit Misra. "Cyber security threats — Smart grid infrastructure". In: *2016 National Power Systems Conference (NPSC)*. Dec. 2016, pp. 1–6.

[501] A.J. Bernheim Brush et al. "Home automation in the wild: challenges and opportunities". en. In: Vancouver BC Canada: ACM, May 2011, pp. 2115–2124. URL: https://dl.acm.org/doi/10.1145/1978942.1979249 (visited on 07/01/2022).

[502] Enam Al-Wer. "Language and Gender in the Middle East and North Africa". en. In: *The Handbook of Language, Gender, and Sexuality*. Section: 20 _eprint: https://onlinelibrary.wiley.com/doi/pdf/. John Wiley & Sons, Ltd, 2014, pp. 396–411. URL: https://onlinelibrary.wiley.com/doi/abs/ (visited on 02/11/2023).

[503] Susan J Peters. "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". en. In: (2009).

[504] Shaddin Almasri. "The Political Economy of Nationality-Based Labor Inclusion Strategies: A Case Study of the Jordan Compact". In: *Middle East Critique* 30.2 (Apr. 2021). Publisher: Routledge _eprint: https://doi.org/10.1080/19436149.2021.1911459, pp. 185–203. URL: https://doi.org/10.1080/19436149.2021.1911459 (visited on 02/11/2023).

[505] Peter Scheuermann, Gerhard Weikum, and Peter Zabback. "Data partitioning and load balancing in parallel disk systems". en. In: *The VLDB Journal The International Journal on Very Large Data Bases* 7.1 (Feb. 1998), pp. 48–66. URL: http://link.springer.com/10.1007/s007780050053 (visited on 02/11/2023).

[506] Richmond Y. Wong and Deirdre K. Mulligan. "Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI". en. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Glasgow Scotland Uk: ACM, May 2019, pp. 1–17. URL: https://dl.acm.org/doi/10.1145/3290605.3300492 (visited on 01/15/2023).

[507] PbD GDPR. *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/ (visited on 02/07/2022).

[508] Ira S. Rubinstein and Nathaniel Good. "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents". In: *Berkeley Technology Law Journal* 28 (2013), p. 1333. URL: https://heinonline.org/HOL/Page?handle=hein.journals/berktech28&id=1367&div=&collection=.

[509] UKRI. *Framework for responsible innovation – UKRI*. 2022. URL: https://www.ukri.org/about-us/epsrc/our-policies-and-standards/framework-for-responsible-innovation/ (visited on 09/13/2022).

[510] Ethical Design Resources. *Ethical Design Resources*. 2022. URL: https://www.ethicaldesignresources.com/ (visited on 02/13/2023).

[511] Ethical Design Network. *Ethical Design Network*. en. 2022. URL: https://ethicaldesignnetwork.com/ (visited on 02/13/2023).

[512] ICO. *About this guidance*. en. Publisher: ICO. Oct. 2022. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/about-this-guidance/ (visited on 02/13/2023).

[513] The Wall Street Journal. *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 (visited on 02/13/2023).

[514] Rob Sobers. *A Year in the Life of the GDPR: Must-Know Stats and Takeaways*. en. 2020. URL: https://www.varonis.com/blog/gdpr-effect-review (visited on 02/13/2023).

[515] World Leaders in Research-Based User Experience. *Discount Usability for the Web: Article by Jakob Nielsen*. en. 1997. URL: https://www.nngroup.com/articles/web-discount-usability/ (visited on 02/13/2023).

[516] Lerone W. LaTouche. "Usability Issues in the User Interfaces of Privacy-Enhancing Technologies". en. ISBN: 9781303370267 Publication Title: ProQuest LLC ERIC Number: ED560349. PhD thesis. ProQuest LLC, 2013. (Visited on 02/13/2023).

[517] World Leaders in Research-Based User Experience. *Agile Development Projects and Usability*. en. Nov. 2008. URL: https://www.nngroup.com/articles/agile-development-and-usability/ (visited on 02/13/2023).

[518] Sevgi Arca and Rattikorn Hewett. "Privacy Protection in Smart Health". en. In: *Proceedings of the 11th International Conference on Advances in Information Technology*. Bangkok Thailand: ACM, July 2020, pp. 1–8. URL: https://dl.acm.org/doi/10.1145/3406601.3406620 (visited on 01/16/2023).

[519] Mohammad Razzaghi and Mariano Jr Ramirez. "The influence of the designers' own culture on the design aspects of products". English. In: Hochschule für Künste Bremen, 2005. URL: http://hdl.handle.net/1959.4/11576 (visited on 02/12/2023).

[520] Guy Julier. *The Culture of Design. Publisher SAGE, 2013 ISBN 144629692X, 9781446296929*. en. Google-Books-ID: _QdPAgAAQBAJ. SAGE, Dec. 2013.

