

# The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home



George Chalhoub  
Pembroke College  
University of Oxford

A thesis submitted for the degree of  
*Doctor of Philosophy*  
Michaelmas 2022

# Acknowledgements

First and foremost, I would like to express my gratitude to my supervisor Prof. Ivan Flechais, for their unwavering support, guidance, and advice. Your patience, encouragement, and enthusiasm have been crucial for the success of this thesis.

I would also like to thank my thesis examiners, Prof Marina Jirotko and Prof Awais Rashid, for their insightful comments and meaningful suggestions throughout the entire process. Thank you for your constructive feedback and guidance.

I also wish to express my deepest gratitude to my scholarship donors. Your generosity has been an incredible gift that has given me the opportunity to gain skills, knowledge, and experience that will benefit my career and future endeavors.

I am also deeply grateful to my collaborators, for their invaluable advice and support. Their knowledge and expertise have been instrumental to the completion of this thesis. Thank you for your patience, dedication and support.

I am also immensely grateful to my Oxford friends and far-away friends. Your support, encouragement, and friendship have been invaluable. Thank you for all of the laughs, advice, and sweet memories throughout time.

I am deeply grateful to my parents Charles Chalhoub and Lucia Chalhoub, and my sister, Theresa Chalhoub, for their unconditional love and support. Their guidance, patience, and faith in me have been unceasing. Your love and support is the greatest gift I have ever received.

Finally, I would like to express my heartfelt gratitude to my partner, for their unwavering support, faith, and love. Thank you for being my pillar of strength. I am forever grateful for your presence in my life. May we never be apart.

# Abstract

Smart homes are under attack. Threats can harm both the security of these homes and the privacy of their inhabitants. As a result, in addition to delivering pleasant and aesthetic experiences, smart devices need to protect households from vulnerabilities and attacks. Further, the need for user-centered security and privacy design is particularly important for such an environment, given that inhabitants are demographically-diverse (e.g., age, gender, educational level) and have different skills and (dis)abilities.

Prior work has explored different usable security and privacy solutions for smart homes; however, the applicability of *user eXperience (UX)* principles to security and privacy design is under-explored. This research project aims to address the on-going challenge of security and privacy in the smart home through the lens of UX design. The objective of this thesis is two-fold. First, to investigate how UX factors and principles affect the security and privacy of smart home users. Secondly, to inform product design through the development of an empirically-tested framework for UX design of security and privacy in smart home products.

In the first step, we explored the relationship between UX, security, and privacy in smart homes from user and designer perspectives: through (i) conducting a qualitative interview study with smart home users (n=13) and (ii) analyzing an ethnomethodologically informed study of six UK households living in smart homes (n=6); and, we then explored the role of UX in the design of security, privacy and data protection in smart homes through qualitative semi-structured interviews with smart home users, designers and business leaders through two rounds of interviews (n=20, n=20).

In the second step, using conceptual framework analysis, we systematically analyzed our previously collected data and the literature to construct a framework of design heuristics for consent and permission in smart homes. We applied these heuristics in four participatory co-design workshops and reported on their use. We further analyzed the use of the heuristics through thematic analysis highlighting how the heuristics were used, their purpose, and their effectiveness.

By bringing UX design to the smart home security and privacy table, we believe that this research project will have a significant impact on academia, industry, and government organizations. Our thesis will improve design practices for security and privacy in domestic smart devices while addressing wider challenges, opportunities, and future work.

# Contents

<b>List of Figures</b>	<b>ix</b>
<b>List of Abbreviations</b>	<b>x</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Problem Statement and Motivation . . . . .	1
1.2 Research Gap . . . . .	2
1.3 Research Questions . . . . .	3
1.4 Thesis Structure . . . . .	3
1.5 Research Contributions . . . . .	4
1.6 Publications from Thesis Work . . . . .	5
<b>2 Background</b>	<b>6</b>
2.1 Literature Review . . . . .	6
2.1.1 Usable Security and Privacy . . . . .	6
2.1.2 User Experience (UX) . . . . .	10
2.1.3 Product Design . . . . .	13
2.1.4 Data Protection . . . . .	19
2.1.5 Smart Home . . . . .	22
2.1.6 Summary . . . . .	27
2.2 Research Approaches . . . . .	28
2.2.1 Information Security Approaches . . . . .	28
2.2.2 HCI Approaches . . . . .	29
2.2.3 Usable Security & Privacy Approaches . . . . .	30
<b>3 Methodology</b>	<b>33</b>
3.1 Common Research Approaches . . . . .	33
3.1.1 Information Security Approaches . . . . .	33
3.1.2 HCI Approaches . . . . .	34
3.1.3 Usable Security and Privacy Approaches . . . . .	35
3.2 Thesis Research Approach . . . . .	35
3.2.1 Research Overview . . . . .	36
3.2.2 Research Methodology . . . . .	36
3.3 Research Ethics . . . . .	42

<b>4</b>	<b>Security and Privacy User Experiences</b>	<b>43</b>
4.1	Perceptions of Security and Privacy . . . . .	44
4.1.1	Motivation . . . . .	44
4.1.2	Methodology . . . . .	44
4.1.3	Results . . . . .	47
4.1.4	Discussion . . . . .	55
4.2	Longitudinal Aspects of Security and Privacy . . . . .	58
4.2.1	Motivation . . . . .	58
4.2.2	Methodology . . . . .	58
4.2.3	Results . . . . .	65
4.2.4	Discussion . . . . .	74
4.3	Discussion . . . . .	77
4.3.1	Consent Needs are Dynamic . . . . .	77
4.3.2	Trigger Points Raise Security and Privacy Concerns . . . . .	77
4.3.3	Users Prefer Physical Privacy Controls . . . . .	78
4.4	Conclusion . . . . .	78
<b>5</b>	<b>User Experience Design in Smart Homes</b>	<b>79</b>
5.1	User Experience of Security and Privacy . . . . .	80
5.1.1	Motivation . . . . .	80
5.1.2	Methods . . . . .	80
5.1.3	Results . . . . .	83
5.1.4	Discussion . . . . .	96
5.2	User Experience of Data Protection . . . . .	98
5.2.1	Motivation . . . . .	98
5.2.2	Methods . . . . .	98
5.2.3	Results . . . . .	104
5.2.4	Discussion . . . . .	116
5.3	Discussion . . . . .	122
5.3.1	Discount Practices . . . . .	122
5.3.2	Lack of Security Innovation . . . . .	123
5.3.3	Difficulty Navigating Data Protection . . . . .	123
5.4	Conclusion . . . . .	124
<b>6</b>	<b>Design Heuristics for Smart Homes</b>	<b>125</b>
6.1	Motivation . . . . .	125
6.2	Methods . . . . .	126
6.2.1	Construction of Framework of Design Heuristics . . . . .	127
6.2.2	Applying the Framework in PD workshops . . . . .	128
6.2.3	Evaluation of the Framework of Heuristics . . . . .	131

6.2.4	Demographics . . . . .	131
6.2.5	Limitations . . . . .	132
6.3	Results . . . . .	133
6.3.1	Framework of Design Heuristics . . . . .	133
6.3.2	Case Studies . . . . .	133
6.3.3	Heuristics Evaluation . . . . .	135
6.4	Discussion . . . . .	140
6.4.1	Prominent Heuristics . . . . .	140
6.4.2	The interplay between Consent and Permissions . . . . .	141
6.4.3	Problems of Designing for Permissions . . . . .	142
6.4.4	Why Are Heuristics Useful . . . . .	142
6.5	Conclusion . . . . .	143
<b>7</b>	<b>Discussion</b>	<b>144</b>
7.1	Consent is Conceptualized as a Relationship . . . . .	144
7.1.1	The Lifecycle of Consent . . . . .	145
7.1.2	Consent is Dynamic not Static . . . . .	145
7.1.3	Withholding Consent can be Unpleasant . . . . .	146
7.1.4	Consent Changes Should be More Forgiving . . . . .	146
7.2	Data Protection Practitioners . . . . .	147
7.2.1	Data Protection Interactions in Smart Homes . . . . .	147
7.2.2	UX can Help Data Protection Interaction Design . . . . .	148
7.2.3	Supporting Data Protection Design More Broadly . . . . .	148
7.3	Innovation . . . . .	151
7.3.1	Implications of Innovative Repurposing . . . . .	151
7.3.2	Privacy vs Security Innovation . . . . .	152
7.3.3	Identifying Innovation Gaps for Business Leaders . . . . .	153
7.3.4	Responsible Innovation in the Design of Security and Privacy	153
<b>8</b>	<b>Conclusion</b>	<b>156</b>
8.1	Key Findings . . . . .	157
8.1.1	UX can Deepen Understanding of Consent Relationships . . . . .	157
8.1.2	Innovation in the UX Design of Security, Privacy and Data Protection . . . . .	157
8.1.3	UX Design can Help Security and Privacy Practitioners . . . . .	158
8.2	Critical Review . . . . .	158
8.3	Directions For Future Work . . . . .	160
8.3.1	Understanding the Effectiveness of Privacy Controls . . . . .	160
8.3.2	Forecasting the Consequences of Technology Repurposing . . . . .	160
8.3.3	Making Consent Choices More Forgiving . . . . .	161

8.3.4	Innovating without Hindering Security . . . . .	161
8.3.5	Creating UX-aware Data Protection Guidelines . . . . .	161
8.3.6	Improving Communication Among Different Stakeholders . .	161
8.3.7	Identifying Heuristics for Individuals . . . . .	162

**Appendices**

<b>A</b>	<b>Thesis Definitions</b>	<b>164</b>
A.1	Definitions . . . . .	164
A.1.1	User Experience . . . . .	164
A.1.2	Security . . . . .	165
A.1.3	Privacy . . . . .	166
A.1.4	Smart Home . . . . .	166
A.1.5	Product Design . . . . .	167
A.1.6	Innovation . . . . .	168
<b>B</b>	<b>Chapter 4 Supplementary Material</b>	<b>169</b>
B.1	Study One . . . . .	169
B.1.1	Interview Questions . . . . .	169
B.2	Study Two . . . . .	171
B.2.1	Recruitment Form . . . . .	171
B.2.2	Diary Template . . . . .	178
B.2.3	Deployment Picture and Notes . . . . .	178
B.2.4	Relation to previous work . . . . .	181
<b>C</b>	<b>Chapter 5 Supplementary Material</b>	<b>182</b>
C.1	Study One . . . . .	182
C.1.1	Screening Questionnaire . . . . .	182
C.1.2	Pilot Interview Questions . . . . .	184
C.1.3	Main Interview Questions . . . . .	184
C.1.4	Codebook . . . . .	189
C.2	Study 2 . . . . .	190
C.2.1	Main Interview Questions . . . . .	190
C.2.2	Codebook . . . . .	192
<b>D</b>	<b>Chapter 6 Supplementary Material</b>	<b>193</b>
D.1	Conceptual Framework Analysis Codebook . . . . .	193
D.2	Design Heuristics . . . . .	194
D.3	Conceptual Framework Analysis Papers . . . . .	196
D.4	Heuristics Evaluation . . . . .	202

<b>E Ethics Applications and Approval</b>	<b>204</b>
E.1 Ethics Application CUREC/CS_C1A_19_024 . . . . .	205
E.1.1 Application Material . . . . .	205
E.1.2 Information Sheet . . . . .	217
E.1.3 Guide to Interview Questions . . . . .	220
E.1.4 Participant Consent Form . . . . .	222
E.1.5 Poster Advertisement . . . . .	224
E.2 Ethics Application CUREC/CS_C1A_1949 . . . . .	225
E.2.1 Application Material . . . . .	225
E.2.2 Information Sheet . . . . .	237
E.2.3 Guide to Interview Questions . . . . .	240
E.2.4 Participant Consent Form . . . . .	242
E.2.5 Poster Advertisement . . . . .	244
E.3 Ethics Application CS_C1A_021_037 . . . . .	245
E.3.1 Application Material . . . . .	245
E.3.2 Information Sheet . . . . .	257
E.3.3 Guide to Interview Questions . . . . .	260
E.3.4 Participant Consent Form . . . . .	261
E.3.5 Poster Advertisement . . . . .	263
<b>References</b>	<b>264</b>



# List of Figures

1.1	Thesis Structure . . . . .	4
2.1	Evolution of the field of UX . . . . .	10
2.2	UX Design Four-step Process. . . . .	16
2.3	UX Innovation Design Space. . . . .	18
3.1	Dissertation Roadmap . . . . .	36
3.2	Summary of our two studies for RQ1 . . . . .	37
3.3	Summary of our two studies for RQ2 . . . . .	39
3.4	Summary of our study for RQ3 . . . . .	40
4.1	Summary of our research methodology . . . . .	44
4.2	Summary of our categories and codes . . . . .	47
4.3	Conceptual model showing UX effect on risk and balancing behavior	58
4.4	Timeline of different phases of data collection . . . . .	61
4.5	Smart products deployed in household four . . . . .	65
4.6	H4's privacy experiences with the Echo Show 5 over time . . . . .	66
4.7	H3's consent experiences with the Google Home over time . . . . .	68
4.8	H1's repurposed use of the Arlo Pro security camera over time . . . .	70
5.1	Theory of UX factors in the Role of Innovation in Smart Homes . . .	84
6.1	Framework of design heuristics . . . . .	129
B.1	Diary Template . . . . .	178
B.2	Deployment Notes (Part 1) . . . . .	179
B.3	Deployment Notes (Part 2) . . . . .	180

# List of Abbreviations

<b>CHI</b> . . . . .	ACM Conference on Human Factors in Computing Systems.
<b>CI</b> . . . . .	Contextual Integrity.
<b>CSCW</b> . . . . .	Computer-Supported Cooperative Work.
<b>CUREC</b> . . . . .	Central University Research Ethics Committee.
<b>DpbD</b> . . . . .	Data Protection by Design and by Default.
<b>DDoS</b> . . . . .	Distributed Denial-of-Service.
<b>DNS</b> . . . . .	Domain Name Service.
<b>EEA</b> . . . . .	European Economic Area.
<b>EMA</b> . . . . .	Ecological Momentary Assessment.
<b>EU</b> . . . . .	European Union.
<b>GDPR</b> . . . . .	General Data Protection Regulation
<b>GT</b> . . . . .	Grounded Theory
<b>HCI</b> . . . . .	Human-Computer Interaction.
<b>HCII</b> . . . . .	International Conference on Human-Computer Interaction.
<b>HCI-SEC</b> . . . . .	Human-Computer Interaction and Security.
<b>ICO</b> . . . . .	Information Commissioner’s Office.
<b>IoT</b> . . . . .	Internet of Things.
<b>ISO</b> . . . . .	International Standardization Organization.
<b>IS</b> . . . . .	Information Security.
<b>IT</b> . . . . .	Information Technology.
<b>NPD</b> . . . . .	New Product Development.
<b>OWASP</b> . . . . .	Open Web Application Security Project.
<b>PbD</b> . . . . .	Privacy by Design.
<b>PD</b> . . . . .	Participatory Design.
<b>QoE</b> . . . . .	Quality of Experience.

<b>QoS</b>	. . . . .	Quality of Service.
<b>RQ</b>	. . . . .	Research Question.
<b>RRM</b>	. . . . .	Risk Rating Methodology.
<b>RFID</b>	. . . . .	Radio-Frequency Identification.
<b>SbD</b>	. . . . .	Secure by Design.
<b>SOUPS</b>	. . . . .	Symposium on Usable Privacy and Security.
<b>SQL</b>	. . . . .	Structured Query Language.
<b>UCD</b>	. . . . .	User Centered Design.
<b>UI</b>	. . . . .	User Interface.
<b>UK</b>	. . . . .	United Kingdom.
<b>US</b>	. . . . .	United States.
<b>UX</b>	. . . . .	User Experience.

*“Privacy means people know what they’re signing up for, in plain English, and repeatedly... Let them know precisely what you’re going to do with their data.”*

— Steve Jobs

# 1

## Introduction

In this chapter, we describe and motivate a research problem that this thesis addresses. We also propose a main research question based on our understanding of the problem and our preliminary study. We then break down the main research question into sub-questions to clarify the main claim made by this proposal. We conclude the chapter by presenting the structure of the dissertation and the existing publications arising from this work.

### 1.1 Problem Statement and Motivation

The rapidly-growing smart home market is predicted to witness a yearly double-digit growth of 26% [1]. Connected smart home devices, such as smart speakers, thermostats, doorbells, and cameras are found in 134 million households and are expected to reach 234 million households by 2024 [2]. The rapid increase and growth of smart home devices is changing the topography of the internet. Smart homes are expected to generate 90 zettabytes of data and reach market revenue of US\$1.1 trillion by 2025 [3]. Smart home devices support beneficial features, such as voice-controlled assistants and remote-controlled thermostats, but they also raise new security and privacy risks.

There has been controversy over how invasive smart home technologies are. Users of Amazon Alexa were outraged after a Bloomberg investigation revealed that Amazon contracted thousands of workers to listen to customer audio recordings. An Amazon team in Romania reportedly heard “*private moments including family rows, money and health discussions*” [4]. In 2016, the Mirai botnet infected 600,000

unsecured IoT (Internet of Things) devices and initiated one of the largest DDoS (Distributed Denial of Service) attacks in history [5]. Moreover, the New York Times' Privacy Project about protecting privacy online recommended people not to use smart home devices unless they are "*willing to give up a little privacy for whatever convenience they provide*" [6]. A recent report showed that people's concerns about their security and privacy when using smart home devices are increasingly hindering the adoption of these devices [7].

Many efforts have been made to increase security and privacy in the smart home. However, the necessity of adopting a user-centered approach has been overlooked [8]. Only a small number of researchers have expressed the need for taking a human-factors approach to the security of smart home devices [9]. In addition, there have been many calls for smart home manufacturers to take an active role in understanding how their security and privacy solutions align with User Experience (UX) [10, 11]. There has been little research into the effect of UX on users and the practices of UX designers of smart home devices [9, 12]. Without an understanding of users and designers' perceptions, challenges, and responsibilities, the existing security and privacy issues in these devices will not be easily addressed.

## 1.2 Research Gap

Usability has been an ongoing concern in Human-Computer Interaction (HCI). However, UX encompasses greater considerations such as value, adoptability, and desirability. Yet, these dimensions have not been explored in detail when applied to security and privacy [13]. This seems a missed opportunity to further improve the quality of security and privacy interactions given the UX focus on emotions, psychological responses, beliefs, perceptions, behaviors, and accomplishments [14–17]. UX is important because it can fulfill users' needs, ensure positive experiences, and warrant secure and private interactions.

**Although security and privacy are two of the most researched areas in the smart home, they are barely tackled from a UX point of view. The relationship between UX and the challenge of security and privacy in the context of the smart home is neither well understood nor well researched [18, 19].** Hence, this thesis aims to research UX design principles and factors in order to inform and inspire the design of security and privacy in smart home devices.

## 1.3 Research Questions

This thesis is motivated by the overarching research question: **How can UX design principles be well supported and understood to inform security and privacy design in the smart home?**

- RQ1: What is the relationship between UX, security, and privacy in the smart home?
  - (i) How do smart home users perceive the importance of UX in relation to smart home products?
  - (ii) How do smart home users perceive security and privacy over time in different real-world contexts in relation to smart home products?
- RQ2 : What is the role of UX in the design of security, privacy and data protection in smart home products?
  - (i) How do designers and their collaborators factor UX into the design of security, privacy and data protection in the smart home products?
  - (ii) How can we understand and support the UX of data protection in smart homes from the perspective of users, designers, and business leaders?
- RQ3: How can UX design be incorporated into the design of security and privacy of smart home devices?
  - (i) How can we inform product design to incorporate UX practices into the security and privacy of smart home devices?
  - (ii) How can we apply and evaluate practices which factor UX in security and privacy in the product design process of smart home devices?

## 1.4 Thesis Structure

Figure 3.1 provides an overview of this proposed dissertation structure showing how the research questions in Section 1.3 and the contributions in Section 1.5 are written up as chapters.

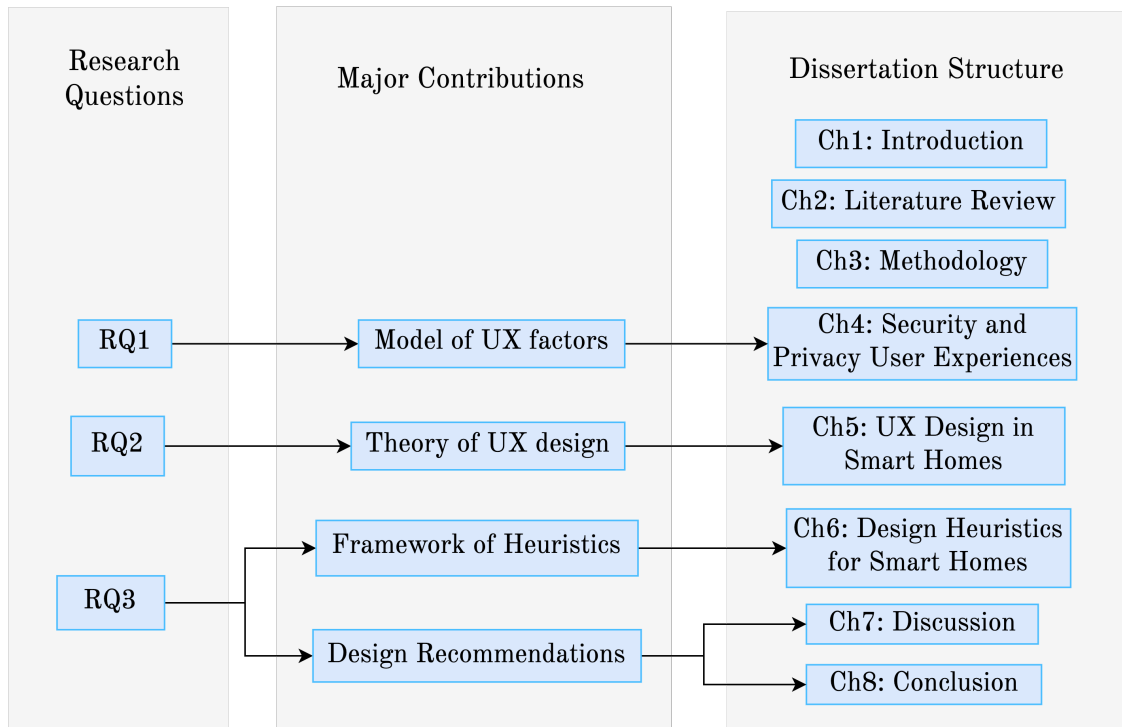


Figure 1.1: Thesis Structure

## 1.5 Research Contributions

The proposed research of this dissertation is a topic that has not been extensively studied. In summary, the proposed contributions from this dissertation are as follows:

1. A **conceptual model** demonstrating the UX effect on risk, perceptions and balancing behavior in smart home products (see Figure 4.3 in Chapter 4).
2. A **longitudinal analysis** and view of security and privacy experiences in smart home products (see Figures 4.4, 4.6, 4.7 and 4.8 in Chapter 4).
3. A **theory** of UX factors in the role of innovation in security and privacy in the design of smart home products (see Figure 5.1 in Chapter 5).
4. A **qualitative investigation** of the UX of Data Protection from designer and business leader perspectives (see Tables 5.4, 5.5 and 5.6 in Chapter 5).
5. A **design framework** that informs the UX design of security, privacy and data protection in smart home products (see Figure 6.1 in Chapter 6).
6. List of **design heuristics** for the design of UX, security and privacy in smart home products (see Chapter 6 and Appendix D.2).

## 1.6 Publications from Thesis Work

Table 1.1 describes elements of this work that have been published in peer-reviewed workshop and conference proceedings.

Publication	RQ	Status	Chapter
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. <i>In the 22nd International Conference on Human-Computer Interaction (HCI2020)</i> . Springer. May, 2020.	RQ1	Published [20]	Chapter 4
George Chalhoub, Martin J. Kraemer, Norbert Nthala and Ivan Flechais. “It did not give me an option to decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. <i>In 2021 CHI Conference on Human Factors in Computing Systems (CHI2021)</i> . ACM. May, 2021.	RQ1	Published [21]	Chapter 4
George Chalhoub, Ivan Flechais, Norbert Nthala and Ruba Abu-Salma. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Devices. <i>In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)</i> . USENIX. August, 2020.	RQ2	Published [22]	Chapter 5
George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma and Elie Tom. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. <i>In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI2020)</i> . ACM. April, 2020.	RQ2	Published [23]	Chapter 5
George Chalhoub and Ivan Flechais. Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives. <i>In The 25th ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW2022)</i> . ACM.	RQ2	Published [24]	Chapter 5
George Chalhoub. The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home. <i>In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI2020)</i> . ACM. April, 2020.	RQ3	Published [25]	Chapter 6

**Table 1.1:** List of existing publications



*“UI is the saddle, the stirrups, & the reins. UX is the feeling you get being able to ride the horse.”*

— Dain Miller

# 2

## Background

In this chapter, we provide a historical review of the UX literature and research methods. Furthermore, we review the state-of-the-art research in the field of usable security and privacy. Additionally, we provide a background review of product design and the product design process, with a focus on innovation. Finally, we synthesize security and privacy and usability issues in the smart home, and conclude this section by summarizing the gaps identified.

### 2.1 Literature Review

#### 2.1.1 Usable Security and Privacy

##### 2.1.1.1 HCI and Security

A group called Human-Computer Interaction and Security (HCI-SEC) was formed in 2003 [27, 28] by researchers with the goal of bridging the gap between security and usability to achieve “Usable Security” [29]. HCI-SEC proposed three fundamental approaches to integrate “usable security” into computer systems: applying it by (i) enforcement, (ii) encouragement, and (iii) teaching and training.

**2.1.1.1.1 Usability and Security** Before 2005, there was little research on security and usability in systems [30]. As such, security in systems was poorly designed, prompting users to avoid using security features or looking for alternative interactions [31]. With a growing need of systems that provide both usability and security, the research on the usability of security is increasingly becoming active. Whitten & Tygar [32]’s ‘Why Johnny Can’t Encrypt’ defined security as usable

if users (i) are accurately informed of security tasks that should be made, (ii) are capable to perform tasks successfully, (iii) do not make threatening mistakes and (iv) are adequately at ease with interfaces. In the past years, usability research has strongly focused on authentication [33–37], email and encryption [32, 38], security systems [39, 40], and device pairing [41–43]. Different efforts were put together to reduce the research gaps between usability and security. Alshamari [44] categorized the efforts into different groups:

1. Recommendations and guidelines.
2. Models and frameworks.
3. Technology use (e.g., new ideas and paradigms).

The previous literature highlights that usability in security and privacy has to be factored early in the design process [45–47], and not treated as a final addition. For instance, Cranor and Garfinkel [48] found that designing security and usability from the beginning of the development lifecycle is critical for computer systems.

Furthermore, the field of user-centered security also emerged which gave birth to security models, frameworks, software, and systems which treat usability as a primary goal [49]. User-centered security has three main approaches, most of which are based on concepts from user-centered design [50]:

1. **Applying usability to secure systems:** Applying confirmed methods for improving usability into existing security systems. Approaches for achieving this include contextual design [51], discount usability testing [52], and in-lab testing [53].
2. **Applying security to usable systems:** Integrating security services into software that has a strong requirement for usability. Work in this stream focuses on developing techniques, models, and frameworks that incorporate security into usable systems [54].
3. **Developing user-centered security design:** Developing user-centered security models and applications. The main focus of the approach is to take into consideration end-user needs as a main goal when developing a model or a feature.

### 2.1.1.2 HCI and privacy

**2.1.1.2.1 Background** The World Wide Web (WWW) emerged in the 90s which prompted changes in regulations to carry the increased number of personal information collected online [55]. Research in privacy followed this development, adopting the use of computing for communication and expanding the adaptability of collected user data. HCI research started to pivot on the utility of IT to support

social and workgroups in society [55]. Following these developments, research began to pay particular attention to interpersonal privacy in everyday communications (e.g., email, internet messaging) [56, 57].

The rise of sensors, wireless networking, and computer devices has driven the development of mobile and ubiquitous applications. Ubiquitous applications such as the smart homes or smart watches do not operate in traditional environments, which creates novel challenges in privacy in HCI [58, 59]. For instance, the inherent nature of interaction in ubiquitous applications prompted researchers to re-examine Donald Norman’s “seven stages of actions” [60] and well-established principles of privacy (e.g., obtaining consent) [61].

Today, HCI provides a wide range of tools that can examine how users react to privacy threats and vulnerabilities [55].

**2.1.1.2.2 Usability and Privacy** There are four major streams of research in privacy and usability research within HCI, we list them below [61]:

- The process of basic designing and evaluating the usability of systems (e.g., usability engineering).
- The examination of users’ interactions with systems (e.g., computer-supported cooperative work).
- The study of users’ differences in their capabilities and preferences in HCI interfaces (e.g., tailorability).
- The role of usability in innovative technologies and architectures (e.g., ubiquitous, pervasive).

While most research has focused on the intersection of usability and security, some has focused on usability and privacy [62]. A prominent research tool is Privacy Bird, a usable privacy tool that informs online users on practices of websites [39]. Usable privacy tools often conform to four principles that are fundamental to their efficiency [63]. We summarize them below:

1. **Privacy is not the main task of users.** Making privacy a specific task for the users can create usability challenges. Privacy tasks should be lightweight or invisible [64].
2. **Privacy should work for all users.** Users differ in many aspects such as technical capabilities, disabilities and skills. Privacy design should deal with individual differences.
3. **Privacy increases the level of risk and reward.** Privacy that has not been designed properly can create adoption issues and threaten the privacy of the users and the organization, which increases reputation risk.

4. **Privacy must abide by regulations.** Privacy law might be complicated as different jurisdictions have different laws. The demand for regulatory expertise increases costs and challenges of privacy design.

### 2.1.1.3 UX in Security and Privacy

Despite the growth of research in HCI and also security and privacy, research at the intersection of these domains has been focused on usable security and privacy, and particularly on user needs [65]. However, as technology use evolves and becomes embedded in everyday life, the focus on usability (i.e., the effectiveness, efficiency, and satisfaction afforded by an interaction) is insufficient. Broader issues need to be considered, such as social communication, contextual trust, and even aesthetic aspects of security and privacy.

For example, people share passwords with family members and spouses, contrary to popular belief of not sharing passwords [66]. Similarly, novel authentication methods that presented security improvements did not “feel secure” [67], whereas supposedly insecure systems did [68]. The focus on only usable security and privacy means that we will lack knowledge on the subjective ways that people make security and privacy decisions.

Earlier works have strongly emphasized on the need to encompass UX research in the security and privacy design of computing technologies. Such approaches would be able to provide an in-depth analysis of people’s perceptions, practices, and experiences [13, 69]. Addressing security and privacy from a UX lens provides the ability to merge and mix three major security and privacy research areas [69]. Exploring security and privacy practice from a UX lens has the ability to uncover novel design ideas in relation to security and privacy. Similarly, factoring the experience aspects of security and privacy in computing is likely to positively affect the adoption rate of such technologies.

Despite the projected benefits, the exploration of UX is not common in usable security and privacy research. Research in “experience-centered security and privacy” argues that existing UX research approaches have slowly been adapting to usable security and privacy research [13]. Researchers suggest that there is a need for understanding and designing the UX of privacy and security technologies through the following:

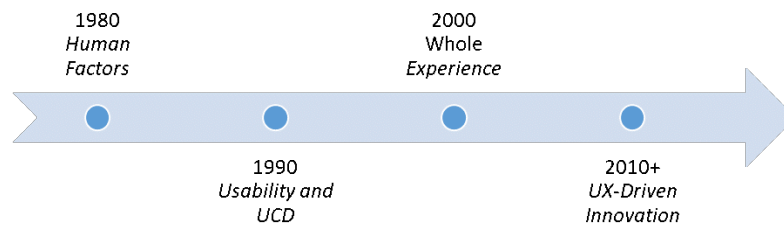
- Building and understanding practices that are context-specific.
- Obtaining insights into perceptions and motivations of users.
- Theorizing about adapting technologies into users’ lifestyles.
- Generating inspirations that assist the design of new technologies.

There are additional gaps in this space: Shava and Van Greunen [70] state that there was a “missing link” between UX and usable security; and other researchers have also found a lack of frameworks, models, and scientific research in UX and security [71, 72]. A literature survey on UX and usable authentication found that only 19% of HCI papers contained UX topics, where a minority of papers explicitly refer to UX as “experience” or “user experience” [73].

## 2.1.2 User Experience (UX)

### 2.1.2.1 Background

Before 1990, UX was embedded in human factors, with a narrow focus on designing for physical spaces (e.g., human factors in aviation [74]). The field evolved in the 1990s toward the usability of computers [75] and user interfaces (UI) [76]. By the early 2000s, the focus had increased towards the whole UX [16], and not just specific design elements. As of the 2010s, UX practitioners are evolving and use experiences to innovate in the product design process [77]. Today, we find more UX practitioners and academics facilitating the dialogue around innovation.



**Figure 2.1:** Evolution of UX

Academics and industry experts have attempted many times to create a common definition of UX [16, 78–80]). However, a survey in 2018 uncovered that there is a disagreement in the HCI community over the importance of UX aspects [79]. There is also a difference in opinion on what design means in high-technology companies. While the UX community cannot agree on a uniformly accepted UX model that drives research, there is an agreement that UX is dynamic, subjective, and context-dependent [79]. UX cannot be specifically designed, one can aim to design for UX [81].

### 2.1.2.2 From Usability to UX

Being a core quality requirement in ISO 25010, usability [82] is defined as “the extent to which a product can be used by specified users to achieve specific goals with effectiveness, efficiency, and satisfaction in a specified context of use” [83]. UX pioneers Jakob Nielsen and Donald Norman, distinguish usability from UX by grounding usability in UIs, and extending UX beyond every part of a system [84]. They add to the standard definition of UX (see Section A.1.1) to include “all aspects of the end-users interaction with the company, its services, and its products” which complies with Preece et al.’s elaboration of the concept [81]. Due to UX being about how users feel and experience interactions, UX requirements have more subjective qualities than usability requirements. Subjective qualities can be abstract words, such as ‘engaging’, ‘supporting creativity’, and ‘rewarding’. Therefore, it would not be enough to design for UX by just considering the aesthetic and functional design [15].

### 2.1.2.3 Interaction and Quality of Experience

While we have distinguished between UX and usability, it is also important to compare UX with Quality of Experience (QoE) and Interaction, as well. The QoE has four attributes: communication situation, service prescription, technical parameters [85] and the UX. UX cannot be equated with QoE but is considered as part of it. Those four attributes are part of the Quality of Service (QoS) which factors measuring technical characteristics affecting the service performance [85]. As for the interaction, it can be understood as a component of designing for the UX. Interaction design moves for planning and controlling the interaction whereas UX design factors the experience that any interaction generates for the end-user [86]. Since interaction design is used with the goal of designing for the UX, the difference cannot be easily made.

### 2.1.2.4 UX and Agile Development

Agile development has gained increased traction in the past years [87]. The agile process consists of a set of core principles defined in 2001 in the “Manifesto for Agile Software Development” [88]. Today, the core principles have evolved into different techniques such as: focus on quality, communication and incremental development [87].

Agile principles do not mention UX or how it is integrated with the software development process. However, some similarities between UCD and agile are

identified [89]. A key element in UCD requires getting early user feedback. In contrast, customer satisfaction is a key aspect of agile development, which delivers small working sets of features frequently delivered to the customers.

Agile and UX design processes are highly iterative in their nature. The use of short iterative cycles in the agile processes indicates that UX activities must be outlined so that the outcome of such activities can be factored by designers and developers promptly [81].

#### **2.1.2.5 Frameworks for researching UX**

UX research is mainly driven into two research methods: one method which advocates a qualitative design approach and one method that promotes a quantitative model approach. There are two prominent UX frameworks for each approach: McCarthy and Wright’s approach [17], which is considered as qualitative design-based and Hassenzahl’s approach [90] which is considered as quantitative model-based.

**2.1.2.5.1 McCarthy and Wright’s approach** McCarthy and Wright explain in “Technology as Experience” [17] their framework which highlights a holistic view of UX without being reductionistic [91]. The framework’s objective is to learn about the complex interactions in the ‘threads’ of UX and recognizing sensemaking as the “central process of experiencing” [91]. Four threads and six processes are suggested to fully grasp an experience. The four threads are: the compositional thread, the emotional thread, the spatiotemporal thread, and the sensual thread.

**2.1.2.5.2 Marc Hassenzahl’s approach** Hassenzahl’s framework [90] focuses on the technological artifacts that affect the experience. Hassenzahl reports distinct dimensions of UX and their relationship to interaction (e.g., artifact). The framework interprets UX as situated, subjective, dynamic and holistic, but also manipulable (“shapeable”) by technology [90]. To link technology and UX, the framework proposes a three-tier UX hierarchical model composed of do-goals, be-goals and motor goals. This model is based on Carver and Scheier’s self-regulation theory [92] and activity theory [93].

#### **2.1.2.6 UX and HCI**

HCI is defined as “a discipline concerned with the design, evaluation, and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them” [94]. Being an interdisciplinary field, it had

been influenced in the past decades by the fields of computer science, cognitive science, ergonomics, social science and the humanities [95].

UX was long rooted in the field of HCI, where it has inherited theoretical concepts, epistemological assumptions, and methodologies [96]. HCI was described as “the forerunner to UX design” [97]. Therefore, HCI and UX are seen as mutually beneficial disciplines and mutually educational endeavors [98].

An existing research gap exists between UX Practice and HCI Research. There have been limited explorations (e.g., understanding the processes of UX professionals, empirical studies around UX practice) of UX practice by HCI researchers [99–101]. Similarly, there is little research on how HCI research could be accessible and reachable to UX professionals [100]. The experience of UX industry experts could have unforeseen implications for HCI research [101].

### **2.1.3 Product Design**

#### **2.1.3.1 Background**

Product design refers to the creation of new products by businesses to market them to users [102]. The process involves a constructive creation and build out of ideas that inform novel products [103]. Therefore, it is an integral aspect of new product development (NPD), which covers the complete process of bringing a new product to market. NPD is referred to as the conversion of an opportunity in the market into a product [102] which can be tangible or intangible where “services” are differentiated from “products”. NPD consists of analysis of competitive environments, user needs, and the type of the market [104].

#### **2.1.3.2 Product Design Process**

Product design processes are varied and often emphasize many aspects. One prominent model is defined by Jim Bagnellin and Don Koberg in “The Seven Universal Stages of Creative Problem-Solving.” Product design process requires a group of people who possess different talents and skill-sets (e.g., hardware designers, software developers, UX designers), depending upon the nature and type of product involved. Product design process generally involves brainstorming, requirement gathering, prototyping and finally generating the product. The final step is critical as the idea needs to be translated into a market product and evaluated. The process involves three major steps that we explain below: Analysis, Concept and Synthesis [105].



**2.1.3.2.1 Analysis Accept Situation:** This is a decision-making phase that requires all stakeholders to commit to a project or an idea, and allocating time to look for a solution. Stakeholders will seek solving the task efficiently [105].

**Analyze:** This is a research phase that requires gathering general and specific information with the aim of addressing the problem. Information can consist of scientific or industry articles, statistics, research data and other sources [105].

**2.1.3.2.2 Concept Define:** This is a major step that prompts stakeholders into converting their conditions into objections; and project restraints into project parameters in which the new product must address [105].

**2.1.3.2.3 Synthesis Ideate:** This is a brainstorming phase where all stakeholders propose novel solutions and new ideas to the existing design challenge. The aim of this phase is to avoid bias and judgment while focusing on novelty [105].

**Select:** This is a filtering phase where all stakeholders narrow down proposed solutions and curate a small list that is most effective in achieving the new product goals [105].

**Implement:** This is a prototyping phase where the proposed plan from the selection step is prototyped. In this phase, the stakeholders should form a realistic idea on how the final product is going to take shape [105].

**Evaluate:** This is the testing phase where all the final product is tested, evaluated and improved. This phase is often iterated with the previous implementation phase, due to prototypes not working as expected [105].

### 2.1.3.3 Data Protection in Product Design

General Data Protection Regulation (GDPR) is a regulation in European law on data protection legislation in the European Union (EU). GDPR's objective is to allow users to have control and transparency over the use of their personal data [106]. The UK implemented GDPR in 2018 in a legislation known as the Data Protection Act [107].

GDPR legally prompts companies to take technical and organization charges to incorporate data protection in the design process through the concept of "data protection by design and by default" (DpbD) [108]. The concept is also known as "privacy by design" (PbD) and affects not only the design phase but the whole lifecycle process of a product. In the UK, DpbD means that businesses "*consider privacy and data protection issues at the design phase of any system, service or product.*" [109] It also ensures that companies abide by the grounding principles and requirements of GDPR, as well as being accountable to any breaches.

**2.1.3.3.1 Privacy by Design** Suggested initially by Ann Cavoukian, the concept of PbB appeared in 1995 as part of group effort by the (i) Dutch Data Protection Authority, (ii) Netherlands Organization for Applied Scientific Research and (iii) the Information and Privacy Commissioner of Ontario (IPC) [110, 111]. In 2010, the “International Assembly of Privacy Commissioners and Data Protection Authorities” [112] adapted the framework for PbB [113]. Just like DpbD, PbB requires that privacy is taken into consideration during the whole engineering process.

Privacy by design is based on seven “foundational principles” [107, 113, 114]:

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”.
7. “Respect for user privacy”.

Since they emerged, those seven principles have had widespread success and have been referenced hundreds of times [114].

**2.1.3.3.2 Secure by design** Secure by Design (SbD) is a principle in software development, indicating that a particular software has been designed and developed from the beginning of its lifecycle with security as principle. In an SbD approach, the alternative security strategies and structures are first examined; where the strongest principles are picked and imposed by the engineering design. They are later used as a leading and then used as guiding concepts for developers [115]. SbD has been becoming widely used in development approaches to ensure the security of software engineering platforms. In an SbD approach, security always begins with a strong architecture design that factors security from scratch as soon as the development of a system starts.

#### **2.1.3.4 Product Design Categories**

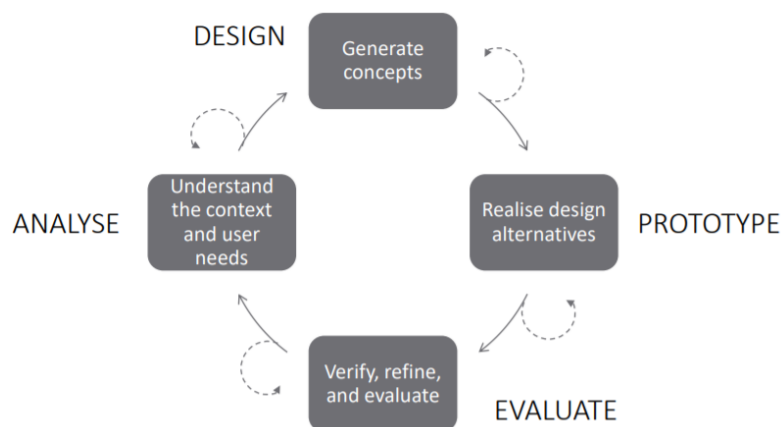
Two categories of product design are identified in the literature, both relating directly to innovation: demand-pull innovation and invention-push innovation [116]. We briefly describe each category below:

**2.1.3.4.1 Demand-pull innovation** Demand-pull innovation corresponds to a market opportunity grabbed by product design [116]. In demand-pull, the product addresses the problem by either (i) building a new product from the ground, or (ii) developing an existing product (e.g., invention) for another purpose [116].

**2.1.3.4.2 Invention-push innovation** Invention-push innovation corresponds to a development and improvement in intelligence gathered by product teams. In invention-push, intelligence can develop either through (i) research done by developing teams or (ii) novel product design ideas proposed by stakeholders (e.g., the product designer) [116].

### 2.1.3.5 UX Design in Product Design

There has been existing work that merges UX design with product design process. The ‘UX Design Process’ is a four-step method for including UX in the product development (see Figure 2.2); the steps are: analyze, design, prototype and evaluate [117]. This process is iterative; meaning all four phases are iterated regularly through the process. The first ‘analysis’ phase consists of contextual and user research [81]. The second ‘design’ phase consists of design activities that are aimed to design different solutions to be used as alternatives. The third ‘prototype’ phase consists of activities (e.g., sketching, story-boarding, personas) that are aimed to develop prototypes and conceptual requirements [118]. The fourth ‘evaluation’ phase consists of an iterative cycle with the ‘prototype’ phase that aims at evaluating and improving the prototyped design [117].



**Figure 2.2:** UX Design Four-step Process. Adapted from Hartson and Pyla [117].

### 2.1.3.6 Experience-Driven Innovation

UX has long been seen as a driver and enabler of Innovation in technological products.

**2.1.3.6.1 Background** UX factors have started to drive innovation in computing due to the strong link between the need for novelty and technological advancements. The advancement of technology and science brought forward novel technologies (e.g., smart watches, smart homes) in users and companies [119]. By addressing user needs, experience-driven innovation shifted competition from usability to UX, e.g., businesses must innovate in the design of services and products to foster a good UX. Enabling experience-driven innovation in the market increases the demand for innovation, which drives positive advances in computing [120]. Experience-driven innovation often addresses market needs by creating novel solutions that satisfies demand, or by finding a novel way to match needs to a solution [121, 122].

User needs (e.g., psychological) have constantly been used in the literature to drive innovation through UX. A prominent method to design for UX innovation, is known as the, “UX Concept Exploration” [123], explores user needs to extract user-generated ideas for prioritizing and selecting them. User needs have experimentally improved the UX of new technological products by considering UX factors in the early stage of design and development [124].

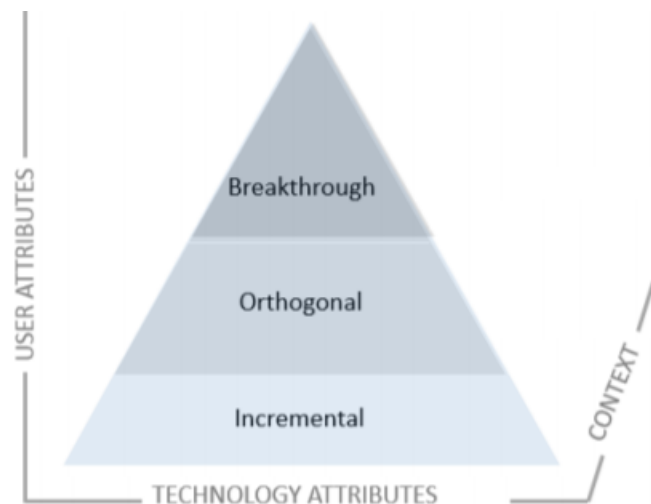
**2.1.3.6.2 Types** We distinguish two types of innovation used in UX-driven innovations: “Open Innovation” and “Co-Creation”.

**Open Innovation:** Chesbrough defines Open Innovation as “the use of purposive inflows and outflows of knowledge to accelerate internal innovation, and expand the markets for external use of innovation, respectively.” In open innovation, companies use different sources of knowledge to transform ideas into commercial products. Innovations are often drawn from employees, users, or even in some cases, competitors. In this model, knowledge is freely exchanged between universities, businesses, and users. An opposite approach to open innovation is “closed innovation”, where businesses restrict the creation of novel ideas through their research and development departments.

**Co-Creation:** Co-creation is defined by Rindfleisch and O’Hern as “a collaborative NPD activity in which customers actively contribute and/or select the content of a new product offering”. Co-creation requires two steps: the contribution of content and the selection of the best contributions. In co-creation, customers and end-users play a key role in the product design process. The process of co-creation is strongly dependent on the flexibility of the requirements of contributions (e.g., fixed, open) and the decision-makers of the selection of the customer contributions (e.g., firm-led selection, customer-led selection)) [125].

**2.1.3.6.3 Categories** UX-driven innovation requires at least these innovations: orthogonal, breakthrough and incremental. In orthogonal innovation, customer needs are matched with novel products or services (e.g., the need for hands-free communication and the introduction of Alexa). In breakthrough innovation, new knowledge is obtained by gaining new information from customers (e.g., Google’s DeepMind innovations in reinforcement learning). Incremental innovation refers to making outstanding improvements to existing products and services (e.g., the switch from Flash Player to HTML5) [122].

**2.1.3.6.4 Dimensions** UX innovations have three dimensions: user attributes, technology attributes, and the context (see Figure 2.3). UX requires individuals to use technology attributes for a purpose in a context [16, 126]. In this design space, the user dimension factors individual characteristics (e.g., age, gender, expertise) whereas the technology dimension factors technology and interaction type (e.g., touch, voice, gaze), and physical characteristics (e.g., size, shape). The context dimension factors the environment in which the interaction happens (e.g., task, setting physical and environment).



**Figure 2.3:** UX Innovation Design Space. Adapted from Djamasbi and Strong [127].

### 2.1.3.7 UX and UCD in Product Innovation

The concepts of UX and UCD have been crucial in the product design process for the past 10 years [16, 79, 128]. As mentioned early, user needs have been the center focus of academics and businesses [79, 129], which prompted businesses to heavily invest in those fields [130]. The introduction of UX-based innovation

introduced a common holistic approach where knowledge is analyzed by stakeholders to foster innovation [131]. As such, there has been consensus among organizations, business leaders, UX and design experts that it is crucial to factor UCD and UX in product innovation [131].

However, an existing research gap in this area is that it is challenging for entities to determine how to use and interpret the concepts of UX and UCD. A survey by Law et al. demonstrated difficulties and obstacles resulting from using UX and UCD concepts among designers, developers, managers and directors [79]. One reason for those challenges would be UX being interpreted differently between researchers and practitioners (see Section 2.1.2.6), which makes UX design for users situation-specific. In addition, holistic perspectives in UCD and UX are under-researched [128, 132]. Despite the challenges, UX and UCD models and frameworks are feasible in both industry and academia [16]. To fill the research gap in the area of bringing UX and UCD in product innovation, three challenges needed to be addressed [133]:

1. Establishing a common ground in UX.
2. Focusing on discovering the most efficient and valuable UX factors.
3. Providing a deep comprehension of UCD in product design and innovation process.

## 2.1.4 Data Protection

### 2.1.4.1 User Studies in Data Protection

Before GDPR was implemented, studies of privacy policies and seeking user consent to data processing have been ongoing for nearly two decades [134]. A substantial body of research has explored the experiences of privacy policies and notices (e.g., [135–138]), novel privacy notification tools (e.g., [139–141]), and technical means to support privacy notice interfaces (e.g., [142, 143]). The increasing adoption of wearable devices and smart home products has resulted in interactions that are constrained (e.g., lack of interfaces). As such, finding user-friendly privacy notices for wearable and smart home products is difficult [58, 144].