[521] Geraldine Gay and Helene Hembrooke. *Activity-Centered Design: An Ecological Approach to Designing Smart Tools and Usable Systems*. en. Google-Books-ID: 5eRITE5tfvcC. MIT Press, Feb. 2004.

[522] Pablo A. Haya, Germán Montoro, and Xavier Alamán. "A Prototype of a Context-Based Architecture for Intelligent Home Environments". en. In: *On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE*. Springer, Berlin, Heidelberg, 2004, pp. 477–491. URL: https://link.springer.com/chapter/10.1007/978-3-540-30468-5_30 (visited on 02/11/2023).

[523] Lindsay McGregor and Neel Doshi. "How Company Culture Shapes Employee Motivation. Harvard business review". en. In: (Nov. 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.

[524] Claudio Dell'era and Roberto Verganti. "The impact of international designers on firm innovation capability and consumer interest". In: *International Journal of Operations & Production Management* 29.9 (Jan. 2009). Ed. by Nuran Acur and Chris Voss. Publisher: Emerald Group Publishing Limited, pp. 870–893. URL: https://doi.org/10.1108/01443570910986201 (visited on 02/13/2022).

[525] Bettina Von Stamm. "Whose Design is it? The Use of External Designers". en. In: *The Design Journal* 1.1 (Mar. 1998), pp. 41–53. URL: https://www.tandfonline.com/doi/full/10.2752/146069298790225235 (visited on 02/13/2023).

[526] Tekla S. Perry. "How Small Firms Innovate: Designing a Culture for Creativity". en. In: *Research-Technology Management* 38.2 (Mar. 1995), pp. 14–17. URL: https://www.tandfonline.com/doi/full/10.1080/08956308.1995.11671678 (visited on 02/13/2023).

[527] Hatchd. *Design | The dangers of dishonest design*. en-AU. 2017. URL: https://www.hatchd.com.au/blog/the-dangers-of-dishonest-design (visited on 02/13/2023).

[528] Kyle Gawley. *Dark Patterns - The Art of Online Deception*. Apr. 2013. URL: https://blog.kylegawley.com/dark-patterns-the-art-of-online-deception/ (visited on 02/13/2023).

[529] Greg Bensinger. "Opinion | Stopping the Manipulation Machines". en-US. In: *The New York Times* (Apr. 2021). URL: https://www.nytimes.com/2021/04/30/opinion/dark-pattern-internet-ecommerce-regulation.html (visited on 02/13/2022).

[530] Flavio Lamenza. *Stop calling these Dark Design Patterns or Dark UX — these are simply a**hole designs*. en. June 2020. URL: https://uxdesign.cc/stop-calling-these-dark-design-patterns-or-dark-ux-these-are-simply-asshole-designs-bb02df378ba (visited on 02/13/2023).

[531] Agarzola. *Going Dark: The Ethical Implications of Willfully Dishonest Design*. en. Sept. 2018. URL: https://events.drupal.org/seattle2019/sessions/going-dark-ethical-implications-willfully-dishonest-design (visited on 02/13/2023).

[532] Kristina Milanovic. "Smart Home Security: How Safe is Your Data? [Opinion]". In: *IEEE Technology and Society Magazine* 39.1 (Mar. 2020). Conference Name: IEEE Technology and Society Magazine, pp. 26–29.

[533] Cindy Dampier. *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 (visited on 02/13/2023).

[534] Sebastian Rieger and Caroline Sinders. "Dark Patterns: Regulating Digital Design". en. In: (2020).

[535] Sandra J. *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/ (visited on 02/13/2023).

[536] Marketing Week. *How losing trust costs brands customers – and what marketers can do to prevent it*. en. Nov. 2021. URL: https://www.marketingweek.com/losing-trust-costs-brands-customers/ (visited on 02/13/2023).

[537] Greg Petro. *Amazon's Crisis Of Trust*. en. Section: Investing. Mar. 2019. URL: https://www.forbes.com/sites/gregpetro/2019/03/08/amazons-crisis-of-trust/ (visited on 02/13/2023).

[538] Tim Ventura. *Google's Crisis of Trust Is Damaging Its Reputation*. en. Dec. 2019. URL: https://medium.com/swlh/googles-crisis-of-trust-is-damaging-its-reputation-3d5ab1b8430e (visited on 02/13/2023).

[539] Amazon (Alexa). *Design for International Markets | Alexa Design Guide*. en-US. Feb. 2021. URL: https://developer.amazon.com/en-US/docs/alexa/alexa-design/internationalization.html (visited on 02/13/2023).

[540] Google. *Leveraging content localization to reach new audiences*. ar. 2020. URL: https://adsense.google.com/intl/ar_jo/start/resources/localizing-your-content-can-help/ (visited on 02/13/2023).

[541] Apple Inc. *Localize your SwiftUI app - WWDC21 - Videos*. en. 2022. URL: https://developer.apple.com/videos/play/wwdc2021/10220/ (visited on 02/13/2023).