Research suggests that consent interactions and privacy notices generally don't function well: users tend to ignore impactful privacy notices [145, 146], perceive them as a privacy threat [147] and are accustomed to “clicking away” consent interactions [148]. To improve consent interactions, researchers looked into improving mobile application notification permission requests. They found that nearly half of permission requests can be automated, which resulted in decreased user attention [149]. Machuletz and Böhme [150] suggested that GDPR-compliant consent

permission requests can similarly be automated. However, research into automating GDPR privacy notices is under-explored.

Since GDPR came into effect, many studies have investigated its impact on smart home users and devices [151–162]. More research emerged into facilitating GDPR-compliant consent notices. Ulbricht and Pallas [163] presented a privacy preference language, called YaPP, which complies with GDPR consent requirements in smart homes. Utz et al. [164] explored GDPR consent notices and found that ‘nudging’ practices were widespread and had strongly influenced user choices. They recommended that data protection regulation should explicitly state (e.g., clearer requirements and guidance) how consent has to be obtained. Mangini [165] conducted a survey study with users and organizations on the impact of GDPR’s right to erasure (‘right to be forgotten’) on privacy. They reported that companies found GDPR costly and difficult to implement while users strongly mistrusted the companies.

Another research has addressed the impact of GDPR on web interfaces. Anderson and von Seek [166] found that after GDPR, websites were collecting fewer cookies and users had the ability to inform themselves about data processing. However, GDPR did not result in more web transparency because policies were too long and complex. Machuletz and Bohme conducted an experiment with 150 university students in two countries and found that consent decisions were highly affected by highlighted buttons and the number of options offered [150]. Degeling et al. [167] measured the 500 most popular websites in the EU and found that websites were more transparent after GDPR, but there was a lack of user-centric tools to support users in consenting or denying access to their data.

Moreover, dark patterns used to steer or nudge users into consenting to data collection have been recently explored [164]. A dark pattern is defined as a “*user interface that has been carefully crafted with an understanding of human psychology to trick users into doing things they did not intend to.*” Dark patterns for privacy notices have been previously reported in the literature [168–171], protection organizations [172], whitepapers [173], and press articles [174]. For instance, Nouwens et al. [175] analyzed the most 10,000 websites visited in the UK and found that only 12% of the websites were free of dark patterns.

Dark patterns techniques reported in the literature include hiding away privacy-friendly choices, hiding advanced settings, preselecting checkboxes, requiring more effort to reject consent, and take-it-or-leave-it choices [171, 172]. The infamy of dark patterns has led California to outlaw them under the California Consumer Privacy Act (CCPA) [176] and EU data protection officers to explicitly cite dark patterns examples in their advisory documents [175].

#### 2.1.4.2 Economics of Personal Data

Personal data has been consistently described as the new “oil” of the internet [177, 178]. Bauer et al. describe personal data as “*one of the world’s most valuable commodities*” [179]. Tech giants such as Facebook and Google have based their business models on collecting and analyzing user data (e.g., Google [180]). While large companies were capitalizing on consumer data and demands for privacy, personal data markets (e.g., PFP (Paying For Privacy) and PDE (personal data economy) [180]) have been growing. Studies investigating and anticipating personal data markets [178, 181–184] date back to the 1990s. Personal data markets refer to an online destination where customers were compensated for their use of their data [185]. Personal data markets are often regarded as GDPR-compliant as they allow users to completely prevent their personal data from being used (compared to the “right to erasure”). However, since personal data use is highly regulated, existing personal data markets must navigate law’s gray areas or operate within regulatory restrictions (e.g., enforcement gaps, cross-jurisdiction arbitrage) [186].

Moreover, legislators and researchers have strongly advocated for enforcing property right (data ownership) regimes for personal data [187, 188] where data is treated as property. However, researchers argue that data property rights would not be effective in protecting user privacy. Data property rights would reduce privacy to a commodity, rely heavily on consumer choice, and are notoriously difficult to implement [189]. Further, the current notice-and-choice models (e.g., users clicking past privacy notices) system are already failing because users are unable to understand the potential uses of data, how it will be used, and the accompanying privacy risks [190]. Data property rights would face the same challenges of existing consent models because they rely entirely on individual control [191]. Other researchers argue that data property rights may result in scarcity of personal data and make business models entirely obsolete (e.g., [192]) which might hinder an economy’s potential to innovate (e.g., disruption to businesses, hardware supply chains and software development) [186].

Furthermore, measuring and estimating the monetary value of personal data have been a key focus to many researchers; different approaches include: examining market capitalization, examining revenues or net income per user, assessing the cost of data breaches and running economic experiments and surveys [193]. However, estimating the value of personal data has been previously reported to be difficult because personal data is highly context-dependent and lacks harmonization and measurable impacts over time [190, 193–195]. Previous studies that have attempted to explore price tags for personal data [196–198] were unsuccessful because user



privacy choices were affected by heuristics and biases (e.g., users' own valuations of their personal data) [195, 199]. Further, the monetary values of personal data cannot cover the full economic and social benefits [193].

Lastly, studies exploring privacy interactions from the perspectives of users and designers rarely consider the economic interests of product manufacturers or business leaders [150]. To our knowledge, previous smart home studies have not explored how the strategic interests of the business leaders conflict with the personal interests of the users.

## 2.1.5 Smart Home

### 2.1.5.1 Security in Smart Homes

Numerous concerns have emerged concerning the security of smart devices. Singh et al. [200] have identified numerous security issues in IoT such as identity management, cloud data transfer and management, certification, trust and compliance, the scale of IoT and cloud decentralization. As a result, smart home devices carry numerous security vulnerabilities such as unencrypted messages, weak authentication, SQL vulnerabilities and unverifiable software updates [201]. Those vulnerabilities could have catastrophic consequences. In September 2016, a malware called Mirai infected targeted smart devices with weak passwords and ended up infecting around 200,000 – 300,000 smart devices, launching distributed DDoS attacks on DNS provider Dyn [202]. Highly-trafficked websites such as Amazon.com, Netflix and Twitter were taken offline as a result [203]. Security experts regularly call for government regulation which could be vital to the security of IoT devices [204]. A legislation in California which came into effect in January 2020 required every IoT device to have reasonable security features *'appropriate to the nature and function of the device.'* [205].

### 2.1.5.2 Privacy in Smart Homes

Many people express worries that smart homes and privacy are incompatible. Ziegeldorf, Morchon and Wehrle analyzed privacy issues in smart homes and found that previous issues such as tracking, identification and profiling will worsen [206]. Novel smart home-related threats were found to be lifecycle transitions vulnerabilities, privacy violations and inventory threats [206]. A wide range of smart devices encrypt the data sent and received to protect it, however that doesn't fully protect user privacy. Acar et al. demonstrated machine learning-based methods which effectively attack encrypted communications within smart homes. The privacy attack can identify different types of smart home devices and monitor user activities,

states and actions [207]. Furthermore, law enforcement may eavesdrop or seek data from smart devices for many purposes which may cause egregious violations of individual privacy rights [208]. The head of Scotland Yard’s digital, cyber and forensics department stated that police officers are being trained to seek data from fridges, doorbells and washing machines [201].

### 2.1.5.3 UX in Smart Homes

Unlike desktop computing, smart home applications span across inter-connected physical and digital devices [209], increasing the complexity of UX design for smart homes [210]. While UX and usability guidelines are established for desktop systems and web applications, guidelines that specifically target smart home devices are under-researched [209, 211]. Moreover, smart home devices lack standardization and quality dimensions [212]. Some general UX rules are recommended for the design and implementation of smart home devices [213], but their effectiveness and suitability have not been explored in detail [214].

### 2.1.5.4 User Studies in Smart Homes

Privacy researchers have begun developing a body of work on people’s understandings, expectations, and concerns about how smart home devices—collect, use, and share data [215–220]. For example, Zeng et al. [219] interviewed 15 smart home users and found that their understanding of threats depended on the sophistication of their mental models. Similarly, Apthorpe et al. [221] surveyed 1731 users to measure users’ acceptability in the smart home data shared to different parties and extracted actionable recommendations and design best practices. Abdi et al. [222] conducted interviews with smart personal assistant users and found that they have incomplete mental models which lead to limited understanding of data storage and sharing.

Previous studies have explored security and privacy issues resulting from third parties (e.g., manufacturers, advertisers, government). For example, Malkin et al. [223] surveyed 116 smart speakers users and found that they are protective of the audio command history of non-users and that they strongly oppose third-party data tracking. Malkin et al. [224] also surveyed 591 smart TV users and found that users disagreed with their data being shared with other parties despite having a lack of understanding of laws and regulations that protect their rights. Similarly, Naeini et al. [225] conducted a vignette study with around 1,000 participants to investigate privacy expectations and preferences, and found that end-users are less comfortable with data collected privately (vs publically) and they would more likely consent to providing data if the practice is perceived as beneficial.

Many studies focus on how people’s preferences and concerns about data collection and sharing vary according to particular contextual and situational factors [224–229]. Geeng and Roesner [230] investigated multi-user interactions in the smart home with 18 users and found tensions during installation, normal use and long-term use. Most studies that compared locales for data collection found that people are more sensitive about data collected in their homes than, for example, in their workplaces or in business establishments [225, 227, 231, 232]. There is work that investigates how people think about privacy when the context for data collection blends features and norms from multiple contexts. Researchers have used the framework of Contextual Integrity (CI) [233, 234] to examine how people reason about data collection that blurs or crosses the boundary between private and public contexts (e.g., consumer profiling or RFID tracking). CI researchers have also examined how people think about smart-home devices based on (or not based on) norms about privacy in the home vs., for example, the Internet (e.g., [229, 235, 236]), finding that the crossing of contexts these devices represent can give rise to new considerations [237].

Personal data monitoring in smart homes has also been explored [238]. Choe et al. looked into audio and video sensing in the home and found significant tensions between married couples (e.g., concerns over divorce evidence), parents and their children (e.g., parent monitoring), and house owners and guests [215]. A study by He et al. found that smart home multi-users prefer control at function-level over access control per devices [239].

Some research has also focused on the concerns and perceptions of bystanders such as visitors to smart homes or co-habitants who did not make the choice to install smart devices [215, 219, 240]. For example, Yao et al. [241] conducted design activities with 18 smart home users and found factors affecting bystanders’ privacy perceptions. Some researchers [242] propose the use of the analytical framework of CI to research the privacy of domestic workers that are prone to be affected by smart devices, and the design process of product teams who build such devices.

#### **2.1.5.5 Developer Studies in Smart Homes**

There has been some work on current privacy practices in smart home product design, and to work on how to improve them [243–248]. For example, Bamberger and Mulligan [249] interviewed privacy officers viewed as leaders in the field to develop a model of how privacy is (or is not) operationalized in IoT companies. Their work demonstrates the importance of getting privacy knowledge and decision-making capability down to the level of product teams. However, an interview study by

Waldman [250] with product developers found that most companies do not actually do so—in other words, product teams mostly do not consider privacy in their decision-making. A few studies have examined how factors beyond the company level can encourage privacy-conscious decisions, for example in the mobile app development ecosystem [251, 252]. Baldini et al. [253] present an ethical-design-based framework for designing user privacy controls for smart homes, which we will use as an example in developing our content. Existing research has focused mostly on developers’ usable security and privacy practices [243, 254–256]. Assal and Chiasson [257] interviewed 20 developers to explore real-life software security practices during the development lifecycle and found that security was not considered in the design stage. Similarly, Waldman [250] interviewed product developers and found that product teams did not consider privacy in their decision-making. Previous research has found that many gaps existed between product teams and security experts, which included miscommunication and lack of security knowledge [258, 259]. As a result, they found that some companies contracted developers who were knowledgeable in security to act as an intermediary between product and security teams [260].

#### **2.1.5.6 UX in Smart Home Security and Privacy**

There is an increased focus on user-centered smart home security and privacy [219, 222, 229, 230, 261–263], however there has been little research into the wider aspects of security and privacy UX for smart home devices, and little work exploring how designers and their collaborators architect the UX of security and privacy for these smart home devices [9, 12]. In particular, there is a research gap in how designers consider UX during the security and privacy design/development of smart home devices. Bergman et al. [18] conducted a structured literature review of 150 smart home themed papers and found that there was no research into how product teams perceived or evaluated UX in the security or privacy design of smart home devices. Without an in-depth understanding of designers’ processes, challenges, and responsibilities, we argue that existing security and privacy issues in smart home devices will persist.

The literature suggests that security and privacy design may pose UX challenges for smart home product teams. Oh and Lee [264] analyzed reviews of quantified self applications and found that privacy was a key problem affecting both UX and security and privacy design processes. This was later confirmed by Bergman et al. [265], where they explored how 11 smart home companies captured UX requirements and found that security and privacy posed a UX challenge for designers. Rowland et

al. [266] found that designers often faced tensions between UX and security in smart homes (e.g., trade-off between strong authentication and ease of interaction).

Unlike desktop and mobile computing systems, smart home devices require data sharing over a network without human intervention. These computing devices typically generate a massive amount of data. With the proliferation of reliable and affordable consumer grade smart home devices, these smart and connected environments offer increased UX, which, in turn, will likely increase the pace of user demand for innovation. Despite the accelerated need for innovation, smart homes lack proper tools, guidelines and means to facilitate examination of new service/product experiences. In addition, smart and connected homes produce a collection of behavioral data through sensors and, thus, produces a rich, real-time data artifact. Such rich continual data can serve as the feedback for the designed artifact to adapt itself. However, it becomes challenging to use this data to provide information for creating new or modified interventions [127]. Because the data artifact contains detailed information about individuals, their environment, their behavior, and the outcomes of the behavior, it can facilitate the development of advanced models that can lead to a more nuanced and dynamic understanding of user reactions and behavior change over time [267, 268].

Despite the identified gaps and challenges, some existing works have attempted to tackle this challenge. Djamasbi and Strong [127] developed two conceptual models for UX-driven innovations in smart and connected environments (e.g., smart homes). The models outlined how to capitalize on the power of smart and connected environments to develop innovative experiences that are continually tested and improved by automatic experimentation and build advanced theories. Similarly, using Experiential Living Labs, Pallot et al. [269] presented a UX conceptual model and framework for smart homes. A Living Lab [211, 270] is a user-centered method which uses realistic environments to design and develop solutions. The methodology consists of observing and recording the behavior of smart home stakeholders (e.g., users) to initiate an iterative product design process and foster open innovation [270].

Finally, security and innovation might pose difficulties for UX designers. Security specialist Webroot and data center organization IO conducted a survey with 500 decision makers in IoT UK businesses. They found that 80% of participants postulate that security issues hinder innovation. In addition, 57% think that speedy and hurried innovation compromises security [271]. The results represent an interesting challenge within the context of smart homes where security and innovation do not align well in the product design process.

### 2.1.6 Summary

In this chapter, we reviewed the state-of-the-art of research relating to UX, usable security and privacy, product design, innovation and smart homes. We have identified major gaps in the literature that we summarize below:

- There is no consensus in the UX research and practitioner community on what are the different aspects of UX and what UX design means in technology companies. As such, there is no uniformly accepted UX definition or model in HCI that drives research.
- There is a knowledge gap between UX practice and HCI research due to limited explorations in this field. As a result, HCI research has been less accessible to UX professionals; and knowledge from UX professionals did not have strong significance in HCI research.
- Research at the intersection of HCI with security and privacy has been focused on usability in the past two decades. However, there was a strong need to consider the whole experience and not just usability as technology evolved and became embedded in everyday life. As such, the necessity to include principles from UX research into security and privacy research has become evident. UX encompasses not just usability, but emotions, feelings, and psychological responses.
- There is an increased focus on smart home security and privacy, however there has been little research into the wider aspects of UX of security and privacy for smart home devices, and little work exploring how designers and their collaborators architect the UX of security and privacy for these smart home devices. In particular, there is a research gap in how designers consider UX during the product design of security and privacy in smart home devices.
- The consensus in the field of HCI, design and business is highlighting the value of UX and UCD in product innovation. Integrating UX in product innovation allows stakeholders to solve new challenges that immature technologies (e.g., smart homes) bring to the table. However, it has been shown that it is difficult for design and development stakeholders to use those concepts due to mismatch between academia and industry and lack of research. Therefore, there is a need for more research in UCD and UX during the product design and innovation process.
- UX studies exploring privacy interactions from the perspectives of users and designers rarely consider the economic interests of product manufacturers or business leaders. There is a need for studies exploring how the strategic interests of the business leaders conflict with the personal interests of the users.

## 2.2 Research Approaches

We list common research approaches in this section. We clarify which methods we chose in this thesis in Section 3.1.

### 2.2.1 Information Security Approaches

#### 2.2.1.1 Theory Building

Theory building is the process of building a statement of concepts which shows how and why a phenomenon occurs. In IS, it consists of the development of ideas, concepts, methods, models (i.e., data, simulation, mathematical), simulation, and frameworks (i.e., conceptual, practical) [272]. Theory building focuses on more generalizability and less on practical relevance (e.g., impact on practical applications in a domain field) [272]. While theory building doesn't produce practical applications or systems, it is often used to propose research hypotheses, advise the design of scientific experiments, and run systematic observations [272].

#### 2.2.1.2 Experimentation

Experimentation sits between *observation* and *theory building* and aims to validate underlying theories (e.g., backward view on the research lifecycle) and address the challenges of technology transfer and acceptance (forward view on the research lifecycle) [272]. Experimentation is often driven by theory and made possible/smoothed by system development (e.g., consists of concept design, systems architectural design, prototyping, product development, and technology transfer [273]) where the results impact theories and systems [272].

#### 2.2.1.3 Observation

Observation is the acquisition of information from a primary source, often through the recording of data by using scientific instruments [272]. It is often used when there is little information known about the primary source. Case studies, field studies and sample surveys use the observation research methodology [273]. Observation studies have the advantage of collecting holistic and detailed insights that are more relevant to the domain of study [273]. As such, it can derive hypotheses for *experimentation* testing, or produce generalizations that can help other studies [272].

#### 2.2.1.4 Systems Development

Systems development is the process of defining, designing, testing, and implementing a new software application or program [274] and consists of a five-stage process: *concept design*, *constructing the system architecture*, *prototyping*, *product development*, and *technology transfer* [275]. Concept design adapts technological and theoretic advances into practical applications; Prototyping demonstrates feasibility of design ideas and concepts through proof-of-concepts; Product development involves the complete development and implementation of systems in production environment; Technology transfer represents the *ultimate success* of system development.

### 2.2.2 HCI Approaches

#### 2.2.2.1 Experimental Design

Experimental design is defined as the process of carrying out research in an objective and controlled environment with maximum precision to allow the extraction of conclusions that can validate or refute hypothesis statements [276]. In HCI, experimental design is used in laboratory-based and non-laboratory-based environments such as observations, field studies, interviews/focus groups, and controlled experiments [273, 277]. Experimental design studies are context-dependent and depend on many complex factors (e.g., study purpose, time, cost, participant availability). Experimental studies in HCI have limitations such as (i) inability to tackle weakly-defined issues, (ii) requiring strict control factors, and (iii) inability to represent typical interaction behaviors. [278].

#### 2.2.2.2 Survey Research

Survey research is defined as the set of information collected from the responses to questions from a sample of individuals [279]. Survey research allows for numerous methods to participant recruitment, data collection, and instrumentation methods [280]. Surveys are commonly used in descriptive research studies that are aimed at estimating specific parameters in a population, and describing their associations [281]. Usable security and privacy researchers have used surveys to explore security and privacy concerns, behaviors and needs [281–284].



### 2.2.2.3 Case Study

Case study research is the in-depth and detailed examination of case(s) within a real-world context and has been extensively practiced in social and natural sciences [285–287]. Case studies examine a phenomenon in its natural setting, through employing numerous data collection methods (e.g., from users, groups or organizations) [288, 289] without experimental control or manipulation. Case study research is most appropriate when study subjects are valuable and action contexts are critical [290, 291] It aims to represent particular contexts at a specific point in time. It attempts to capture and communicate the reality of a particular context at the point of study [273, 292].

### 2.2.2.4 Ethnography

Ethnography is a branch of anthropology and defined as the systematic and scientific study of individual cultures [293]. Ethnography studies cultural phenomena through the point of view of study subjects [294]. It is also a type of social research that provides rich, holistic insights into the participant’s social interactions, views, interpretations, perceptions of peoples, and behaviors in social situations and natural settings [273, 295]. Ethnography studies are conducted usually through the collection of detailed observations and interviews, lasting for long periods (e.g., at least 3 years) [296].

### 2.2.2.5 Diary Study

Diary study (also known as experience sampling or ecological momentary assessment (EMA)) is a research method that collects qualitative information by having users record entries about their everyday lives in a log, diary or journal about the activity or experience being studied [278]. Diary studies are longitudinal because they study participants over time. Diary studies benefit from offering a vast amount of contextual information (including scheduled tasks and personal reflections) without the costs of a true field study [297, 298] In HCI, diaries are useful in exploring usage patterns across different technologies, locations and environments [273, 299].

## 2.2.3 Usable Security & Privacy Approaches

The following methods have been used as usable security and privacy approaches.

### 2.2.3.1 Grounded theory

Grounded Theory (GT) is a systematic methodology involving the construction of hypotheses and theories through the collecting and analysis of data, often involving the application of inductive reasoning. GT enables the examination of topics and situations from many different angles, leading to comprehensive and deep explanations. It can uncover beliefs and meanings behind behaviors and events, through examining both rational and irrational aspects of behaviors. GT is well-fit for exploratory work and will allow the development of a substantive theory and deep explanation of processes. [300]. Flechais [301] used Grounded Theory [302] to identify factors that affect the design of security, and Nthala [273] used Grounded Theory [302] to identify the factors affecting security behaviors.

### 2.2.3.2 Content Analysis

Content analysis is a research tool used to determine the presence of certain words, themes, or concepts within some given qualitative data (i.e. text). Using content analysis, researchers can quantify and analyze the presence, meanings and relationships of such certain words, themes, or concepts ([303]). Content analysis can be used with qualitative and quantitative data, and was used by usable security and privacy researchers to identify links between human/organizational factors and security/privacy vulnerabilities [304–308]. While content analysis provides numeral description of text features [309], it remains purely descriptive (e.g., describes factors rather than motives or patterns).

### 2.2.3.3 Thematic Analysis

Thematic analysis is a common and foundational method of analysis of qualitative research [310]. It mainly involves identifying, analyzing, interpreting, and reporting patterns of meaning (known as themes or codes) from qualitative data [310, 311]. Thematic analysis can be based on themes derived from the literature [312]), or during the analysis ([313, 314]). Thematic analysis is better used with existing theoretical frameworks to provide interpretive power. The flexibility of thematic analysis makes the process of developing higher-level analysis challenging. Therefore, it can cause difficulties when deciding to focus on data aspects [310, 311].

#### **2.2.3.4 Action Research**

Action Research is [315] a five-step process composed of problem diagnosis, action planning, action taking, evaluating, and specifying learning. The aim of action research is to understand complex processes rather than deriving generalized rules or laws. Researchers used [301] Action Research to investigate socio-technical security design approaches through researcher interventions.

#### **2.2.3.5 Field Experiments**

Field experiments are studies using experimental design that occur in a natural setting. Field experiments consist of a mix of experimental designs, with various degrees of generality. Some criteria of generality include the authenticity of treatments, number of participants, different contexts, and outcome measures. Field experiments were used in evaluating security and privacy interventions [316, 317]. In addition, they were used to investigate how social proof could influence security and privacy behaviors of individuals [318].

*“Your job as leader of a UX team is much like that of a movie director: Your most important task is casting the right actors and getting them to work together as a team to meet the needs of both the business and the users.”*

— John Innes

# 3

## Methodology

### 3.1 Common Research Approaches

Our literature review (see Chapter 2) shows that smart home security and privacy experts adopted research approaches consisting of a mix of Information Security approaches, HCI approaches and usable security and privacy approaches. We summarize these approaches below:

#### 3.1.1 Information Security Approaches

Existing IS research efforts have investigated four core security issues: access to IS, secure communication, security management, development of secure IS. Security issues have been addressed in three major viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. Surveys reveal that most IS research has focused on technical aspects, and on issues of access to IS and secure communication [319]. Researchers have recognized that IS is a meta-subject that spans across suitable reference theories (e.g., psychology, sociology and semiotics) and various disciplines (e.g., social sciences, business, management, computer science) [320, 321]. As such, different researchers have adapted different fields and disciplines to answer IS research problems. Researchers have focused on studying the behavior, intentions and domination patterns of people using interpretivism – an approach to social science that opposes the positivism of natural science. Nthala [273]’s research shows that notable approaches adopted from different fields to fit IS research have been action research [315], surveys [284], case study [288], ethnography, [322]. IS experts argue for the pluralist methodology

[323], which aims to combine different research methods [272, 273]. Most notably, Nunamaker et al. [272]’s *multimethodological approach* to IS research combines common empirical and technical approaches: **theory building**, **experimentation** [317, 324], **observation** and **systems development**. In this thesis, we focused on the observation approach which is used when there is little information known about the primary source. We also focused on the theory building approach which helped with the development of ideas, concepts, methods, and frameworks. Observation studies have the advantage of collecting holistic and detailed insights that are more relevant to the UX of security and privacy in smart homes [273]. We provide more information about these approaches in Section 2.2.1.

### 3.1.2 HCI Approaches

Human-computer interaction (HCI) is a research field that interfaces between users and machines. HCI is interdisciplinary and often incorporates multiple disciplines, such as computer science, psychology, human factors, and ergonomics [325]. HCI research contributions can be grouped into seven different categories: empirical, artifact, methodological, dataset, theoretical, survey and opinion [278]. Most contributions belong to either into **empirical contributions**, interfaces, toolkits, architectures, mock-ups, and envisionments [273, 278] (e.g., qualitative and quantitative studies) or **artifact contributions** interfaces, toolkits, architectures, mock-ups, and envisionments [273, 278] (e.g., interfaces, toolkits, architectures, mock-ups, and environments). Nthala [273]’s research shows that prominent HCI research methods are: **experimental design**, **interview**, **case study**, **surveys**, and **diaries**. In this thesis, all our contributions fall into the HCI *empirical contributions* category. We conducted qualitative studies using HCI research methods such as interview, case study and diary. Beutement et al. [313] demonstrated that interviews and thematic analysis [310, 311], are a phenomenological approach suitable to study security and privacy behavior. In addition, we analyzed data consisting of diaries which benefit from having a vast amount of contextual information (including scheduled tasks and personal reflections) without the costs of a true field study [297, 298]. We provide more information about these approaches in Section 2.2.2.

### 3.1.3 Usable Security and Privacy Approaches

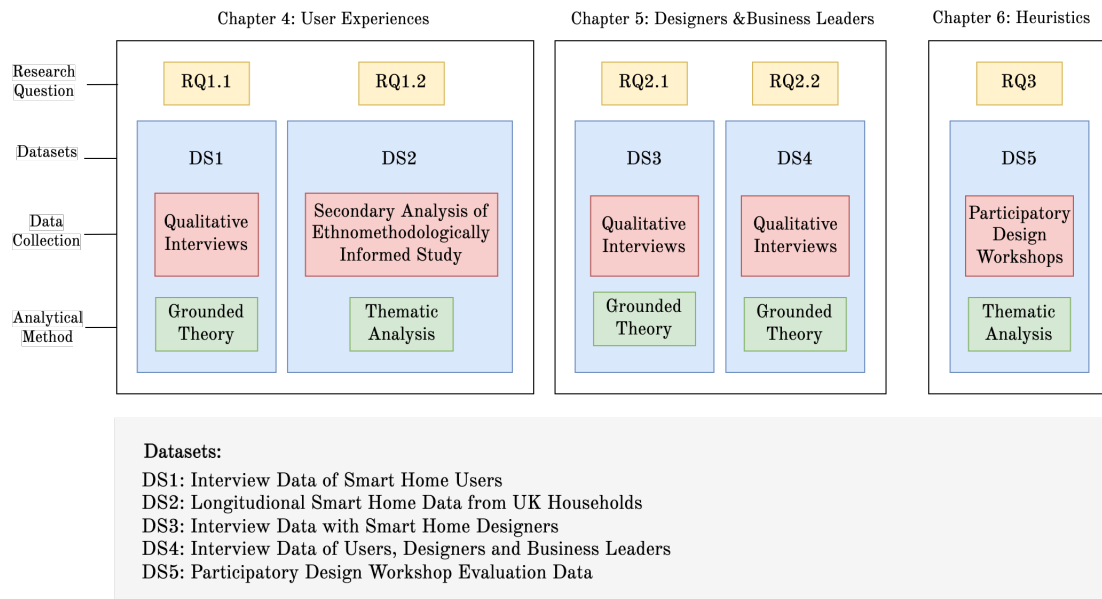
Saltzer and Schroeder stated in the 1970s that “*it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly*” [326] which is regarded as the birth of the ‘*Usable Security and Privacy*’ research area [327]. The rapid evolution this field has led to common research trends: understanding new technologies [328–330] (e.g., smart speakers, smart watches, smart glasses), designing for different stakeholders [331–333] (e.g., designers, developers, administrators), exploring novel application areas [334–336] (e.g., application of smart technologies in the home), extending and developing new technologies [337–340] (e.g., diary study, automated logging of interaction, post-hoc interviews) and learning from other disciplines (e.g., warning sciences, risk perception, and persuasive technologies) [341]. Studies of usable security and privacy attempt to bridge the gap between usability and traditional security and privacy [30, 333, 342] through qualitative and quantitative approaches. Qualitative approaches include **focus groups**, **content analysis**, **action research**, **grounded theory**, **interviews**, **thematic analysis**, and often aim to provide *in-depth understanding* of security and privacy practices in a given context. Conversely, quantitative approaches include **survey research**, **field experiments** and aim to build a *generalizable understanding* of security and privacy practices. In this thesis, we exclusively use qualitative approaches because qualitative research provides a deep dive into lived user experiences, allowing access to deep insights of unique experiences and needs of individuals. For example, we use Grounded Theory research as it enables the examination of topics and situations from many different angles, leading to comprehensive and deep explanations [300]. Similarly, we used Thematic Analysis to identify, analyze, interpret, and report patterns of meaning from qualitative data [310, 311] and also to derive themes from both the literature [312]) and during the analysis ([313, 314]). We provide more information about these approaches in Section 2.2.3.

## 3.2 Thesis Research Approach

To address the research questions of this thesis (see Section 1.3), our research method aims to (1) understanding smart home user perceptions and experiences (RQ1), (2) exploring smart home design from the perspectives of designers and business leaders (RQ2), (3) supporting design practices by disseminating heuristics and testing them through co-design workshops with stakeholders (RQ3).

### 3.2.1 Research Overview

Informed by our discussion of existing research approaches in relevant fields (see Section 3.1), we derived a research approach (see Figure 3.1) which allowed us to address our research questions sequentially and separately. We detail the next section why and how we employed our data collection and data analysis methods that resulted in five datasets.



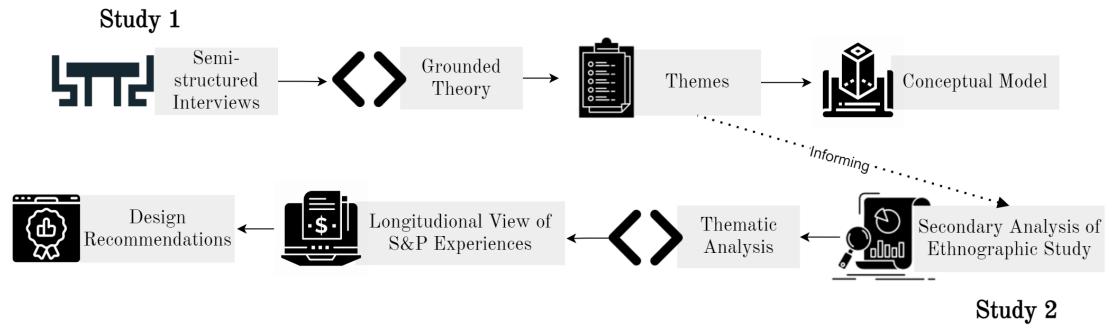
**Figure 3.1:** Research Approach

### 3.2.2 Research Methodology

In this section, we describe the research strategies and methods used to carry out the work reported in this thesis. Our research was carried out sequentially: starting with RQ1, then proceeding with RQ2 and RQ3.

#### 3.2.2.1 Understanding the Smart Home (RQ1)

The aim of RQ1 is to understand the relationship between UX, security and privacy in smart homes by investigating security and privacy user experiences and perceptions in smart homes. To tackle this research question, we conducted a preliminary and scoping study exploring UX of security and privacy with smart home users (see Section 4.1), followed by a secondary analysis of an ethnomethodologically informed study of UK households living with smart homes (see Section 4.2).



**Figure 3.2:** Summary of our two studies for RQ1

In the first study, we designed and conducted a qualitative study with 13 smart home users. Our preliminary and scoping investigation aimed to understand how smart home users perceive the importance of UX in relation to smart home products. We used purposive and theoretical sampling to recruit our participants which allowed us to select specific eligible participants and inform the sample size which was determined by saturation (see Section 4.1.2.2). We illustrate our participants’ demographics in Figure 4.1. We followed a semi-structured interview protocol, utilizing an interview guide to maintain direction while keeping the interview open for both breadth and depth topic exploration (see Section 4.1.2.3).

We analyzed the data using Grounded Theory, following Strauss and Corbin’s procedure [343]. Grounded Theory enables the examination of topics and situations from multiple perspectives, leading to comprehensive and in-depth explanations. It can uncover beliefs and meanings behind behaviors and events, by considering both rational and irrational aspects of behaviors [300]. Grounded Theory also allows for the development of a substantive theory, a thorough exploration of design processes, and the ability to derive grounded recommendations. We initially completed the initial coding of all interview transcripts and cross-checked the codes against the interview transcripts with the help of other researchers. At the same time, we reviewed the initial codes and the supporting quotes. We then grouped the codes into themes (using axial coding; relating codes to each other through a combination of inductive and deductive thinking) and categories (using selective coding; selecting one category to be the core category, and relating all other categories to that category). We provide further details in Section 4.1.2.5.

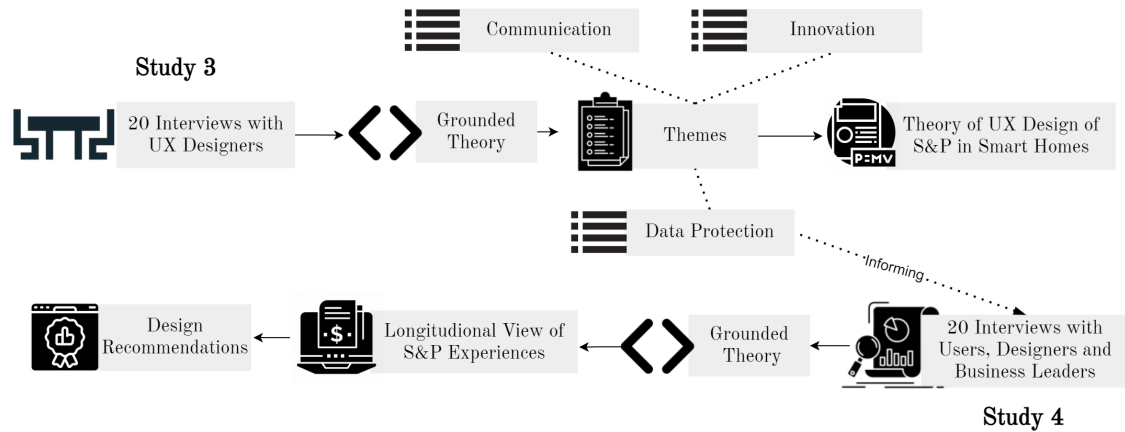
To validate our findings, we consolidated the existing literature and used meta-synthesis [344] to compare our results with the existing literature (see Section 4.1.2.5). A conceptual model, showing how UX factors affect the security and privacy of smart home users, was created from our study (see Figure 4.3). Our study methodology is described in detail in Section 4.1.



In the second study, we used themes and analysis from the first study to inform the secondary analysis of data collected from a six-month longitudinal study of smart device use in six households conducted as part of an ethnomethodologically informed study part of “Informing the Future of Smart Homes”, a research project funded by the Information Commissioner’s Office (ICO). Secondary analysis is a systematic method with procedural and evaluative steps for using existing data to address research questions different from ones used in original research [345, 346]. We chose to perform a secondary analysis of this data because it contained ethnomethodologically informed data detailing accounts of social culture and life in specific social contexts based on observations of what people actually do in the home (see Section 4.2.2.1). Unlike qualitative interview data, ethnomethodologically informed data can provide a detailed account of social culture and life in specific social contexts based on observations of what people actually do in the home. For example, participant observation data enables the researcher to observe and become integrated into the participants’ environment while also taking notes of the process [347]. Moreover, the data was highly relevant to our research question as it contained very detailed information pertaining to an elusive research population (parents and children) and to a sensitive topic (security and privacy). We describe the analyzed dataset in Section 4.2.2.2 and our participants demographics in Table 5.1. The ethnomethodologically informed data analyzed consisted of field notes, participant observation data, self-report data (participant diaries) and interview data (discussions with households) (see Section 4.2.2.2.3). We analyzed the data using iterative open coding [348] in accordance with Braun and Clark’s thematic analysis [310] (see Section 4.2.2.1.4). Thematic analysis allowed flexibility with regards to framing theory, research questions and research design. It also emphasized identifying, analyzing and interpreting patterns of meaning within qualitative data. We focused on security and privacy experiences over time, and clustered relevant codes into themes. Using our results, we were able to present a longitudinal view of smart home security and privacy experiences (see Section 4.2.3). Our methodology is described in detail in Section 4.2.2.

### 3.2.2.2 Exploring Smart Home Design (RQ2)

The aim of RQ2 is to understand the role of UX in the design of security, privacy and data protection in smart home products by investigating how UX stakeholders factor UX in the design of smart home products. To tackle this research question, we conducted a qualitative investigation of UX designers and their collaborators designing security and privacy in smart home products (see Section 5.1), followed



**Figure 3.3:** Summary of our two studies for RQ2

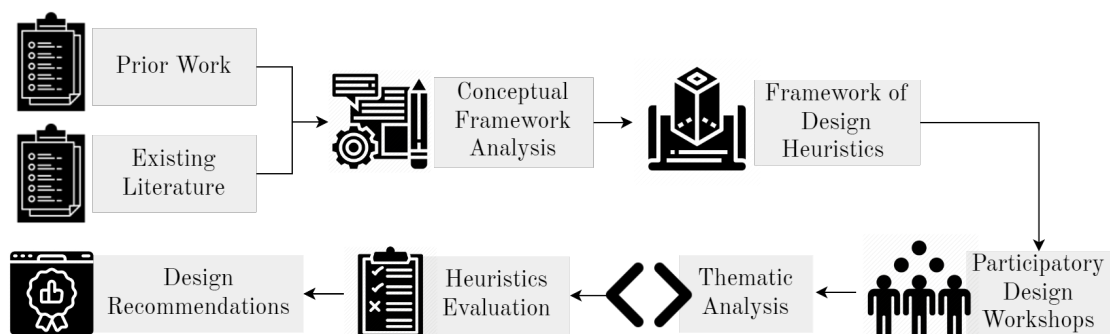
by a qualitative investigation of UX of data protection from the perspective of users, designers, and business leaders (see Section 5.2).

In the first study, we designed and conducted a qualitative user study [289, 349, 350] with 20 smart home UX designers and their collaborators (e.g., developers, managers) of three smart home companies that are located in the United Kingdom (UK), focusing on understanding the product design process in general and in relation to the UX design of security and privacy. We conducted semi-structured interviews with employees of three smart home companies (e.g., Company A (n=6), Company B (n=8), and Company C (n=6)) that designed and manufactured a wide range of smart home devices (see Section 5.1.2). To recruit our participants, we advertised the study on online platforms (e.g., LinkedIn) and used the snowball sampling, which allowed us to reach employees that were not easily accessible through other strategies (see Section 5.1.2.1). We describe our participant demographics in Section 5.1.3.1 and Table 5.1. Before conducting our study, we ran a pilot study with four smart home product designers at a local conference. We used the funnel technique [351] to structure our initial interview questionnaire (study script), starting with general questions and then drilling down to specific ones (see Section 5.1.2.2). We used Grounded Theory to analyze the interviews as described in Sections 3.2.2.1 and 5.1.2.4. Our results highlight smart home security and privacy challenges in smart homes: innovation, data protection and communication among stakeholders. We used our grounded-theoretic analysis to propose a theory showing the role of UX in the design of security and privacy in smart homes. Our methodology is described in detail in Section 5.1.2.

In the second study, we designed and conducted a qualitative user study focusing on understanding smart home data protection experiences and practices from the

perspectives of users (n=7), designers (n=6), and business leaders (n=6) in the United Kingdom. Our motivation to explore data protection user experiences was inspired by our previous study which revealed that data protection poses significant constraints and challenges in the design of security and privacy in smart homes (see Section 5.2.1). Furthermore, the UX of data protection is a designed encounter, the modalities of which arise out of a process that encompasses contextual, economic, regulatory compliance and strategic business priorities. As such, we included designers and business leaders to gain a wider understanding of the complexities and nuances of data protection. To recruit users, we posted flyers, distributed leaflets in the UK, and advertised the study on online platforms. As for designers and business leaders, we recruited a smart home consultant who facilitated referrals to around smart home designers and business leader contacts (see Section 5.2.2.1). We describe our participant demographics in Section 5.2.2.2 and Tables 5.4, 5.5, and 5.6. We derived a common set of interview questions for all participants to make our analysis feasible. However, each user group had their separate set of interview questions (see Section 5.2.2.3.1). Similar to our previous study, we used a funnel technique [351], starting with general questions and then drilling down to specific ones (see Sections 5.2.2.3.2, 5.2.2.3.3 and 5.2.2.3.4). We used Grounded Theory to analyze the interviews as described in Sections 3.2.2.1 and 5.2.2.5. Our analysis revealed that business leaders and designers experienced difficulties in identifying, applying, and tailoring suitable processes and practices for data protection for which some have developed “discount data protection”: shortcuts, heuristics, and common sense practices to overcome these challenges. Our methodology is described in detail in Section 5.2.2.

### 3.2.2.3 Design Heuristics for Smart Homes (RQ3)



**Figure 3.4:** Summary of our study for RQ3

The aim of RQ3 is to incorporate UX design into the security and privacy of smart home devices by extracting and evaluating heuristics into the security and privacy of smart homes. To tackle this research question, we constructed design heuristics using conceptual framework analysis from previously collected data and literature (see Section 6.2.1). We then engaged with groups of UX designers, developers, security engineers, and users in participatory design workshops to explore opportunities for the use of heuristics (see Section 6.2.2), and we systematically analyzed these workshops to evaluate the use of the heuristics (see Section 6.2.3).

In the first step, we used conceptual framework analysis (CFA) to generate heuristics of opportunities and challenges for user experiences of consent processes and permission requests. Conceptual framework analysis [352] has been used widely to create conceptual frameworks. The technique focuses on quantifying and tallying existing concepts and results in an overestimation of the similarity of texts [353]. As a consequence, this method is inappropriate to create theory from existing data sources [354]. We used data collected from our prior investigations in smart homes security and privacy in Chapter 4 and 5 as well as published studies and artifacts (see Section 6.2.1.1). This resulted in a design heuristics framework (see Figure 6.1) with three major themes: Knowledge, Consent and Communication. The framework consisted of (i) a description of lifestyles, process models, repurposing, reuse and usage and (ii) set of 32 design heuristics for smart home security and privacy design.

In the second step, we used participatory design (PD) workshops to present our framework and heuristics to participant groups (see Section 6.2.2.1). We recruited participants through online advertisements and snowball sampling (see Section 6.2.2.2). We conducted a pilot study to address any potential challenges (see Section 6.2.2.3). Participants were presented two problem scenarios: (i) design for consent interactions and (ii) design for permission interactions (see Section 6.2.2.1). We audio-recorded the workshops and collected notes, design ideas, collective feedback and pictures of any sketches. We used thematic and an open coding approach to extract relevant themes (see Section 6.2.2.4).

In the third step, we evaluated the usefulness and the application of the heuristics by individually examining design heuristics (see Section 6.2.3.1). Two researchers analyzed the design workshops with thematic analysis. We evaluated the heuristics based on how they were understood, the number of times referenced, their reception, and the goals they achieved (see Section 6.2.3.2). Our participant workshop demographics is described in Table 6.1 in Section 6.2.4. Our study methodology is described in detail in Section 6.2.

### 3.3 Research Ethics

All studies reported in this thesis were thoroughly reviewed and approved by the Central University Research Ethics Committee (CUREC). CUREC has overall responsibility<sup>1</sup> for policy on research involving human participants and personal data.

Before running each study, we asked participants to read an information sheet that explained the high-level purpose of the study and outlined our data-protection practices. We also asked participants to sign a consent form that presented all the information required in Article 14 of the EU General Data Protection Regulation (GDPR). We emphasized that all data collected was treated as strictly confidential and handled in accordance with the provisions of the UK Data Protection Act 1998 (registration no.: Z6364106/2015/08/61).

Due to the sensitivity of some of our interviews (e.g., privacy, security, compliance), we asked participants not to name specific people or sites so that the interviews will already be anonymous to some degree. All interviews were AES 256 encrypted and stored in a physical safe in our organization. Participants had the option to withdraw at any point during all our studies without providing an explanation. We explained to them that in such a case, none of their data would be used in the analysis.

We list the CUREC approval number of our studies in Table 3.1 below:

Chapter	Study	Curec Approval Number
Chapter 4	Study 1	CUREC/CS_C1A_19_024
Chapter 4	Study 2	CUREC/R59140/RE001
Chapter 5	Study 3-4	CUREC/CS_C1A_19_049
Chapter 6	Study 5	CUREC/CS_C1A_021_037

**Table 3.1:** Ethical Approval Information for Our Studies

<sup>1</sup><https://governance.admin.ox.ac.uk/central-university-research-ethics-committee>

*“User research is actually the way by which designer is able to step into the shoes of the user and go along his or her path feeling all the stones on the way.”*

— Tubik Studio

# 4

## Security and Privacy User Experiences

The purpose of this chapter is to explore the effect of UX on the security and privacy of smart home users. Therefore, this chapter tackles our first research question: *RQ1: What is the relationship between UX, security, and privacy in the smart home?*

To address our research question, we conducted exploratory-based interviews (see Section 4.1) where we investigated the following research question: *How do smart home users perceive the importance of UX in relation to smart home products?* Our exploratory-based interviews resulted in a (i) qualitative investigation of **user perceptions** and (ii) a **conceptual model** demonstrating how UX is linked to risk and balancing behavior. However, it lacked details about user behavior, contextual details, experiences over time, and insights into the real-life lived experience of smart home security and privacy. Therefore we asked the following question: *How do smart home users perceive security and privacy over time in different real-world contexts in relation to smart home products?* To address this, we conducted a longitudinal study (see Section 4.2) where we performed a secondary analysis of a six-month-long ethnomethodologically informed study observing smart technology use in six households (n=22). Our study resulted in (i) a qualitative investigation of **user behavior** and (ii) **longitudinal view** and analysis of security and privacy experiences in smart home products. We discuss the implications of our conducted studies in section 4.3.

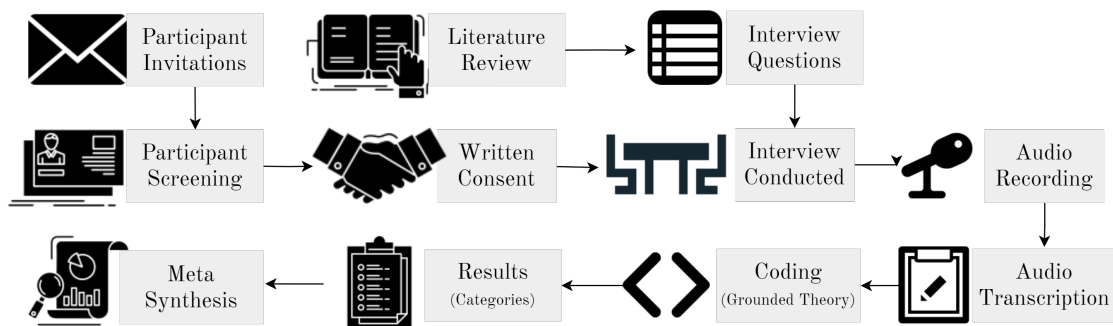
## 4.1 Perceptions of Security and Privacy

### 4.1.1 Motivation

While there have been efforts to increase security and privacy in smart home devices, the necessity of adopting a user-centered approach has been overlooked (e.g., they are barely tackled from a UX point of view). Only a small number of researchers have expressed the need for taking a human-factors approach to the security and privacy of smart home devices [9], Hence, the relationship between UX and the challenge of security and privacy in the context of the smart home is neither well understood nor well researched. To address this, we conduct a qualitative study with smart home users (n=13) where we explore how UX factors influence security and privacy perceptions in the smart home.

### 4.1.2 Methodology

Our study is exploratory with the aim of studying how UX factors affect security and privacy in smart home products, therefore we used a qualitative research approach (see Figure 4.1). Our approach consisted of collecting data using semi-structured thematic interviews. This exploratory approach will allow us to reveal new information from participants and uncover UX factors such as beliefs, feelings, emotions, thoughts, perceptions and motivations. Interviews conducted were semi-structured and one-on-one since they allow us to focus on individuals and explore UX factors in-depth and in-details.



**Figure 4.1:** Summary of our research methodology

#### 4.1.2.1 Recruitment

To recruit participants, we printed recruitment flyers and posted them in different department buildings. We also published announcements in local city forum posts (e.g., our city’s local subreddit [355]). Furthermore, we sent recruitment emails for participants using university-provided mailing lists. The recruitment message contained eligibility criteria and contact details. Initial communication with potential participants happened via university email.

#### 4.1.2.2 Sampling

We used purposive and theoretical sampling to recruit a sample of thirteen smart home users to participate in our research study. Purposive sampling allowed us to select specific eligible participants from preselected criteria. The eligibility criteria consisted of users who: (i) were at least 18 years old, (ii) used smart speakers in the past three months, (iii) were able to communicate in English and (iv) were able to give consent. Theoretical sampling allowed us to inform the sample size (n=13) which was determined based on theoretical saturation. We performed data analysis after each interview and we stopped recruitment when interviews did not provide any additional categories. The demography of the participants is summarized below in Table 4.1.