[542] Apple. *Change Siri voice or language*. en. Feb. 2022. URL: https://support.apple.com/en-us/HT208316 (visited on 02/13/2023).

[543] Larry Hardesty. *How Alexa learned Arabic*. en. Section: News and features. Jan. 2022. URL: https://www.amazon.science/latest-news/how-alexa-learned-arabic (visited on 02/13/2023).

[544] Silicon Labs. *Matter Standard Aligns the Smart Home Market - Silicon Labs*. en. 2022. URL: https://www.silabs.com/applications/matter-standard-aligns-the-smart-home-market (visited on 02/13/2022).

[545] OpenSystems Media. *Matter Standard – the Future of Smart Home Design*. en. Mar. 2022. URL: https://embeddedcomputing.com/application/consumer/smart-home-tech/matter-standard-the-future-of-smart-home-design (visited on 02/13/2023).

[546] Project CHOIP. *Project Connected Home Over IP*. en-US. Dec. 2019. URL: https://developer.amazon.com/en-US/alexa/devices/project-chip.html (visited on 02/13/2023).

[547] Anuroop Gaddam, Subhas Chandra Mukhopadhyay, and Gourab Sen Gupta. "Trial & experimentation of a smart home monitoring system for elderly". In: *2011 IEEE International Instrumentation and Measurement Technology Conference*. ISSN: 1091-5281. May 2011, pp. 1–6.

[548] Ngu Phuc Huy and Do vanThanh. "Evaluation of mobile app paradigms". en. In: *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM '12*. Bali, Indonesia: ACM Press, 2012, p. 25. URL: http://dl.acm.org/citation.cfm?doid=2428955.2428968 (visited on 03/23/2023).

[549] H. Russell Bernard and Harvey Russell Bernard. *Social Research Methods: Qualitative and Quantitative Approaches*. en. Google-Books-ID: 7sZHuhyzBNQC. SAGE, 2013.

[550] Galit Botzer and Michal Yerushalmy. "MOBILE APPLICATION FOR MOBILE LEARNING". en. In: (2007).

[551] Mark Anthony Camilleri and Adriana Caterina Camilleri. "THE TECHNOLOGY ACCEPTANCE OF MOBILE APPLICATIONS IN EDUCATION". en. In: (2017).

[552] Gary A. Klein. *Sources of Power, 20th Anniversary Edition: How People Make Decisions*. en. Google-Books-ID: JW01DwAAQBAJ. MIT Press, Sept. 2017.

[553] Rebecca E. Zietlow. "Slavery, Liberty, and the Right to Contract". eng. In: *Nevada Law Journal* 19.2 (2018), pp. 447–478. URL: https://heinonline.org/HOL/P?h=hein.journals/nevlj19&i=447 (visited on 08/08/2023).

[554] Rochell R. McWhorter and Elisabeth E. Bennett. *Creepy Technologies and the Privacy Issues of Invasive Technologies*. en. Chap. ISBN: 9781799829140 Pages: 243-268 Publisher: IGI Global. 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 (visited on 02/12/2023).

[555] Ezlo. *Platform - Ezlo - Property Empowered*. 2022. URL: https://www.ezlo.com/platform/ (visited on 09/06/2023).

[556] pc. *Wink Hub 2 Review | PCMag*. 2022. URL: https://www.pcmag.com/reviews/wink-hub-2 (visited on 07/01/2022).

[557] R. Lutolf. "Smart Home concept and the integration of energy meters into a home based system". In: *Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply 1992*. Nov. 1992, pp. 277–278.

[558] Berlo. *Design Guidelines on Smart Homes: A COST 219bis Guidebook*. en. Google-Books-ID: k60HGwAACAAJ. COST, European Co-Operation in the Field of Scientific and Technical Research, 1999.

[559] Lalatendu Satpathy. "Smart Housing: Technology to Aid Aging in Place - New Opportunities and Challenges". en. In: (2006). URL: https://scholarsjunction.msstate.edu/cgi/viewcontent.cgi?article=4966&context=td.

[560] Muhammad Raisul Alam, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali. "A Review of Smart Homes—Past, Present, and Future". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42.6 (Nov. 2012). Conference Name: IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), pp. 1190–1203.

[561] Frances K. Aldrich. "Smart Homes: Past, Present and Future". en. In: *Inside the Smart Home*. Ed. by Richard Harper. London: Springer, 2003, pp. 17–39. URL: https://doi.org/10.1007/1-85233-854-7_2 (visited on 03/06/2021).

[562] Smart Home. *What is a Smart Home?* en-US. 2021. URL: https://smarthomeenergy.co.uk/what-smart-home/ (visited on 02/28/2021).

[563] Whitney Quesenbery. "What Does Usability Mean: Looking Beyond 'Ease of Use'". en. In: (2007). URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6b117877a878b3818423262b0b664e6638cb0096.