**Table 4.1:** Participant Demographics

ID	Age Group	Education	Gender	Device
P1	25-30	High School	F	Google Home
P2	30-35	High School	M	Amazon Echo Dot
P3	35-40	Bachelors	M	Amazon Echo Dot
P4	20-25	Bachelors	M	Google Home Mini
P5	20-25	Doctorate	M	Google Home
P6	20-25	Masters	M	Google Home, Apple HomePod
P7	35-40	Bachelors	M	Amazon Echo Dot
P8	20-25	Masters	M	Google Home Mini
P9	25-30	Masters	M	Amazon Echo Dot
P10	40-45	Masters	F	Amazon Echo, Amazon Echo Dot
P11	20-25	Bachelors	F	Amazon Echo Dot
P12	25-30	Masters	M	Amazon Echo
P13	25-30	Bachelors	M	Amazon Echo

#### 4.1.2.3 Data Collection

Interviewees were invited to attend the interview in person. The interviews were conducted within interview rooms in university buildings. Four participants could



not be present and were interviewed via Skype. The interview questions were based on the literature review conducted and tackled topics related to UX factors. All the interviews were audio-recorded using a recording device. Written notes were taken during the interview. The duration of the interviews varied between 28 minutes and 62 minutes. All the participants were thanked with a £10 (\$12) Amazon gift card voucher regardless of whether they completed the interview or not.

#### **4.1.2.4 Interview Process**

We first started with collecting necessary information from interviewees such as their age, gender, education, employment. We then asked about the number and type of smart home products that they use. We probed deeper into the environment of the smart home product. We asked interviewees to justify all of the decisions they have made such as reasons for using a smart home product, picking a particular brand and placement of the speaker in a particular location. We then asked them to explain how they understand the technology behind smart home products and discuss any unpleasant interactions. This was followed by an open-ended discussion of situations where the interviewees felt uncomfortable or uneasy around the smart home product.

Furthermore, we explored any security and privacy concerns participants had around the smart home product. Specifically, we asked if they had adequate security and privacy controls and if they take any measures to protect their security and privacy. Additionally, we inquired about how they felt about the collection and processing of their personal data. Our interview guide can be found in Section B.1.1.

#### **4.1.2.5 Data Analysis**

We transcribed and repeatedly read our interviews for familiarization with the present data. We used Grounded Theory to analyze the interviews as described in Section 3.2.2.1. We did not calculate Cohen's Kappa, as only the thesis author analyzed the interviews. Future studies in this thesis aim to address this limitation by involving other researchers in data analysis.

At the end of our coding process, we were able to identify an initial list of 144 informal codes from interview transcripts. The initial list of codes, where interview excerpts were grouped and conceptualized, included key UX-related factors discussed in our theory section. Additional extra codes and concepts that emerged from the analysis were added. When the initial coding was completed, the code's interview excerpts were rechecked to ensure that they are coherent and consistent. During these check-ups, changes to the codes were made. At the end of the analysis, we identified 127 codes. To validate our findings, we consolidated the existing literature and used meta-synthesis [344] to compare our results with the reviewed literature.

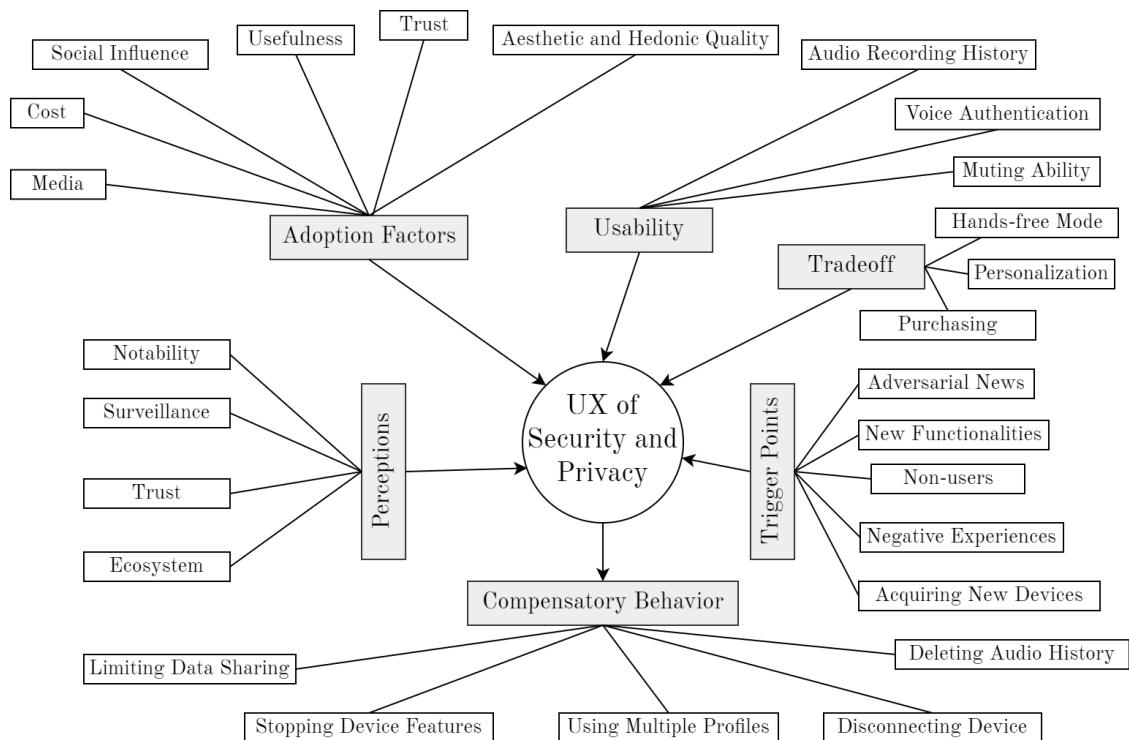
#### 4.1.2.6 Limitations

Most participants in this study were male (see Table 4.1) because our recruitment process had overwhelmingly male respondents. Future studies in this thesis will attempt to balance gender more through different recruitment approaches.

Moreover, we have interviewed smart home participants who clearly chose to use and adopt smart homes. Users of smart homes are not representative of all users. Non-users are likely to have different views and perceptions over the use of smart home products.

#### 4.1.3 Results

We extracted six categories (see Table 4.2) from our analysis (see Figure 4.2).



**Figure 4.2:** Summary of our categories and codes

##### 4.1.3.1 Perceptions and beliefs towards privacy resignation

Users express different perceptions and beliefs towards giving up their personal data to their smart speakers. We identified four perceptions and beliefs:

**Table 4.2:** Summary of extracted categories

<b>Perceptions and beliefs towards privacy resignation</b>
Perceptions leading to privacy resignation: perceived notability, government surveillance, trust, and product ecosystem.
<b>Usability and pragmatic quality of security and privacy controls</b>
Usability of smart speaker’s security and privacy controls: muting ability, voice authentication, and audio recording history.
<b>Influencers in the trade-off between privacy and convenience</b>
Features affecting the trade-off choice between privacy and convenience: personalization, hands-free mode, and purchasing.
<b>Factors and motivators affecting smart home adoption</b>
Factors determining smart home adoption: usefulness, trust, hedonic quality, cost, and social influence.
<b>Trigger points for security and privacy considerations</b>
Occasions prompting security and privacy considerations: adversarial news, non-users and negative experiences.
<b>Security and privacy compensatory behavior</b>
Reported compensatory behavior: limited use, disconnecting the device, stopping audio history and using multiple profiles.

**4.1.3.1.1 Perceived notability** Users of smart speakers are influenced by how notable they think they are. When discussing giving personal data to the speaker, five users said they’re not concerned about data collected by smart users because they have nothing to hide. Other users said they do not feel targeted by any external entities. When asked about concerns regarding their data being stolen, two participants responded by saying they are not an interesting target and don’t feel targeted as a result. P5 said: *“I think it’s easy to kind of get wrapped up in worrying about being followed or being tracked online. But in reality, probably not going to happen to us. We’re not a person of particular importance.”*

**4.1.3.1.2 Surveillance** Some participants dismissed privacy concerns since they believe that government and corporate surveillance can obtain their personal data. Quoting P7: *“At the end of the day, if government agencies want to see what I’m doing, they can. I’ll never know. So, what’s the point of worrying about it?”* Also, some participants dismissed smart home microphone concerns because they claimed they are no different than their smartphones. Quoting P6: *“Why does one smart speaker microphone make a difference? Some people wouldn’t talk around Alexa because it seems like an over-listening device. But also, ultimately, it is not that different from smartphones.”*

**4.1.3.1.3 Trust** All thirteen participants said that they trust their smart home manufacturer (e.g., Google, Apple, Amazon) to secure their personal data. As a result, they feel safe using the devices despite some saying that the companies might use it for “*targeted advertising*” (P6) and “*commercial gains*” (P1).

**4.1.3.1.4 Ecosystem** Some participants dismiss privacy concerns because their data is shared with the smart speaker’s manufacturer through their ecosystem. P6 who massively uses Google’s services (e.g., Gmail, Drive, Photos) thought that adding Google Home won’t make a difference. P6 said: “*I did think of the privacy of it. But once I saw how it was being used on, I thought about this whole Google ecosystem which I’m already tied into, I thought well*”. Similarly, P6 had used Amazon services for more than two decades and was comfortable using the Echo Dot in their home. Quoting P6: “*Amazon must have an incredible profile on me because I’ve used it for the last 20 years, they have a total profile of what my hobbies are, what I like and what I don’t like. So, I don’t care. Really.*”.

#### **4.1.3.2 Usability and Pragmatic Quality of Security and Privacy Controls.**

We explored the usability of common security and privacy controls.

**4.1.3.2.1 Muting ability** Some users wanted to mute the smart speakers for privacy reasons but were frustrated because the devices can only be physically muted. Quoting P10: “*This is unhelpful. Echo devices are on high shelves. I can’t just reach up and click it. I have to actually go and get it and pull it down and then press it. Being able to voice control would be more useful*”. Other participants went further by suggesting that they would be annoyed if the smart speaker is remotely muted because they will need “*to get up to unmute it, because it is not listening anymore*” (P11). P1 said they would prefer to have a temporary remote mute feature that would mute the device for a short period: “*I wish there was a feature where you tell Google not to listen to you for like 10 minutes and it starts listening to you again after 10 minutes.*”

**4.1.3.2.2 Audio Recording History** Most Amazon Echo users know that they can view their audio recordings using the Amazon app. Two participants said that they regularly delete their audio recording history as part of digital hygiene or housekeeping. Three participants described their stored history as “*pointless*”. Two participants who used Google Home said that they wanted to check their

queries online; however, they found the process to be complicated and confusing. Quoting P4: “*You needed to do like 7-8 steps to be able to see your voice commands. After a few minutes, I gave up.*”.

**4.1.3.2.3 Voice Authentication** Echo users expressed feelings of trust and security towards ordering from Amazon due to the Echo’s Purchase by Voice feature. The feature prompts Alexa to individually recognize voices using ‘Alexa Voice Profiles’ and reportedly is easy to set up and effortless. Quoting P3: “*It was easy to set up, Alexa made me say a couple of things and then it easily worked. If someone tries to use the Alexa in my house to order things, they won’t be able to, because the voice thing will be able to block it.*” Google Home’s voice authentication feature was not supported for UK households during the time of the interview.

#### 4.1.3.3 Trigger points for security and privacy considerations

We identified trigger points prompting users to reconsider their security and privacy.

**4.1.3.3.1 Adversarial news** Adversarial news originating from news stories or social contacts tend to prompt smart home users to consider what they share with the device. User P9 recalled a news article about Amazon: “*You could read in the past that Amazon had some issues with the data, for example, gave data from one person A to person B. They didn’t even know each other*”. In addition, P9 felt worried after finding a news article alleging that Alexa would recognize if they were ill.

**4.1.3.3.2 New Functionalities** New smart home functionalities might prompt users to question whether they would use smart speakers. While one participant had the Echo Show 5, which contains a camera, most participants were not comfortable with using a smart speaker with a camera. P11 considers microphones to be less concerning: “*It’s just cameras. It’s like having CCTV in your home. You don’t want people watching you eat peanut butter at 3 am in the morning. It’s a bit more concerning, I guess. Audio is less concerning than video for sure*”. In addition, when asking participants whether they would bank with their device, many have completely dismissed the idea.

**4.1.3.3.3 Non-users** Non-users of smart speakers prompt some users to consider their privacy around the device. P1 warns his guests about the device: “*I would tell my guests that the Google Home is listening to them. You know, if they have anything very private to say, or if they would want me to mute it, then I would mute it.*” P2, who possessed multiple Echo Dots at home and work, started having considerations about leaving it active when co-workers are around. P2 said that they have never muted the device at home but when they began using it at work, they thought that it was appropriate to mute it. Similarly, P13 expressed similar behavior when they had their client visiting them at home.

**4.1.3.3.4 Negative Experiences** Some users reported negative experiences during their use of smart speakers, which prompts them to consider their behavior. Participant P8 who had difficulties checking his Google Home audio log was able to review his logs eventually and discovered that multiple non-intended conversations were recorded. Quoting P8: “*I really thought the Google Home was innocent and all. Until I realized that a lot of unintended conversations were recorded, yikes*”. Another negative experience reported by P10 relates to the use of the purchasing feature by Amazon Echo. P10 discovered later that their son had made multiple orders from Amazon by tweaking the device settings. P10’s negative experience prompted them to consider whether the purchasing feature on their device is secure enough and whether it should remain activated.

**4.1.3.3.5 Acquiring New Devices** Acquiring a new smart home device for the first time might be a trigger point for privacy considerations. Participant P4 explained how receiving a Google Home as a gift triggered a privacy consideration: “*I didn’t want to get a smart speaker. And when I got it as a gift, I just kept it in the drawer. Then I thought: Hey, it’s not recording me randomly. Why would it be? And then, one time, I just put it on and slowly got over the fear of using them*”.

#### **4.1.3.4 Factors and motivators for smart home adoption**

We discovered six major factors and motivators for smart home adoption:

**4.1.3.4.1 Usefulness** Usefulness is the most common factor for smart home adoption. Before acquiring smart speakers, ten participants anticipated that the device would be useful, convenient, and would “*make life easier*” (P13). P1 purchased Google Home to be able to ask the assistant for quick questions: “*I thought the Google Home would be well equipped to answer my queries quickly.*” Other widespread purposes that users anticipated to be very useful were: playing music, managing their calendar, checking the weather, messaging and getting the news.

**4.1.3.4.2 Trust** Participants' trust for smart home manufacturers affects whether they would adopt a smart home product or not. P2 would not have purchased a smart home product if Google was the only company that manufactured those devices because they don't trust the company. P2 said, "*I really trust Amazon as a company, I've used many of their services before*". In contrast, P5 trusts Google and said: "*I like Amazon a lot actually, in terms of products and services. But I don't trust them as much as I trust Google*".

**4.1.3.4.3 Aesthetic and Hedonic Quality** The perceived aesthetic and hedonic quality of smart speakers influences their adoption. Before purchasing the product, P13 watched online videos and felt that the '*humanized voice of Alexa*' is satisfying. Not only were the aesthetics considered, but the size, looks and feels. Another user said that they were positively surprised by how small the Echo Dot was and they thought the small device can easily hide out of sight if needed. Other reported qualities that were considered are the audio quality of the device, as well as the color and mobility.

**4.1.3.4.4 Cost** The cost of smart speakers seems to play a significant factor in acquiring and adopting smart speakers. Eight participants had either got smart speakers for free or paid a small amount during a sale period. Participant P10 "*won one*" while P4 "*got it as a gift*". Other participants acquired the device during sales such as "*black friday sales*" (P11), "*prime day*" (P13) or during a "*promotion*" (P8). Participant P3 was torn between getting Amazon's Echo Dot or Apple's HomePod, but after finding a promotion online for the Echo Dot, they made their decision: "*The Apple stuff is too expensive. We got a deal for the Echo Dots for 30 quid*". Two participants said they would not have purchased their smart home device at the usual price sold.

**4.1.3.4.5 Social influence** Social contacts who own smart speakers seem to influence non-users into acquiring them. P6 bought their own Google Home after a Google Home Mini was set up at their family's house. Similarly, P11 purchased their own device after they used the smart home product of their partner a couple of times. P12 saw an Echo Dot at his cousin's residence before getting one: "*When I was at his place once, it looked like a very compact tool to have, I got jealous, and I thought that's a device that would like to have*".

**4.1.3.4.6 Media** Mass media also seems to influence or motivate users to purchase and use smart speakers. Two participants heard about smart speakers on the news before acquiring them. Quoting P7: *“I read an article in the newspaper and it said the next third generation of the Echo Dot is out. I saw something in the paper that was like, very interesting. I just thought this is going to be pretty cool. Actually, I was just kind of intrigued”*. Similarly, participant P1 had watched videos and read about the Google Home before making the purchase.

#### 4.1.3.5 Security and Privacy Compensatory Behavior

Users reported different cases of compensatory behavior.

**4.1.3.5.1 Deleting Audio history** When P8 went through his Google Home audio commands history and reviewed their audio history, the discovery of accidental recordings triggered compensatory behavior. Unintended conversations could be recorded by the accidental triggering of the smart home assistant (e.g., mishearing the wake words). After this experience, P8 mentioned that they regularly review and monitor audio commands and delete queries that are considered to be non-intended or malicious.

**4.1.3.5.2 Stopping Device Features** P10’s negative experience of having unauthorized purchases on their smart home product from their child prompted a compensatory behavior. P10 had contacted Amazon customer service and was able to turn off the purchasing feature from their smart speaker: *“I was able to chat with customer support and completely stop this feature from working on my Alexa.”* In that case, P10 had a negative experience that caused them to lose money, and this has led them to take a course of action and stop this feature from their Alexa device.

**4.1.3.5.3 Disconnecting Device** Another reported example of compensatory behavior involved participant P13 and his client. They were having a regular discussion at P13’s residence, which ought to be private and confidential. P13 had noticed that their client seemed very uncomfortable after spotting the Google Home’s LED Light showing *“running lights in white color”* which meant that Google Home was listening. P13 described the situation as very *“awkward.”* After facing this experience, P13 disconnects his smart speakers whenever they have a client visiting: *“We never discussed the matter. But whenever they are in my home, I make sure to plug off all the smart assistants”*.



**4.1.3.5.4 Using multiple Profiles** Two participants set separate profiles for security or privacy reasons. P3 had enabled different profiles on their account to be the only person able to make purchases on the Alexa app. Quoting P3: “*So they’re there, attached to me and set so that only I could make purchases through them.*” Another participant set up profiles on the Google Home to be able to receive personalized results on that without feeling uncomfortable. Personalized results include data from Google apps such as Photos, Calendar, Contacts, and Purchases [356].

**4.1.3.5.5 Limiting Data Sharing** P4 described themselves as “*cautious*” when using their Google Home. In particular, when sending a command to the device, they make sure no compromising information is sent. Quoting P4: “*I make sure I don’t say anything risky when it is recording. You know, I’m not going to, like, say my SSN out loud when it’s talking.*” Some participants do not completely adopt smart speakers. They express reservations when looking at different features. For instance, P11 said they would never use the purchasing feature in the device, whereas P13 said they refuse to give the Alexa app access to their iPhone’s list of contacts.

#### **4.1.3.6 Deliberations in Privacy/Security and UX Trade-off**

**4.1.3.6.1 Personalization** Smart assistants like Alexa, Siri, and Google Assistant are personalized; they tend to use customer’s data and audio logs to provide a personalized experience with the device. We asked users if they prefer a neutral smart assistant that does not store any of their personal data, which might reduce the UX with the smart speaker. Only one user said they wish to have a non-personalized assistant. Most participants said they prefer smart assistants that are personified, personalized and integrated into their daily lives. Some participants express numerous positive emotional reactions that heavily influence their trade-off choice. Quoting P12: “*I feel cognizant of the fact that sometimes I refer to the device as “the device”. But sometimes I’ll refer to the device as “she” or “her”. Kind of like humanizing the device in a sense.*” Many users utilize their smart speakers daily for different tasks at different times of the day and the devices seem to be integrated into their lifestyle. P10 discussing personalization: “*Alexa almost feels like a member of the family and we just love her. We want her to stay smart and remembering our details*”.

**4.1.3.6.2 Hands-free mode.** We asked participants if they prefer a version of smart speakers without the always-listening mode. 12 out of 13 participants dismissed the idea. When examining the trade-off between privacy and UX, they chose to sacrifice privacy for their comfort. Participants described a not-always-listening mode smart speaker as “*bothersome*” (P5), “*annoying*” (P1), “*a hassle*” (P12), “*difficult*” (P9) and “*defeating the purpose*” (P7) (P11). For disabled users, having a not always-listening mode could significantly impact their comfort. P10 weighted in “*I like the fact that I can wake up and ask what to do Alexa with my voice because I’m disabled, I can ask Alexa dozens of things to do for me without having to find my phone or another human being.*”.

**4.1.3.6.3 Purchasing** Both Google and Amazon allow users to purchase items through smart speakers. Some non-users of this feature said that they don’t trust the whole process of buying via the device. One participant was okay with using their smart speaker for small purchases but some felt “*uncomfortable sometimes for not knowing what is happening behind the scenes. Where is my credit card stored? What if they overcharged me?*” (P2). Participants who order via smart speakers expressed positive feelings, good UX, and trust towards purchasing and using the devices. Some users expressed feelings of trust and security from ordering off Amazon due to the Echo’s ‘Purchase by Voice’ feature. The feature prompts Alexa to recognize voices using “Alexa Voice Profiles” and as a result, only allows the smart speaker owner to order from Amazon.

## 4.1.4 Discussion

### 4.1.4.1 Privacy Design Recommendations

We discuss the following privacy design recommendations for smart home products:

**4.1.4.1.1 Improvements to muting** Amazon Echo and Google Home users cannot mute their smart speakers remotely (e.g., Alexa stop listening), which creates an inconvenience. For instance, disabled users suffer from significant disadvantages for not being able to mute their devices remotely. Manufacturers should add a device feature allowing users to remotely mute their speakers. Remote muting would require a physical trigger to unmute the device. Therefore, the feature should be accompanied by two complementary functions: *Temporary Remote Mute* and *Mobile App Unmute*. *Temporary Remote Mute* would allow participants to mute the speaker for a period of time (e.g., ‘Ok Google, stop listening for the remainder of the day.’).

*Mobile App Unmute* would allow users to unmute their devices via their mobile applications. Manufacturers of such applications should ensure that unmuting from apps is straightforward and easy to use (e.g., using GUI on/off toggle components).

**4.1.4.1.2 Support for multiple devices** It is not unlikely for household users to own multiple smart speakers. Having to remotely mute every device by voice may decrease the usefulness and usability. Manufacturers should support muting all (e.g., Hey Google mute all devices) or part of household devices from one device (e.g., Ok Alexa mute the living room speakers).

**4.1.4.1.3 Changing Privacy Default Settings** Google and Amazon store the audio history of their customers' commands by default. Google activates the 'Voice & Audio Activity' feature by default storing all of the customer's recordings. Similarly, Amazon turns on two features by default which permits their contractors to manually review a portion of the audio recordings. A significant number of our interviewees were not aware that their audio recordings are cataloged and stored. It seems highly unlikely that smart home users will go through the settings and disable features that pose a risk to their privacy or security (e.g., consenting to human review of their audio activity). Companies should ensure that privacy-preserving settings are switched on by default.

**4.1.4.1.4 Improvements to the audio logs feature.** While Google allows its customers to switch off the audio log activity feature, Amazon does not [357]. Users who do not want to have their audio activity stored would still need to delete their log from the device regularly – which would result in decreased UX.

**4.1.4.1.5 Private Mode** Some users mentioned that they would like to keep their audio recordings for practical reasons, which would increase the UX. Smart home manufacturers should introduce a private mode that is equivalent to the private mode of a web browser. Users who wish to have their activity logged could temporarily pause activity logging using the suggested private mode feature. The private mode could be complemented with two additional associated features: *Voice Activation* and *Associated Colors*. *Voice Activation* allows users to toggle the private mode by voice (e.g., Hey Alexa, turn on private mode). *Associated Colors* would change the color of the speaker to a specific color (e.g., red) when private mode is on.

#### 4.1.4.2 Security Design Recommendations

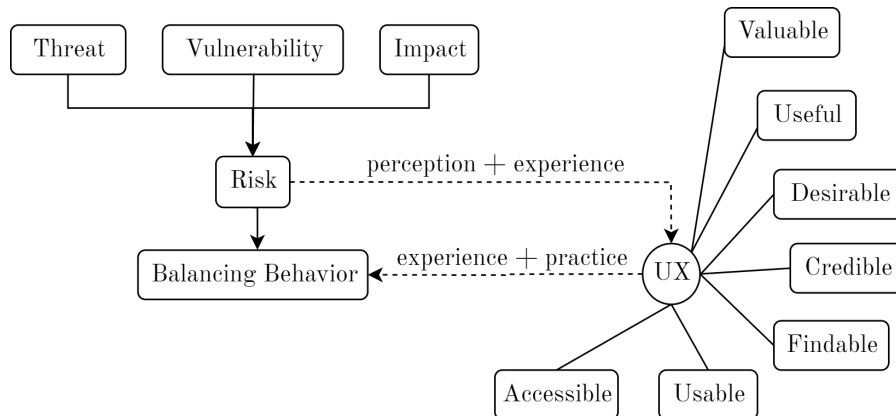
**4.1.4.2.1 Adding Security Layers to Voice Recognition** Voice Recognition technologies have a history of security vulnerabilities (e.g., voice impersonation attacks [358]). Many of our interviewees had difficulties trusting the voice recognition features available on smart speakers – Google uses ‘Voice Match’ whereas Amazon uses ‘Voice Recognition’. Smart home companies can add additional security layers to voice recognition (e.g., asking for memorable passphrases) – which is likely to increase the security and nurture trust.

**4.1.4.2.2 Offline Capabilities** While some participants use their devices for multiple and varied tasks, some report minimal use of the devices. Two participants have suggested they would like to use offline smart speakers. One of the participants’ uses of their smart speaker is limited to controlling their smart home. The three major commercial smart speakers send every user query to the cloud for processing even if the command was straightforward (e.g., ‘Alexa, shut off the lights’).

Creating an offline smart home product for performing basic tasks is possible. The company Sensory has developed an offline smart speaker that does not require any internet access. The device can perform voice recognition offline and perform many tasks such as setting the timer, control smart homes and playing music via Bluetooth [359]. Offline smart speakers nearly eliminate the security and privacy risks associated with cloud smart speakers.

#### 4.1.4.3 UX Effect on Risk and Balancing Behavior

Our results show that UX qualities (e.g., findable, desirable, credible) influence security and privacy in three areas: the perception of risk, the experience of harm and the mitigation practice. To present a model showing how UX affects behavior, we explored John Adam’s theory of risk compensation, which states that there is a “*risk thermostat*” influencing human behavior. The theory explains that users experiencing a safe lifestyle eventually seek out risky behavior; but overcompensate before returning to safety [360, 361]. Using the risk thermostat and our study findings, we proposed a conceptual model demonstrating how UX qualities interact with the concepts on risk and balancing behavior. In our model, the experience [17] of impact, vulnerability, and threat strongly influence users’ perceptions of risk which would affect balancing behavior (see Figure 4.3).



**Figure 4.3:** Conceptual model demonstrating UX effect on risk and balancing behavior

## 4.2 Longitudinal Aspects of Security and Privacy

### 4.2.1 Motivation

Previous work addressing security and privacy experiences in smart homes has been conducted using surveys, in-situ design evaluations and interviews. Smart home technologies have become more smart, invasive, and complex, resulting in the need to better understand security and privacy behaviors in real-world contexts over long periods of time. To address this, our research investigates the longitudinal aspects of user experiences of security and privacy by analyzing an ethnomethodologically informed study observing smart technology use in six households ( $n=22$ ) over a six-month period.

### 4.2.2 Methodology

The research reported in this section is based on the analysis of a six-month-long ethnomethodologically informed study of six UK households living in smart homes conducted as part of the ‘Informing the Future of Data Protection by Design and by Default’ project. The study consisted of:

1. planning workshops with participants where they selected smart home products for their home.
2. procuring and providing the chosen smart home products to participants.
3. observing the deployment, installation and use.

We carried out a secondary analysis of data collected which consisted of fieldnotes, photographs, unstructured interviews, and diaries. We chose to perform a secondary analysis of this data as (i) it is highly relevant to our research question, it contains very detailed information pertaining to both (ii) an elusive research population

(parents and children), and (iii) to a sensitive topic (security and privacy), and finally (iv) two researchers were directly involved in the primary study and thus already familiar with the data.

#### 4.2.2.1 Secondary Analysis

The secondary analysis we conducted followed the approach described by Johnston [362] which consists of forming the research questions, and identifying, evaluating, and then analyzing appropriate datasets.

**4.2.2.1.1 Developing the Research Question** The first step in the secondary analysis process is to formulate a research question. As described above, the gap in research, into the longitudinal aspects of security and privacy user experiences among households living in smart homes, prompted our research question: ‘What is the security and privacy experience over time in smart homes?’

**4.2.2.1.2 Identifying the Dataset** To identify a suitable dataset to answer our research question, we reviewed both past and currently available research in the field of usable security and privacy in smart homes. We selected the ‘Informing the Future of Data Protection by Design and by Default’ dataset on the basis of its suitability and familiarity. From a suitability perspective, our research question fits very well with the purpose of the original study since both studies focused on smart home product use. We found the ethnomethodologically informed dataset suitable for carrying out multiple interpretations and investigating different phenomena. Moreover, ethnomethodologically informed approaches of observing people and cultural groups are highly suitable for researching UX [363]. On a more practical note, several investigators from the primary study were available to provide detailed insights and contribute to the secondary analysis, which has proven to be instrumental in ensuring that secondary analysis remains faithful to the data.

We note that ethnomethodology is different from sociological approaches (e.g., sociology and psychology) even though all speak of social action [364]. Ethnomethodology was not established to repair or criticize traditional sociological approaches [365]. A key difference between sociological approaches and ethnomethodology is that ethnomethodology adopts a commonsense attitude towards knowledge [366].

**4.2.2.1.3 Evaluating the Dataset** We evaluated the data of the primary study to ensure its appropriateness and quality in advance of actual use. We were given access to and utilized all documentation on the collection of the data, and consulted and involved investigators from the primary ethnomethodologically informed study in order to complete this evaluation. We used Stewart and Kamins' [367] reflective approach to evaluate the data in a "*stepwise fashion*". The approach consisted of evaluative steps (e.g., [346, 368, 369]) to ensure congruence, quality of the primary study and the resulting dataset. The steps taken were determining (a) the purpose of the study; (b) the entities responsible for data collection; (c) what, when and how the information was obtained; and (d) the consistency of the information obtained.

**4.2.2.1.4 Analyzing the Data** The dataset consisted of diaries, fieldnotes and interviews which had been audio recorded and professionally transcribed. We coded this data using iterative open coding [348] in accordance with Braun and Clark's thematic analysis [310]. The thesis author and principal investigator both coded the data: the thesis author was not part of the data collection; however, the principal investigator collected the data in the original study. Throughout the coding process, the thesis author was able to ask for clarifications and additional insights while the principal investigator annotated the study data to provide additional context. Both coded the data focusing on home practices and experiences and developed an initial codebook. Triangulation was used to clarify and differentiate between conflicting meanings.

To verify the credibility of our codebook, a third researcher cross-checked the codes against the interview transcripts. At the same time, a fourth researcher reviewed the initial codes and supporting quotes. All researchers discussed any differences and generated a final codebook. We tested for inter-rater reliability. The average Cohen's kappa coefficient ( $\kappa$ ) for all codes in our data was 0.84. Cohen's kappa values over 0.80 indicate almost perfect agreement [370]. Further, we explored the codes to focus on evolving security and privacy experiences over time, and clustered relevant codes into themes.

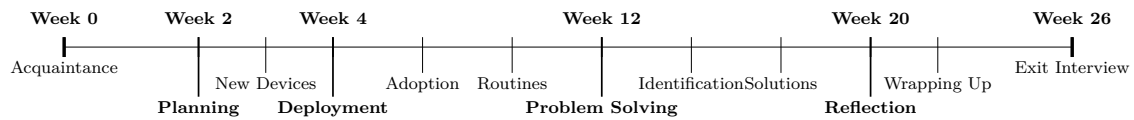
In total, the study material analyzed consisted of 47 interviews (~45 minutes per interview), 47 fieldnotes (~200 words per note), 13 participant diaries (~1,485 words per diary) and 22 photographs.

All the contributions presented in this chapter are solely the thesis author's contributions, additional researchers provided additional context during the analysis phase.

#### 4.2.2.2 Data Source

We describe in more detail the data provided by the ‘Informing the Future of Data Protection by Design and by Default’ project. The study researched communal use of smart technology in the home and used an ethnomethodologically informed study approach to observe six households setting up and using smart home devices over time. Materials from the study can be found in Appendix B.

**4.2.2.2.1 Description** The data was collected in four different phases (see Figure 4.4): planning (week 0-4), deployment (week 4-12), problem solving (week 12-20) and reflection (week 20-26). We describe three phases below.



**Figure 4.4:** Timeline of different phases of data collection

*Planning:* Participants were visited by a researcher who learned about their practices and conducted a planning workshop for selecting products. They were asked to sketch their floor plan and were provided with a budget and a card deck designed for the study which contained descriptions of different products (e.g., cost, compatibility and functionalities). Participants placed cards into their drawing based on available budget, household need and perceived benefits.

*Deployment:* Based on their choices in the planning phase, smart home products were then provided to households who installed, explored, and started to form routines. During the setup and installation phase, households negotiated occupant needs, device placement, configuration and usage. The researcher did not interfere in the setup phase except when asked to help. Households were then visited every two to four weeks over the next four months where informal and unstructured interviews were conducted.

*Reflection:* The study was concluded through exit interviews with participants. Participants were encouraged to share and discuss security and privacy experiences. Feedback was collected so that the study approach would be refined and improved. Household members contrasted and compared their own experiences with one another and reported frequent challenges experienced. Finally, the completed participant diaries were collected.



**4.2.2.2.2 Recruitment** To recruit participants, the study was advertised on social media and online platforms. Interested participants were asked to complete an online screening questionnaire. The study aimed to recruit demographically-diverse dual-income families that are in favor of technology adoption [371]. Hence, demographic questions about gender, age, educational level, employment status and household income were included. Additionally, participants were asked to specify the smart products they own and use, or intend to purchase. They were also asked to describe their existing knowledge of smart products, and their interest behind wanting to participate.

Different levels of technical competence were defined (Novice, Competent, Expert) using a simplified Dreyfus model of skill acquisition [372]. Dreyfus' model has been widely used to define levels for assessing one's competence. Participants were asked to report their own and their household members' skill level using the recruitment questionnaire. Our recruitment questionnaire form can be found in Appendix B.2.1.

**4.2.2.2.3 Data Collection** Data collection tools consisted of unstructured group interviews, fieldnotes and diaries.

*Unstructured group interviews:* Observing households in real-life settings is difficult [373]. Instead, unstructured group interviews were conducted during all visits. Such interviews enable conversational groups within households which allows observation of open and unfettered discussions [373]. Interviews depended on the availability of household members and took place in communal living spaces. Interview prompts were based on information from diaries and previous visits. They focused on eliciting information about experiences and practices. Interviews conducted after March 2020 were moved online due to the COVID-19 lockdown.

*Researcher fieldnotes:* To gain insight into cultural practices and phenomena, descriptive and reflective field notes [374] were collected in line with Yin's best practices for recording qualitative field notes [375]. Descriptive field notes consisted of time and date, present family members, their conduct, remarkable interactions, and a general reflection on the home visit. Reflective information consisted of the researcher's reflections about the observation being conducted and included ideas, questions, concerns, and related thoughts. Deployment notes and photos can be found in Appendix B.2.3.

*Participant diaries:* To gain longer and regular insight into lived experiences, diaries were provided to participants who were encouraged to report their experiences regularly. A diary study template was used that listed an example entry, the project

aims, list of questions and minimum entry expectations (e.g., at least two entries per week). Questions asked about instances of shared use, comments on interactions with new devices, likes/dislikes, and positive/negative experiences. Diary options offered were both paper-based and digital. Diaries used can be found in Appendix B.2.2. The data described above was collected in five stages that we describe below:

1. **Acquainting Phase:** Research lead sets up introductory meetings with households to learn about existing practices and environment.
2. **Planning Phase:** Research lead prepares and plans the introduction of new smart home products to households. Households plan their smart home by choosing their devices from a deck of cards.
3. **Deployment Phase:** Research lead brings new smart home devices to households that are observed configuring and installing the devices.
4. **Post-Deployment Phase:** – Research lead observes participants two weeks after the households have deployed and begun using the devices.
5. **Wrapping-up Phase:** – concluding the study by contrasting and comparing household experiences in discussion with the researcher.

#### 4.2.2.3 Participant Demographics

Table 4.3 summarizes the demographics of our sample consisting of 22 participants from six households. Households included twelve male and ten female participants. Seven reported having an undergraduate degree, and five a graduate degree. Twelve participants were working age adults (30-49) and eight participants were school-age children and young adolescents (8-17). Two members were too young to participate (1-3). Three households had not used smart products before. Five households consisted of a family structure (two parents and children) and one consisted of a couple.

#### 4.2.2.4 Research Ethics

As described in Section 3.3, this study was reviewed and approved by CUREC which determined that the secondary analysis was consistent with the consent given by participants in the original study (R59140/RE001) and did not require additional consent. Participants kept the smart home products provided to them; and no data was accessed from these products. Each household was compensated with £200.

**Table 4.3:** Participant Demographics

H# (Income)	P#	Age	Alias (Gender)	Occupation	Role	Education	Competence	Smart Home Devices
H1 (£70k-£80k)	H1a	40-49	Rosa (F)	Practice Manager	Mother	Postgraduate	Competent	1x Smart Speaker (Amazon Echo Dot)
	H1b	40-49	Jaco (M)	Automotive Auditor	Father	Undergraduate	Competent	1x Smart Display (Amazon Echo Show 5)
	H1c	16-18	Iria (F)	No occupation	Daughter	High School	Competent	1x Smart Camera (Arlo Pro Smart Home-Security CCTV Camera System VMS4330)
	H1d	06-08	Peter (M)	No occupation	Son	Elementary School	Novice	1x Base Station (Arlo Base Station)
	H1e	01-03	Tom (M)	No occupation	Son	None	Novice	1x Smart Television (Samsung TV)
	H1f	16-18	None (M)	No occupation	Lodger	High School	Varying	1x Smart Meter (British Gas)
H2 (£70k-£80k)	H2a	30-39	Monique (F)	Comms Manager	Mother	Undergraduate	Competent	2x Smart Speakers (Google Home Mini)
	H2b	40-49	Adam (M)	IT manager	Father	Undergraduate	Competent	1x Smart Display (Google Nest Hub)
	H2c	01-03	Eric (M)	No occupation	Son	None	Competent	1x Smart Camera (Arlo Pro Camera)
H3 (£40k-£50k)	H3a	40-49	Carrie (F)	Support Teacher	Mother	Postgraduate	Competent	1x Smart Speaker (Google Home Mini)
	H3b	40-49	Paul (F)	No occupation	Father	Undergraduate	Competent	1x Smart Display (Google Hub Max)
	H3c	10-12	Felicity (F)	No occupation	Daughter	Middle School	Competent	1x Streaming Device (Google Chromecast) 1x Smart Thermostat (Tado Thermostat)
H4 (£60k-£70k)	H4a	40-49	Carla (F)	UX designer	Mother	Postgraduate	Competent	3x Smart Speaker (Home Mini, Echo)
	H4b	40-49	Aaron (M)	Media Design Teacher	Father	Undergraduate	Expert	1x Smart Display (Google Echo Show 5)
	H4c	10-13	Malte (M)	No occupation	Son	Primary School	Competent	1x Smart Camera (Arlo Pro Camera)
	H4d	08-10	Ester (F)	No occupation	Daughter	Primary School	Novice	1x Smart Light (Philips Hue) 1x Smart Television (Samsung TV)
H5 (£70k-£80k)	H5a	40-49	Frank (M)	Innovation Manager	Father	Postgraduate	Expert	2x Smart Speakers (Amazon Echo, Pure)
	H5b	40-49	Cassie (F)	Furniture Restoration	Mother	Undergraduate	Expert	1x Smart Display (Amazon Echo Show 5)
	H5c	08-10	Donald (M)	No occupation	Son	Primary School	Competent	3x Streaming Device (Apple TV, Samsung)
	H5d	06-08	Fabian (M)	No occupation	Son	Primary School	Novice	2x Smart Lights (Philips Hue bulbs) 2x Smart Thermostat (Tado)
H6 (£100k-£150k)	H6a	30-39	Tobias (M)	Innovation Director	Husband	Postgraduate	Expert	1x Smart Display (Amazon Echo Show 5) 1x Streaming Device (Apple TV 4K)
	H6b	30-39	Sylvie (F)	Midwife	Wife	Undergraduate	Novice	2x Smart Bridge (Tado, Philips Hue) 4x Smart Plug (WiFiPlug Home 2.0) 8x Smart Switch/Bulb (Philips Hue)

#### 4.2.2.5 Limitations

First, a major limitation inherent in the nature of secondary data analysis is that the data used was not collected to address our research questions [367, 369]. To address this limitation, we followed a process of careful reflective examination and critical evaluation of the data to ensure a match between our research questions and the existing data.

Second, the data collected might not have captured all aspects of the experience of security and privacy. Had we explicitly gathered the data, more population subgroups and geographic regions may have been considered; which might have made security and privacy experiences more apparent.

Third, not every researcher was involved in the original study or data collection process, and as a result some were not aware of the nuances of the collected data or the rich detail of the observed socio-cultural phenomena. To address this limitation, we jointly performed our study analysis with the researcher that collected the data in the primary study (who provided study-specific nuances and insights in the data collection process). We also consulted with other investigators from the original study to ensure our analysis was a valid interpretation of the original study's data.

### 4.2.3 Results

In this section, we present our findings. We discuss our key themes: the experience of privacy (Section 4.2.3.1), the experience of security (Section 4.2.3.3) and technology repurposing (Section 4.2.3.4);



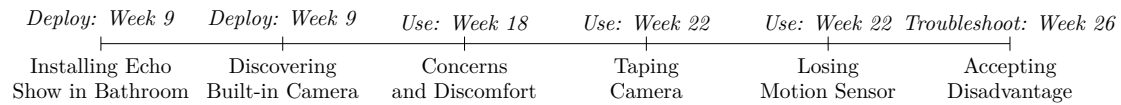
**Figure 4.5:** Smart products deployed in household four. Images from left to right: (a) Arlo Pro security camera at the front entry door, (b) Arlo Pro security camera in the bedroom, (c) Philips Hue light bulb in the bedroom, (d) Amazon Echo smart speaker in the bedroom, (e) Google Home smart speaker in the bedroom and (f) Amazon Echo Show smart display in the bathroom.

#### 4.2.3.1 The Experience of Privacy

We use the term ‘*experience of privacy*’ to refer to a person’s privacy-related perceptions and responses that result from the use or anticipated use of a product, system or service. Participants’ privacy experiences consisted of *feelings of intrusiveness* (Section 4.2.3.1.1), *tracking concerns* (Section 4.2.3.1.2), and *privacy management* (Section 4.2.3.2).

**4.2.3.1.1 Intrusiveness** Intrusiveness was experienced by the discovery and use of cameras and microphones.

**Cameras:** Participants (n=10) expressed concerns over security cameras (e.g., Arlo Pro) and smart display cameras (e.g., Echo Show 5). In H1, Jaco H1b and Iria H1c were concerned after discovering a camera in an Echo Show 5; but they were reassured by Rosa H1a who said that the camera can be muted anytime. In H4, Carla H4a and Aaron H4b installed smart displays in different rooms in the house to increase utility and connectivity. However, they were worried about the ones placed in sensitive locations (e.g., bedroom, bathroom). Aaron H4b stated it was ‘*unethical*’ to add cameras in children’s bedrooms. He explained: “*You realize that some people literally have one of those in their children’s bedrooms watching their children sleep, you know. [...] That is really creepy.*” However, Aaron H4b



**Figure 4.6:** Timeline illustrating H4’s privacy experiences with the Echo Show 5 over time.

placed an Arlo Pro security camera at the front entrance door because he did not consider it to be a private space (see Figure 4.5a).

**Microphones:** Participants (n=3) expressed privacy concerns over microphones found in smart speakers (e.g., Amazon Echo, Google Home) and displays (e.g., Echo Show 5) due to their *always-listening* capabilities. In H1, Iria H1c explained that she mutes her Echo Show during sleep: “*I put it on the ‘do not disturb’ one so when you press it, the red light comes on. And I do not know, it could still be listening.*” In H3, Carrie H3a was worried the device would listen to her conversations. She wrote in her diary: “*I also wondered how much of what I was saying was being captured and passed on, including things I wasn’t saying to the Google Home.*” In H2, Adam H2b was initially ‘*scared*’ of using Google Home speakers but later ‘*felt comfortable*’ because he ‘*had the control to stop it*’ through the physical-mute button.

**4.2.3.1.2 Tracking** Participants (n=5) were worried about tracking of their behavior and activities by manufacturers (e.g., Google, Amazon). In H1, Rosa H1a read on Mumsnet – a forum website for parents – an article claiming that Alexa is tracking all household activities. She believed that the manufacturer was listening to the household’s conversations to target them with advertisements. She said: ‘*I think they are listening to us.*’ Jaco H1b echoed Rosa H1a’s belief and added that private companies (e.g., Amazon) cannot be trusted. In H2, Adam H2b feared that his Google Home might create an ‘*invasion of privacy*’ and ‘*start throwing adverts*’. In H4, Aaron H4b was concerned that the Echo Show 5 was displaying targeted and personalized advertisements after finding news and advertisements that could not be hidden.

#### 4.2.3.2 Management of Privacy

We describe how privacy experiences were managed below:

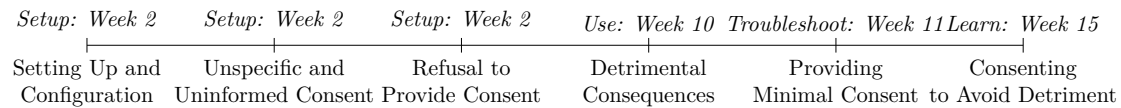
**4.2.3.2.1 Privacy Experiences** Participants managed negative privacy experiences (e.g., intrusiveness) and needs through a three-step process of (i) developing awareness of data collection, processing and use (ii) making decisions based on risks and benefits, and (iii) taking action through behaviors and attitudes.

**Awareness:** Awareness refers to a user's attention and cognition in relation to the control, use, and disclosure of personal data. Participants (n=9) developed privacy awareness through learning (i) how their personal data is processed and used, and (ii) which personal information is received by companies (e.g., home presence, activities). In H4, Aaron H4b enabled the '*Follow-Up Mode*' feature on Amazon Alexa which allows for successive requests without repeating the wake word; but he was worried about recordings of his private conversations (see Figure 4.5d). He said: "*The issue with this is that more of our private conversations have the potential to be recorded.*" In H2, Adam H2b was concerned that his Google Home data would be '*mined*' and '*exploited*' for the provision of free services (e.g., Google Assistant).

**Decision making:** Decision making refers to a user's process of making privacy-related decisions. Participants (n=8) made decisions based on weighing risks and benefits. In H4, Carla H4a and Aaron H4b believed that providing personal data (e.g., home footage) to the Arlo Pro security camera was required to receive useful and personalized services (see Figure 4.5b). Carla H4a said: "*If you want to give people good services and personalization, you need their data.*" In H3, Carrie H3a was prompted to provide her home address to the Google Home during setup to be able to query for local places, weather, and time. Unwilling to provide her home address, Carrie H3a provided the address of a nearby street instead; which protected her address without hindering the ability to query for local information.

**Action:** Action refers to the privacy behavior and attitude of users. Participants' (n=12) action consisted of (i) using physical privacy controls and (ii) managing personal information. Physical privacy controls strongly alleviated concerns of monitoring, listening and tracking. In H4, the camera of an Amazon Echo Show 5 placed in the bathroom created privacy concerns (see Figure 4.5f). Aaron H4b enabled the built-in camera shutter which provided assurance. He explained: "*It physically puts something in front of it, so actually it is perfectly safe to have it in a bathroom*" (see Figure 4.6). In H3, Carrie H3a covered the camera of the Google Hub Max with a sticker. Moreover, personal data (e.g., audio logs, video footage) collected by smart products were reviewed and often deleted. In H4, Aaron H4b reviewed the audio history stored by Alexa's mobile application and configured his audio history to be periodically deleted.

**4.2.3.2.2 Management of Consent** Privacy concerns were managed through consent preferences (e.g., privacy permissions). Consent management was inconsistent: *granting consent* (e.g., H1) was straightforward, but *withholding consent* (e.g., H3, H4) caused detriment and prompted reconfiguration of consent preferences (see Figure 4.7).



**Figure 4.7:** Timeline illustrating H3's consent experiences with the Google Home over time

**Granting consent:** Participants (n=10) consented to providing some of their personal data during setup and use. Granting consent was a quick and effortless experience among users. In H1, Rosa H1a and Jaco H1b granted consent during setup of the Echo Dot and the Echo Show 5, and did not revisit their preferences later during use.

**Withholding consent:** Participants (n=4) withheld consent by explicitly rejecting smart home privacy permission requests. In H2, Adam H2b refused to provide 'financial details' to Amazon Echo. Some permission requests were unspecific (e.g., vaguely worded, confusing terminology) and unjustified. In H3, Carrie H3a rejected permission requests to access her mobile phone's storage, calendar data and contact details as she did not see the need. In H4, Carla H4a was puzzled when prompted to save audio interactions inside 'Web & Activity' tracking in her Google account. In H3, Felicity H3c was confused when asked to enable personalisation and provide contact details while setting up Spotify on her Google Home. She asked: "Do you think we should [say] no thanks? Do we really need all this?"

**Managing consent:** Participants (n=2) managed their consent settings through preference-management tools. Some settings were difficult to find or non-existent which prevented participants from managing consent as needed. In H3, Carrie H3a was unable to withhold consent for certain data collected when configuring her Google Home device. Instead, she was only informed of the data collected. She said: "It did not give me an option to decline, I do not think. It has just given me information." In H4, Carla H4a was frustrated over her inability to find privacy settings in her device.

**Detriment from withholding consent:** Participants (n=2) faced problems from withholding consent. Some were unable to set up products or use certain features. In H3, Carrie H3a was unable to set up her Google Home because it required

‘location services’ on her Android phone to be enabled; a location tracking feature that Carrie H3a refused to activate. She said: “*I do not really want somebody following me around where I am going all the time.*” Moreover, Carrie H3a refused to enable ‘Web & Activity’ tracking when setting up a Google Nest Mini. As a result, she was unable to play music on the device as streaming required ‘Web & Activity’ tracking to be activated [376]. In H4, Aaron H4b obscured the camera of the Echo Show (see Figure 4.6) using a built-in physical shutter. However, Aaron H4b lost access to the device’s motion detector, which used the camera to function to wake up the device when someone was in range.

**Troubleshooting consent:** Participants that experienced detriment from withholding consent revisited their preferences. In H3, Carrie H3a revisited her privacy settings and activated ‘Web & Activity’ tracking to be able to stream music. She said: “*You have to be willing for some kind of data to be collected. [...] We cannot do anything about that otherwise we lose YouTube.*” Carrie H3a also temporarily enabled *location services* to set up her Google Home. Over time, Carrie H3a learned to automatically consent to ‘Web & Activity’ tracking when setting up Google Home devices.

#### 4.2.3.3 The Experience of Security

We use the term ‘*experience of security*’ to refer to a person’s security-related perceptions and responses that result from the use or anticipated use of a product, system or service. We describe security experiences below:

**4.2.3.3.1 Security Experiences** We report observed security experiences below:

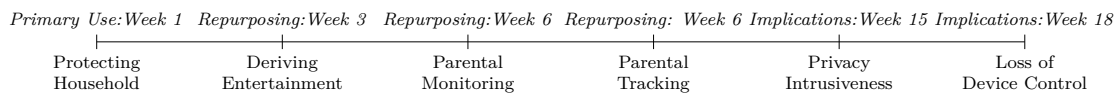
**Registration:** Registration refers to the process that creates a new user’s identity, that can be used to provide access to smart home products. Registration experiences consisted of creating accounts (i) directly by providing a valid email address and creating a password or (ii) through linking social media accounts (e.g., Facebook, Twitter). Frustration with registration was experienced by some participants. In H1, Rosa H1a was annoyed with seemingly ‘*forced registration*’, where she had to register for an account before using devices. She explained: “*Oh my god, this is already boring me. You should be able just to try it without having to register for an account.*” In H3, Carrie H3a was confused when trying to register for an account for the Tado thermostat prompting her to email customer support to receive help.

**Authentication:** Authentication refers to the process that confirms a user’s identity and provides them access to smart home products. Authentication experiences



mostly consisted of using a combination of emails, usernames and passwords (n=11). Password fatigue was experienced by participants (n=4) who were required to remember an excessive number of passwords as part of their daily routine. In H1, Rosa H1a was frustrated after being unexpectedly prompted to create and remember multiple passwords. She said: “*What kind of world do we live in that it is so complicated that you need a username and a password for nearly everything you want to do?*” Similarly, in H6, Tobias H6a was frustrated with the high number of accounts the household was using. He explained: “*I would prefer not to have multiple accounts because I will just forget. [...] You are speaking to someone who forgot their Dropbox password last week.*”

**Authorization:** Authorization refers to the process that verifies a user’s privileges or permissions against specific actions in a smart home product. Authorization experiences consisted of exploring and using family sharing features across smart home products (n=8). For some participants, family sharing features (e.g., Amazon Household, Nest Family Accounts) were confusing, difficult to set up and did not work as expected. In H4, Carla H4a and Aaron H4b set up Amazon Household to share free shipping, purchases, and other benefits across their accounts. However, Carla H4a was not able to share audio-books. She said: “*We linked our Amazon accounts together, we got this family thing. It was too confusing [...] I cannot really listen to my audio books; which I would like to do.*” In H2, Monique H2a and Adam H2b needed to sync their Arlo Video Doorbell with their mobile phones; however, it was difficult to set up the feature. As a result, Adam H2b used his own account on both mobile phones instead of setting up permissions.



**Figure 4.8:** Timeline illustrating H1’s repurposed use of the Arlo Pro security camera over time.

**Security threats:** Security threats refer to potential violations of security vulnerabilities that result in unwanted impact, such as harm or theft of sensitive data. Participants (n=6) learned about security threats from external sources (e.g., forums, news). In H2, Adam H2b learned from a forum about potential security threats associated with Arlo security cameras. He also discovered ways that landlords had exploited smart controls associated with smart heating systems. In H6, Tobias H6a read online about news articles describing Ring security cameras as vulnerable and discussed his concerns: “*I don’t know if you saw on the news that these things were*

*all hackable?* In H2, Rosa H1a learned from mumsnet, a forum website, that cyber criminals could turn an Amazon Echo into an eavesdropping microphone.

**Security breaches:** Security breaches refer to incidents that result in unauthorized access to secure, private or confidential information to an untrusted environment. One participant experienced a security breach (n=1) while other households were concerned about security breaches (n=4). In H6, Tobias H6a was alerted that his password was compromised when setting up a smart home product. He said: “*It has a list of compromised companies or sites, and so it tells you: ‘Look, this company has had a data breach. You might want to change your password’.*” In H2, Adam H2b raised security breach concerns regarding the household’s Google Home Mini. He said: “*It was just the kind of general [fear] like oh, you know, if it will be hacked, there will be people looking to hack this straight away.*” Similarly, Aaron H4b in H4 said he is ‘*paranoid*’ in installing smart home products with cameras in bedrooms due to data breaches targeting security features cameras.

**4.2.3.3.2 Management of Security** We report password management (e.g., storage) and security update experiences.

**Password creation:** Participants were prompted to create passwords during the registration process (see Section 4.2.3.3.1). Participants (n=2) found some password policies to be complicated and confusing. In H3, Felicity H3c was confused with password instructions prompting her to create a “*strong*” password without offering password complexity guidance and recommendations. Felicity H3c said: “*I wonder what a strong password is. [...] How do you make a strong password?*” Further, in H4, Carla H4a was confused when prompted to create a new password when setting up an Amazon Echo device. She was unsure whether her existing password from her Amazon account would work.

**Password storage:** Participants (n=3) used password managers and physical notebooks to store a large number of distinct and complex passwords. Different password managers were incompatible among products and caused inconsistent password synchronization. For instance, in H6, smart home products produced by different manufacturers (Amazon and Apple) prompted Tobias T6a to use two password managers: 1Password and Apple’s Keychain Access. However, the password managers were incompatible causing frustration when Tobias T6a tried to authenticate to a Ring device. Tobias H6a explained: “*I think it [1Password] conflicts with the in-built password manager, so even though having a password manager, signing up to something like Philips, or whatever it may be [...], it is trumped by Apple’s own one. So you have to hit ‘No’, and then every time you*

use 1Password to auto-fill it asks whether you want to update the in-built one.” In H1, Rosa H1a and Jaco H1b stored their passwords on a physical notebook. Rosa H1a did not trust the security of password managers while Jaco H1b found the approach handy when passwords could not be remembered.

**Password reset:** Participants (n=2) used password recovery features that allowed them to reset their passwords via their email address and other related information. Some password reset interactions caused frustration due to unclear instructions. In H3, Felicity H3c was not able to reset her forgotten password for Tado thermostat’s application due to poor self-service password reset instructions. Felicity H3c explained: “*If I can remember my password. [...] And then you can set it like that and change it and I can not remember how to do that.*”

**Security update management:** Security updates refer to widely released fixes for product-specific, security-related vulnerabilities. Participants (n=2) had both positive and negative experiences managing smart home security updates. In H6, Tobias H6a was satisfied with automated security updates installed on his Ring doorbell. He said: “*They released this software and I thought, ‘Let’s just see if ours has updated automatically and it had so I was quite impressed with that.’*” In contrast, in H2, Adam H2b was frustrated with frequent security updates that required manual configuration and interrupted video playback on the Amazon Fire Stick. He explained: “*It took me maybe ten or so times to get the devices to connect, and there was lots of firmware updates.*”

#### 4.2.3.4 The Experience of Technology Repurposing

Technology repurposing refers to the use of technology for a purpose other than its original intended use. We report how smart products were repurposed for parenting and entertainment; and discuss security and privacy implications.

**4.2.3.4.1 Repurposing Uses** We report the repurposing uses for parenting and entertainment (see Figure 4.8 and Table 4.4).

**Parenting:** Some products brought for entertainment and home security were repurposed for parenting. Participants (n=6) used smart home products to monitor and track minors’ online and offline activities. In H1, Jaco H1b and Rosa H1a used the footage recorded by security cameras to monitor their children’s activities. Jaco H1b told Iria H1c that he is constantly worried about her safety. In H4, Carla H4a used smart lights to track her children. She wrote in her diary: “*[The lamp] seems to be up and working again. I’m definitely relying on it to track the kids.*”

In H4, Aaron H4b changed the wake word from ‘*Alexa*’ to ‘*Computer*’ to control Malte H4c’s use of the Echo device. In H3, Carrie H3a expressed concerns over Felicity H3c’s access to the Google Home after the device told her: ‘*Your friendship keeps me warm*’. Carrie found Google Home’s response to her daughter Felicity H3c inappropriate. As a result, she was concerned about her daughter’s safety.

**Entertainment:** Participants (n=4) used smart cameras to derive entertainment from recorded footage. In H4, households used smart cameras as a means of ‘*nature spotting*’. Aaron H4b pointed his Arlo Pro camera at a birdhouse to record baby birds (see Figure 4.5b). In H1, households regularly reviewed camera footage to watch and share memorable moments and family activities. Rosa H1a shared interesting moments with other household members while Jaco H1b monitored the footage for entertainment. He said: “*I was excited to see what’s going on and who’s going to come [...] And I was seeing some cars and catching some cars, and then I just started inside the house, and they [children] just leave home to go school. I really cheer for that. It’s really good stuff.*”

**Table 4.4:** Examples of repurposed uses and implications for each household

Household	Product	Planned Use	Repurposed Use	Security/Privacy Implications
H1	Smart Camera	Automation, Security	Entertainment, Parenting	Loss of Control, Intrusiveness
H2	Voice Assistant	Entertainment, Communication	Well-being, Education	No reported implications
H3	Voice Assistant	Entertainment, Education	Well-being, Control	No reported implications
H4	Voice Assistant	Automation, Control, Entertainment	Monitoring, Control, Parenting	Loss of Control, Frustration
H6	Smart Camera	Home Security, Interoperability	Streaming, Family Sharing	Loss of Control, Intrusiveness

**4.2.3.4.2 Security and Privacy Implications** We discuss the implications of repurposing: intrusiveness and loss of control.

**Intrusiveness:** Participants (n=3) experienced privacy concerns and intrusiveness in repurposed smart home devices. In H1, tension arose between Iria H1c and her mother Rosa H1a. Rosa H1a said the camera footage can be used to catch “*Iria coming [home] with someone*” while Iria H1c perceived the smart cameras as intrusive and invasive of her personal privacy. She said: “*Everyone in our year, in my year, literally knows where we live. And all the boys love to cycle past our house. And they will always knock and come and say, ‘Hello’ to me, so they are just worried.*” In H6, Tobias H6a turned smart cameras into a live streaming feed to observe the cat remotely while being away. However, his wife Sylvie H6b felt that her private life had been violated after Tobias H6a provided stream access to his mother. She explained: “*Tobias rigged up a camera so that we could observe what the kitten was doing when we were not in, and we could*

access it using a web link, and Tobias gave the link to his mum. So his family members, mum could then observe the cat plus us.”

**Loss of control:** Participants felt (n=3) loss of control over their personal data in repurposed smart home devices. In H1, Iria H1c was unable to remove video footage from smart cameras because her parents refused to provide password access to her. Jaco H1b worried that Iria H1c would delete footage and said: “*I do not want to give it to her, I want to keep it for me.*” In H4, Carla H4a and Aaron H4b received activity notifications over applications installed by Malte H4c on smart devices. Malte H4c knew his activity had been tracked and controlled. He was unable to take control and told his parents: “*You have been deleting all my games. [...] You have lied to me, you say that you have nothing to do with it.*”

#### 4.2.4 Discussion

We discuss the implications of our study in the security and privacy design of smart home products.

##### 4.2.4.1 Privacy Design

We discuss our results in relation to *intrusiveness and tracking* and the *perception of the effectiveness of privacy controls* in smart home products.

**4.2.4.1.1 Intrusiveness and tracking:** Our findings on user concerns with intrusiveness and tracking confirm previous research by Nguyen et al. [377] who found that smart home users feel *too watched* (for camera-enabled devices) or *too listened to* (for voice-enabled devices). While most of the experiences from our participants revolve around data directly collected by the devices, data inferred from those collected by the devices can be even more intrusive [378]. For instance, continuous recording and retention of data can be used to infer physical information about the user’s home (e.g., location data), and behavioral patterns in the home (e.g., when people wake up, take a shower, leave for work, return from work, go to bed, receive visitors, who the visitors were, and many more). Companies are not mandated to reveal what inferences they make from the data and for what purposes. Without such details, it is hard for users to know the kinds of inferences that will or can be made and to negotiate allowable use. Users are left to speculate about this (e.g., Carrie H3a speculated that Bluetooth can be used by manufacturers to locate her, hence she turned it off).

**4.2.4.1.2 Perception of effectiveness of privacy controls:** Our results suggest that it is the *perception of effectiveness of controls* that improves the experience of privacy and assurance. Smart home devices must be designed to give users control over the functional elements of a device, but also assurance that privacy features are effective in enabling the user to achieve their expectations. Not all privacy features provide the same effective assurance. In H4, Echo Show 5's physical camera shutter was perceived to be highly effective, and provided enough privacy assurance that it was kept in the bathroom. Malte H4c explained: "*People do actually hack on it [...] where in fact they can still take pictures but it will just be a black screen.*" In contrast, Iria H1c pressed the 'mute' button on an Amazon Echo, but was not reassured it was no longer listening despite the device showing a red indicator confirming that the microphone is muted. As a result, simple physical privacy protections may prove more convincing and provide a greater degree of assurance as their protective effect can be perceived directly. In contrast, settings, data use policies, warning lights, and other intangible controls may be perceived as less effective.

#### 4.2.4.2 Security Design

We discuss our results in relation to *password fatigue*, *authorization*, *interoperability* and *threat intelligence* in smart home products.

**4.2.4.2.1 Password fatigue:** Our results confirm the continued existence of a well-known problem: password fatigue (e.g., Rosa H1a writing her passwords on a notebook). This results in poorly chosen and excessive reuse of passwords, thereby weakening the security of the protected services [379]. Given the current proliferation of smart home devices (e.g., each requiring a username and password), there are higher chances that passwords will be reused on devices and services on the home network; hence compromising one account exposes other accounts. Password fatigue may also encourage users to use insecure passwords that can be cracked.

**4.2.4.2.2 Authorization:** We also show that authorization mechanisms (e.g., family sharing features) were not user-friendly and often not used. Some households (e.g., H3) were not aware of multi-user features (e.g., family sharing); while other households (e.g., H1) tried them but found them unsuitable. In H1, Rosa H1a and Iria H1c found that using two Amazon accounts on an Echo was inconvenient (e.g., Amazon Music did not work and required another subscription). Households that used multi-user features found difficulties in configuring them (e.g., H2 and

H4 struggled to set up sharing on Amazon Household and Arlo Video Doorbell). Prior work has also shown that sharing smart home products with others can be troublesome [380]. A team from CNET Smart Home that performed extensive testing on smart home devices described the process of setting up multiple devices and users as ‘*anything but simple*’ and ‘*smart home from hell*’ [381].

More work needs to be done to streamline the setup and management processes of authorization methods to fit the context, communal implications, and competence levels available in the home. One specific area of concern is that product manufacturers (e.g., Apple, Amazon, Google) have different rules and procedures for multi-user features which can cause confusion. For instance, Apple’s HomeKit does not permit owners to selectively share devices with family members whereas Amazon Household does [382].

**4.2.4.2.3 Interoperability:** Authentication and authorization challenges in smart homes emphasize the need for coordination, consistency, and interoperability across heterogeneous smart home systems. Manufacturers need to work to align the security features across ecosystems (e.g., consistent terminology, APIs, access and identity management) in order to provide a more harmonious user experience of security in smart products. This is particularly important given that – unlike in professional settings – the home user population does not typically rely on qualified professional staff and supporting technology to procure, configure, maintain, and deal with problems or incidents in smart products. As a result, the experience of security is critically dependent on the quality of UX design in smart products across the whole ecosystem.

**4.2.4.2.4 Threat intelligence:** Another option is for designers to research threat intelligence and understand how adversaries are misusing smart products to design and provide educational material at relevant times (such as during configuration choices, or provided in response to attempted misuse or breaches). For instance, when smart camera footage is being reviewed, a notification could be sent to all enrolled devices and accompanied by a visible light on the cameras as a means of notifying users that someone is accessing the footage. Designers can then provide additional information through the notifications detailing how such footage can be misused by attackers – both foreign and domestic.

A summary of the major contributions of this study and how they relate to existing work can be found in Appendix B.2.4 in Table B.1.

## 4.3 Discussion

### 4.3.1 Consent Needs are Dynamic

Both studies highlighted the importance of improving the design of consent management. They revealed that the life cycle of consent can change over time (see Figure 4.7): users can withhold - grant - revoke - amend consent as they see fit at different times of product use and for different reasons and purposes.

In the first study, P8 who had difficulties checking their Google Home audio log was able to review his logs eventually and discovered that multiple non-intended conversations were recorded. After this experience, P8 changed their privacy settings to prevent storing of audio logs. In the second study, Carrie H3a revisited her privacy settings and activated ‘*Web & Activity*’ tracking to be able to stream music. Carrie H3a also temporarily enabled *location services* to set up her Google Home. Over time, Carrie H3a learned to automatically consent to tracking when setting up Google Home devices.

A key difference between the studies is that study 2 revealed that withholding consent can be an unpleasant experience, particularly in cases where users are given options to either grant consent wholesale or be denied services; or be allowed to withhold consent, but have broken features in a device/service.

### 4.3.2 Trigger Points Raise Security and Privacy Concerns

Both studies revealed that security and privacy concerns often result from media and online sources (e.g., reading an article about security breaches) and/or device use and features (e.g., experiencing a negative interaction with the device).

In the first study, P9 expressed privacy concerns after finding a news article alleging that Alexa would recognize if they were ill. Furthermore, P10 discovered that their son had made multiple orders from Amazon by tweaking the device settings which developed security concerns. In the second study, Aaron H4b was concerned that the Echo Show 5 was displaying targeted and personalized advertisements after finding news and advertisements that could not be hidden. Furthermore, in H6, Tobias H6a developed new concerns after he was alerted that his password was compromised when setting up a smart home product.

A key difference between the studies is that study 2 revealed that both privacy and security concerns arose from mass media and online sources (e.g., hearing about breaches); however, privacy concerns also arose from device use and features (e.g., using devices led to new privacy concerns but not to security concerns).



### 4.3.3 Users Prefer Physical Privacy Controls

Both studies revealed that physical privacy protections proved to be more convincing and provided a greater degree of assurance as their protective effect was perceived directly by the participants. In contrast, settings, data use policies, warning lights, and other intangible controls may be perceived as less effective.

In the first study, P13 said they disconnected their smart speaker whenever they had a client visiting, which provided more assurance to both P13 and their guest that the device was not listening. In the second study, H4's Echo Show 5's physical camera shutter was perceived to be highly effective, and provided enough privacy assurance that it was kept in the bathroom. In contrast, Iria H1c pressed the 'mute' button on an Amazon Echo, but was not reassured it was no longer listening despite the device showing a red indicator confirming that the microphone is muted.

A key difference between the studies is that study 2 provided contextual details to users preference of physical privacy controls. Study 2 encompassed a variety of smart home devices (e.g., cameras) which elaborated the findings from study 1.

## 4.4 Conclusion

In this chapter, we explored the effect of the UX on the security and privacy of smart home users. To achieve our research goal, we conducted two studies. First, we conducted an interview-based study which resulted in a qualitative investigation of user perceptions and a conceptual model of UX links to risk and balancing behavior. Second, we conducted a secondary analysis of a six-month-long ethnomethodologically informed smart home study which resulted in a qualitative investigation of user behavior and a longitudinal view of security and privacy experiences.

*“Most business models have focused on self interest instead of user experience. Those are the kinds of problems we solve.”*

— Tim Cook

# 5

## User Experience Design in Smart Homes

The purpose of this chapter is to explore the role of UX in the design of security, privacy and data protection in smart homes. Therefore, this chapter tackles our second research question: *RQ2: What is the role of UX in the design of security, privacy and data protection in smart home products?*

To address our research question, we conducted a qualitative interview-based study with 20 smart home UX designers and their collaborators (see Section 5.1) where we investigated the following research question: *How do designers and their collaborators factor UX into the design of security, privacy and data protection in the smart home products?* Our semi-structured interviews resulted in a (i) **qualitative investigation** of UX design processes and (ii) a **theory** of UX factors in the role of innovation in the design of security and privacy in smart home products. Our study revealed three core challenges in smart home products: innovation, data protection and communication. To dig deeper into data protection challenges, we asked the following question: *How can we understand and support the UX of data protection in smart homes from the perspective of users, designers, and business leaders?* To address this, we conducted a qualitative interview-based study (see Section 5.2) where we investigated smart home data protection experiences and practices from the perspectives of users (n=7), designers (n=6), and business leaders (n=6). Our study resulted in a **qualitative investigation** of data protection experiences. We discuss the implications of this chapter in Section 5.3.

## 5.1 User Experience of Security and Privacy

### 5.1.1 Motivation

Prior research has uncovered a variety of design-related security and privacy issues from the user perspective for which UX is critical (e.g., the need to consider aesthetic aspects of security and privacy). Researchers have argued for understanding and designing the UX of security and privacy [13]. However, the literature reveals that there has been limited work on frameworks, models, and scientific research bridging UX, security, and privacy. Our work takes a step to solve this problem by investigating the role of UX in the security and privacy design of smart home cameras. To address our main research question, we explore the following sub-questions:

1. How do designers and their collaborators make decisions during the security and privacy design process of smart home cameras?
2. What are the different aspects of the design process of smart home cameras that explicitly deal with UX factors?
3. What are the challenges that different stakeholders face when factoring UX into the security and privacy design of smart home cameras?

### 5.1.2 Methods

We designed and conducted a qualitative user study of designers of smart home cameras based on approaches described in [289, 349, 350]. We interviewed 20 participants in the United Kingdom, focusing on understanding the design processes and practices of smart home cameras manufactured by three different companies A (n=6), B (n=8), and C (n=6). We aimed to investigate the design, development, and implementation of three security camera products that had been in production for years. We concentrated on the design of these products because smart home security cameras (i) have a growing adoption rate [383], (ii) are subject to increased security attacks [384], and (iii) are seen as particularly invasive by end-users [385, 386].

#### 5.1.2.1 Recruitment

To recruit our participants, we posted flyers and distributed leaflets in the United Kingdom, and advertised the study on online platforms (e.g., LinkedIn). We also recruited participants through snowball sampling, which allowed us to reach employees that were not easily accessible through other strategies. At the time of recruitment, interested participants were employees who were active at their company and responsible for the design, development, or maintenance of a smart

home camera product. The participants we recruited from each company were all on the same development team and worked on the same product.

We asked interested participants to complete an online screening questionnaire (see Appendix C.1.1). We received 31 complete responses. In addition to asking demographic questions, we provided participants with a list of job titles and then asked them to choose the title that best described their position at the company (e.g., UX Designer, Security Engineer, Product Manager). We describe the demographics of our participants in Table 5.1 in Section 5.1.3.

Additionally, we asked participants to provide information about their company. We also asked them to specify the type of products that their company manufactured (e.g., security, lighting, or phone systems), as well as the specific products their company manufactured (e.g., cameras, hubs, voice assistants, lights). Finally, we asked participants to estimate the number of employees who worked at their company. The number allowed us to establish the company size (e.g., startup, mid-size, enterprise) since we were interested in targeting large-scale product development companies that were more likely to put effort into improving the UX of products [387].

### **5.1.2.2 Interview Procedure**

We conducted semi-structured interviews with 20 employees working at companies that manufactured smart home devices: Company A (n=6), Company B (n=8), and Company C (n=6). We used the funnel technique [351] to structure our initial interview questionnaire (study script), starting with general questions and then drilling down to specific ones.

The interview started with general questions characterizing participants' role in the company (e.g., responsibilities, duration of employment), the type of products they designed or developed, and their perspectives on UX, security, and privacy. Members of design teams referred to different groups of people (e.g., device purchaser, device administrator, and device user in the house) as 'users' without distinction. We then asked questions related to requirements gathering and specification in the design phase, as well as questions about how UX was factored into the design process (e.g., UX in the security and privacy design process, UX design methods, techniques, and artifacts).

Finally, we asked specific questions related to the profession of participants. Regulatory stakeholders were asked about: data protection regulations, product liabilities, and regulatory affairs. Moreover, management stakeholders were asked about: roles and responsibilities, regulatory restrictions, security and privacy roles,

and data protection for multi-user products. Finally, security stakeholders were asked about: security requirements, the design of security, communication with other teams, responsibility for security, security maintenance, security updates and security breaches.

We conducted our interviews remotely using Skype and Zoom. We also audio-recorded and transcribed all interviews. Interviews lasted for an average of 52 minutes. Our interview questions can be found in Appendix C.1.3.

### 5.1.2.3 Pilot Study

After creating our initial interview questions (see Appendix C.1.2), we conducted a pilot study with four smart home product designers at a local conference. Two researchers recorded and analyzed the pilot interviews. We used the findings to identify potential problems (e.g., adverse events, time, cost) in advance prior to conducting the full-scale study. Drawing from our findings, we made the following changes:

- We refined our interview questions to reduce bias and improve their quality.
- We changed our data analysis method from Thematic Analysis to Grounded Theory because we aimed to (i) develop a substantive theory, (ii) deeply explore design processes, and (iii) derive grounded recommendations.
- We were better informed of the average duration of our interviews, which turned out to be around 50 minutes.

### 5.1.2.4 Data Analysis

We transcribed and analyzed all 20 semi-structured interviews using Grounded Theory as described in Section 3.2.2.1. At the end of our coding process, we generated a codebook of 155 codes. We observed data saturation [388–390] between the 18<sup>th</sup> and the 20<sup>th</sup> interview; i.e., no new codes emerged in interviews 18–20, and, hence, we stopped interviewing. After creating the final codebook (see Table C.2 in Appendix C.1.4), we tested for inter-rater reliability. The average Cohen’s kappa coefficient ( $\kappa$ ) for all codes in our data was 0.81. Cohen’s kappa values over 0.80 indicate almost perfect agreement [370].

### 5.1.2.5 Limitations

Security, privacy, and regulatory matters are sensitive issues in big organizations like the ones we interviewed (see Table 5.2). Our participants’ corporate responsibilities as well as their company’s reputation might have biased their responses. To mitigate

this, we explained to our participants that data would be collected and processed in accordance with the General Data Protection Regulation (GDPR).

Further, self-reporting bias is common in user studies [391]. Some participants might not have responded accurately to our questions because they did not remember specific details or wanted to be viewed as socially acceptable. To maximize validity and minimize self-reporting bias, we avoided leading questions and relied on open-ended questions, inviting participants to provide in-depth answers in their own words. Moreover, our data consists of only what participants said rather than an observation of design processes. This makes it hard to distinguish between the perceptions of participants and the reality of the actual development processes. Future work should aim to study smart home development processes through a wider variety of data collection methods.

Finally, our qualitative work is limited by the size and diversity of our sample. Following recommendations from prior work to interview between 12 and 20 participants [392], we interviewed 20 participants until new codes stopped emerging. We also recruited a demographically-diverse sample of participants in order to increase the likelihood that relevant findings have been mentioned by at least one participant.

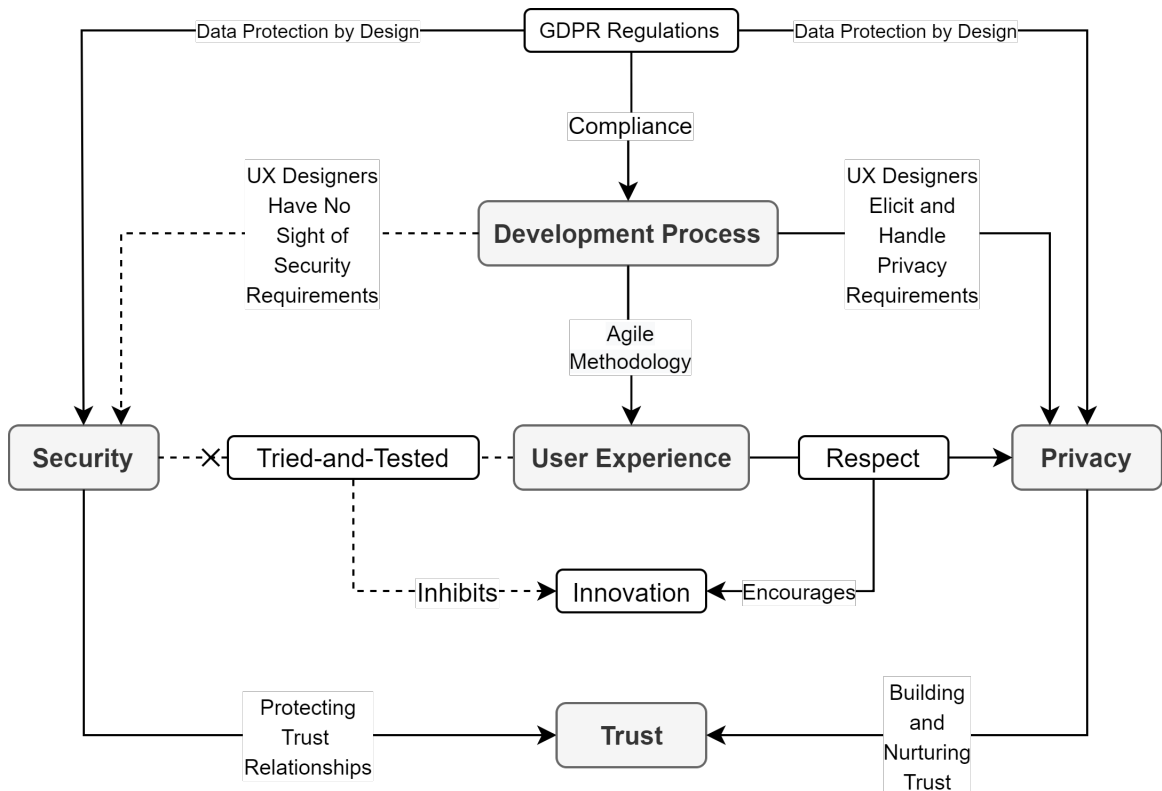
### 5.1.3 Results

In this section, we detail the findings of our study. We present our participant demographics (see Section 5.1.3.1), and then discuss our key findings organized according to the main themes of our analysis, as illustrated in Figure 5.1. The main themes are:

- Development Process (Section 5.1.3.2);
- UX in Security Design (Section 5.1.3.3);
- UX in Privacy Design (Section 5.1.3.4);
- Innovation in Security and Privacy Design (Section 5.1.3.5);
- Trust (Section 5.1.3.6).

#### 5.1.3.1 Participant Demographics

Table 5.1 summarizes the demographics of our sample (n=20). We interviewed 12 male and eight female participants. Ages ranged from 25 to 52. Ten participants had a college (or an undergraduate) degree, and ten had a graduate (or postgraduate) degree. We divided our participants (n=20) into six groups of stakeholders based on employment: security stakeholders (n=4), regulatory stakeholders (n=3), UX stakeholders (n=5), management stakeholders (n=4), software stakeholders (n=2), and hardware stakeholders (n=2).



**Figure 5.1:** Drawing from the findings of our study, the figure describes a model showing how UX was factored into the security and privacy design of smart home cameras.

### 5.1.3.2 Development Process

All participants (designers and their collaborators) followed an agile product development process, which included requirements analysis, design, development, testing, and maintenance [393]. In this section, we report on the requirements analysis, design, and development stages that companies A, B, and C (see Table 5.2) followed to develop products PA, PB, and PC (see Table 5.3). We describe how GDPR influenced the development process of smart home cameras. We also describe the challenges that UX design activities and smart homes introduced to our participants.

**5.1.3.2.1 Processes and Approaches** We briefly describe the processes and approaches of the design teams working at companies A, B, and C. All teams combined hardware and software development in agile and iterative design processes. **Company A.** A cross-functional team that involved various stakeholders (e.g., senior UX/UI designers, software and mobile application developers, industrial designers, product managers) was in charge of questioning, exploring, defining, and making decisions related to the design of product PA (a camera). The team ran

	Gender	Age	Degree	Experience	Employment
<b>A01</b>	Female	46	M.A.	4 years	Product Manager
<b>A02</b>	Male	28	B.A.	2 years	UX Designer
<b>A03</b>	Female	42	M.Sc.	5 years	Security Manager
<b>A04</b>	Male	30	M.Eng.	2 years	Security Engineer
<b>A05</b>	Male	32	M.Sc.	2 years	Hardware Designer
<b>A06</b>	Male	44	M.A.	6 years	UX Director
<b>B07</b>	Female	52	J.D.	7 years	Legal Counsel
<b>B08</b>	Female	31	J.D.	2 years	Compliance Counsel
<b>B09</b>	Female	38	B.A.	4 years	Experience Designer
<b>B10</b>	Male	43	B.A.	7 years	Product Designer
<b>B11</b>	Male	27	B.A.	2 years	UX Designer
<b>B12</b>	Male	35	M.Sc.	4 years	Security Architect
<b>B13</b>	Male	28	M.Sc.	3 years	Mobile Developer
<b>B14</b>	Female	31	B.Sc.	4 years	Software Engineer
<b>C15</b>	Female	46	J.D.	6 years	Product Counsel
<b>C16</b>	Male	36	B.A.	6 years	Senior UX Designer
<b>C17</b>	Male	29	B.Eng.	2 years	Hardware Engineer
<b>C18</b>	Male	50	B.Bus.	8 years	Product Manager
<b>C19</b>	Female	34	B.Sc.	4 years	Security Engineer
<b>C20</b>	Male	25	B.Sc.	1 year	Software Developer

**Table 5.1:** Semi-structured interview participant demographics.

Company	HQ	Employees	Product	Designed in
<b>A</b>	UK	500+	PA	UK
<b>B</b>	USA	1000+	PB	UK
<b>C</b>	USA	1000+	PC	UK

**Table 5.2:** Summary of companies.

Product	Type	Major Functionality
<b>PA</b>	Camera	Motion and sound detection with alerts.
<b>PB</b>	Doorbell	Real-time monitoring/audio features.
<b>PC</b>	Camera	Face recognition/detection of intruders.

**Table 5.3:** Summary of products.

multiple workshops with designers and developers to explore various ideas and techniques, to become familiar with common design patterns, and to understand the product's business strategy. They followed a collaborative UX design process (multi-staged UX [394]).

**Company B.** A self-managing agile team was in charge of the design and development of product PB (a doorbell). The team was composed of different experts



(e.g., designers, developers, engineers) who met on a regular basis to share data, communicate, collaborate, and discuss their progress. No managers were controlling or directing the team because team members decided how to prioritize their work, manage their team, and achieve the goals of the project. UX designers were in charge of eliciting functional and quality requirements by applying different UX activities related to the use cases of the product. The requirements were extracted from user needs identified by UX research (e.g., personas, prototypes, interviews).

**Company C.** A functional team—operating in a traditional organizational structure—adopted agile mindsets, principles, and practices and was in charge of the development lifecycle of product PC (a camera). The team consisted of senior UX designers, product managers, and software developers. The team leader reshuffled team members regularly depending on the project’s needs and requirements. Team members met regularly and were familiar with each other’s work processes. UX designers, developers, and content designers conducted user research and made explicit UX decisions during the early stages of their projects. The team elicited requirements during the design, development, and implementation phases.

**5.1.3.2.2 GDPR and Compliance** All three companies were required to comply with GDPR [395], which mandated *Data Protection by Design* (DPbD) [108] practices (as reported by A3, B7, and C15). In practice, a DPbD approach requires companies to “*consider privacy and data protection issues at the design phase of any system, service, or product.*” [109]

**Delayed effect.** GDPR came into force on May 25<sup>th</sup>, 2018, after the smart cameras of companies A, B, and C had been developed and released. Product Counsel C15 said that the devices produced before the enforcement date were non-compliant with GDPR. Similarly, Legal Counsel B7 said that the company’s infrastructure that stored user data was not equipped to deal with GDPR requests. Security Architect B12 stated that making changes in the existing product architecture required an increased demand for labor, money, and effort.

**Obtaining consent.** GDPR requires smart home companies to obtain clear and valid consent from users to the use of their data. Due to the large amount of data exchanged in the ecosystem of company C’s products, consenting to *all* uses of data was described as technically challenging by Product Manager C18. UX Designer A2, who was familiar with GDPR, stated that asking users to consent to all uses of data in their ecosystem would be detrimental to UX. A2 said: “*I think it would be too overwhelming for users to see every single piece of data that we collect.*”

**Right to withdraw consent.** Under GDPR rules, smart home users have the right to withdraw their consent at any time, which requires companies to delete user data. However, in the case of company C, Security Engineer C19 reported that their smart camera was often used with other company products as well as by third-party products (e.g., Amazon Alexa). C19 explained that the increased number of devices that shared customer data has made complying with this regulation demanding. C19 described that their infrastructure “*is not designed to destroy the data just like this, with one click.*” C19 also mentioned that lack of control of data collected by third-party devices has made complying with this regulation “*very challenging.*” In particular, C19 stated that it was difficult to determine whether third-party devices; e.g., Amazon Echo, were GDPR-compliant due to the lack of clear guidelines showing how third-parties collected and processed user data.

**Conflict between business and regulation.** Different and conflicting design goals could arise during the design phase. Security Manager A3 reported dealing with a tension between commercial and regulatory stakeholders. The *Legal Department* wanted some of the data collected from users to remain stored on users’ cameras (i.e., offline); however, the *Commercial Department* requested all data collected to be stored on the company’s cloud servers. A3 explained: “*The legal team asked to keep the data local only, but at the same time the commercial team wanted us to collect it. I guess they wanted to monetize it.*” This reported conflict highlights the important role of regulation in smart homes.

**5.1.3.2.3 UX Design Activities** Participants reported different challenges during different activities of the UX design process.

**Identifying pain points.** UX designers (n=2) investigated data monitoring and collection in smart home cameras (through conducting research) to appropriately “*identify the main sort of frustrations and pain points*” (A2). A2 interviewed smart camera users to research “*acceptable areas of monitoring*”; however, they could not identify the pain points resulting from monitoring. To address this problem, A2 interviewed psychologists and visited existing customers in their house. A2 was able to identify six major pain points related to video monitoring. For example, A2 found that customers were concerned about cameras spying on them—by passively collecting data without their knowledge.

**Making UX design decisions.** UX designers made recommendations, but did not always make design decisions. UX Designer B11 reported that despite conducting user research and suggesting UX-aware changes, they did not make any final decisions; they were instead made by the project manager. B11 said: “*Ultimately,*

*it's always their decision at the end of the day, but it has always been difficult for my job to ensure that I'm providing the best experience possible."*

**Fully understanding user behavior.** UX designers (n=3) mentioned that one persistent UX challenge they faced was to fully understand the security behavior of users. A6 commented: "*The reality is we won't know the exact behavior until the product is out.*" The difficulty of understanding real user behavior is a challenge that is well-known to the usable security and privacy community [396].

**Making hardware design changes.** Hardware stakeholders (n=2) faced issues when applying UX-related changes to existing products. In company A, industrial designers faced difficulties when implementing a privacy feature which would visualize the on/off state of smart cameras. Hardware Designer A5 explained that software developers were more flexible: "*while mobile developers are flexible, we have to make early decisions that are not easy to change.*" Similarly, Hardware Engineer C17 said there was not enough time to build hardware sprints. The lack of flexibility (e.g., time, effort) made it difficult to apply UX changes to existing products.

**5.1.3.2.4 Interoperability of Smart Home Devices** Participants reported two smart home interoperability challenges that occurred during design and development.

**Heterogeneous devices.** Participants (n=2) stated that the integration between heterogeneous devices and company products was important to companies. For example, most products in company A supported heterogeneous devices and services, such as Amazon Alexa, If This Then That (IFTTT) applications, and Apple's Siri (A1). Third-party services (e.g., Amazon Alexa) "*improve[d] [user] experience*" (A2); however, they created difficulties for security stakeholders. Security Engineer A4—who worked on encrypting the data exchanged between the company's ecosystem of products and Amazon Alexa—described the process as "*complex*" and "*time-consuming.*" A4 specifically reported dealing with a legacy platform unable to send and receive encrypted messages with the API of Alexa Voice Service [397].

**Securing connections between devices.** Security Engineer C19 stressed that their company's smart home devices had "*solid security.*" The challenge, however, was encrypting data exchanged among the increased number of devices in the company's ecosystem. C19 explained: "*Smart home devices are generally secure... The problem is the number of connections between all of those devices, they all have to be protected.*" In addition, Product Designer B10 explained that the increased connections between devices, touch points, and objects would add to the complexity of this challenge. Complexity in smart homes was previously reported in the literature [398].

### 5.1.3.3 UX in Security Design

In this section, we present how design teams applied UX principles and practices to the design of security features that end-users interacted with. We found that UX was not factored into the design of security solutions due to lack of expertise and the misperception of security being a low-priority technical-only problem. In addition, we found that GDPR and security audits motivated UX considerations.

**5.1.3.3.1 Alignments between UX and Security Design** We describe alignments between UX and security design below:

**Regulations and legal liabilities.** We found that regulation triggered security design considerations. Although security was not explicitly factored into company B's design phase, regulations and legal liabilities required designers to consider some security requirements. UX designers in company B attempted to consider regulatory requirements in the design phase although they faced several obstacles (i.e., high-level guidelines). Legal Counsel B7 mentioned that the introduction of GDPR's "*Data Protection by Design*" requirements prompted doorbell design teams to implement new security features (i.e., stronger encryption during authentication). **Security audits looking into user behavior.** All three companies conducted security audits to establish how well their information system conformed to security standards and frameworks. We found that security audits in companies B and C prompted security design considerations. During a security audit led by Security Architect B12, a security review was conducted to investigate the password strength of the accounts of PB's users. B12 found several instances of poor password behavior, which prompted an evaluation of password strength as well as the creation of UX-aware password requirements (e.g., the addition of password strength meters).

**5.1.3.3.2 Incompatibilities between UX & Security Design** We describe incompatibilities between UX and security design below:

**Design of security features was not explicitly anyone's responsibility.** Among our participants (n=20), no one took responsibility for the design of security features. Participants (n=5) who handled security design tasks said they were not accountable for security design issues. Those participants did not have UX design expertise. For instance, Product Manager A1, who made security design decisions based on their understanding of common security practices, said that the *Information Security Team* was responsible for all matters related to security, including security design. However, Security Engineer A4 from the *Information Security Team* dismissed any responsibilities related to the design of security features.

**Security design was a low-priority concern.** For some stakeholders (n=2), security design was acknowledged but perceived as low-priority. As a result, minimal efforts were made to introduce security stakeholders in design teams that handled UX design. Security Manager A3 explained that the budget of the *Information Security Team* was limited, and that adding security experts to the design team was a “*luxury*” they could not afford. Moreover, Product Designer B10 expressed similar thoughts when discussing the addition of a ‘*usable security expert*’ to the design team.

**Security was seen only as a technical problem.** Many participants (n=15) described security as being only a technical problem that should be addressed from a technical perspective. As a result, participants expected that security to be exclusively handled by developers and security experts. This perception gave little to no consideration to social aspects of security. For instance, when we asked UX Designer B11 why security was not part of the design process, B11 stated that this was “*a development question.*” Security Engineer A4 had a similar response: “*Designers do not have any security expertise and it doesn’t make sense to expect them to handle security problems.*” This finding is not novel, but confirms the existence of a long-term challenge in HCI where security is treated as a technical problem [399], regardless of ongoing efforts to bridge the gap between social and technical aspects of security design [396].

**Security features were not designed by usable security or UX experts.** In company C, sensitive features related to the connectivity of security cameras, firmware upgrades, and registration were designed by Software Developer C20. Similarly, Product Manager A1 – in company A – did not “*see the value*” of including security experts in the design team, and chose security features – such as authentication – based on their understanding of common security practices.

**UX designers had no sight of security requirements.** Security requirements were not always present in the UX design phase. Experience Designer B9, who played a core part in the design of the doorbell (PB), said that the requirements he was provided with did not include data protection or security requirements. Similarly, UX Designer A2 explained that the security of registering and processing data was discussed during the design phase. However, there were no requirements related to security design: “*There wasn’t specific kind of UX work around data protection or user protection or something like that.*”

**Security design considerations were ad hoc.** For some participants (n=5), features handling sensitive information (e.g., authentication, software patches, access to video footage) created security design considerations on an ad hoc basis. For example, Mobile Developer B13 designed the software update development process

for the doorbell mobile application. B13 strongly valued the design of update features because they realized that these features could be used to deliver security updates. In all five cases, ad hoc design security considerations were triggered by non-experts of security design: management stakeholders (n=3) and development stakeholders (n=2). This finding confirms Assal and Chiasson's study results [257], which suggested that ad hoc security considerations are fragile because non-experts of security design (e.g., developers) could fail to identify security-sensitive features.

**Lack of security experts in design teams.** The product design teams of companies A, B, and C did not include security experts. In company A, the *Information Security Team* was not involved in the design phase of their smart camera. Justifying the decision, Security Manager A3 stated that all company employees underwent annual training and followed the company's "*information security management framework*."

**Security was only considered at the implementation stage.** For some security stakeholders, security design was acknowledged but was not seen as a priority. The *Security Team* in company B prioritized working with the *Development Team* over the *Design Team*. Security Architect B12 who worked with the doorbell *Development Team* said: "*I know that we can get involved with designers, but well, it's more efficient to work with the development team.*"

**Security was reactive and not proactive.** Security stakeholders (n=2) reported that security design was treated as reactive, rather than proactive, in companies A and B. Companies preferred a reactive approach, in which they made security design considerations or changes based on security incidents reported by customers. For example, Security Architect B12 reported that their security teams implemented multi-factor authentication as an option to secure user accounts after successful account hijacking attacks had been reported.

#### 5.1.3.4 UX in Privacy Design

In this section, we present how design teams applied UX principles and practices to the design of privacy features that end-users interacted with. We found that UX was factored into the design of privacy solutions in companies A and B through considerations of consent, transparency, and user control. However, in company C, UX was not considered in the design of privacy features due to lack of expertise and relying on a general understanding of privacy issues and product use.

**5.1.3.4.1 Alignments between UX and Privacy Design Giving users control.** Companies A and B gave customers more control of their privacy settings, which UX designers reported to increase trust. For example, both companies implemented a privacy mode in their mobile application in order to allow users to stop camera monitoring. In company A, designers also aimed to make users “*feel in control*” by adding (1) a visible on/off feature that showed the current state of cameras and (2) a privacy mode to give users “*peace of mind*” (A2)—allowing users to automatically or manually disable cameras when using their mobile application. In company B, UX Designer B11 explained that they added a private mode because their customers shared their cameras with family members: “*We do have a privacy feature in our product which allows you to switch the [...] whenever users want to have privacy. [...] When we interviewed users, we realized that a lot of them share their camera with others, mostly family members.*”

**Being transparent with users.** Participants (n=7) reported that their company made numerous efforts to be transparent with users. Legal Counsel B7 described that the *Legal Department* at company B worked with UX designers to create user-friendly FAQ pages that explained how their company collected and processed user data, as well as the measures they took to protect data. Further, B7 mentioned that the company constantly reminded users of their right to get their data deleted (by sending regular reminder emails). On the other hand, company A, which had to deal with multiple security vulnerabilities in the past, had recently updated its data breach incident response plan to inform customers of data breaches (A3). UX Director A6 helped the company use best practices to ensure that affected users had the best experience possible.

**Obtaining explicit consent from users.** UX designers (n=2) described different projects that looked into obtaining explicit consent from users in relation to data collection and sharing. UX Director A6 described an on-going project looking into obtaining consent through visual indicators instead of text-heavy documentation that would be difficult for users to read. UX Designer B11 worked on developing user-friendly consent notifications for the camera’s mobile application. In addition, developments were made to allow customers to change their own privacy settings based on their needs.

**Ensuring smart home cameras were not ‘creepy’ or intrusive.** UX designers (n=3) conducted user research with the aim to design smart home products that were not ‘creepy’ or ‘intrusive’. In company A, the goal of UX designers was to ensure users felt comfortable with their camera (PA), and that it did not make them feel it was a “*tool of surveillance*” (A6). To achieve their goal, UX Designer A2

interviewed psychologists and visited existing customers in their house to identify acceptable and non-intrusive “*areas of monitoring*.” In company B, Experience Designer B9 assisted in the design of a feature which allowed cameras to “*detect human activity based on geographic location*.” B9 explained that the feature allowed users to automatically disable their smart home camera when they were at home and, hence, the device did not feel “*creepy*.”

**5.1.3.4.2 Incompatibilities between UX and Privacy Design** We describe incompatibilities observed between UX and Privacy Design below:

**Designers of privacy features lacked expertise.** In company C, privacy features were designed by stakeholders (n=2) who did not possess design or privacy expertise (e.g., developers, product managers). Software Developer C20 designed the privacy mode settings of the camera’s mobile application during the development process. C20 made privacy design decisions based on their own understanding of sensitive data. Similarly, Product Manager C18 made privacy decisions related to a feature that allowed family members to disable video monitoring and notifications. Both stakeholders did not refer to any design or data protection guidelines. C18 said: “*We didn’t follow any requirements, no. [...] I don’t know why, I wasn’t aware of any requirements.*”

**Some privacy solutions were designed based on a general understanding of product use.** Company C’s *Product Design Team* appeared to deal with privacy design based on a general understanding of product use, rather than a thorough investigation of the specific context of use. For instance, Product Manager C18 believed that privacy concerns of users would rather be encountered by understanding users in a broad and wider context of user-centered design.

**Privacy was not explicitly discussed during user research.** The *Product Design Team* of company C did not explicitly discuss privacy during the design phase. Senior UX Designer C16 – who worked with product designers, engineers, and managers – said that privacy was not discussed during the user research phase when user interviews were conducted.

### 5.1.3.5 Innovation in Security and Privacy Design

We found that innovation cross-cut UX with security and privacy. In this section, we describe how innovation seemed to enhance the design of privacy solutions, but also to impede the design of security solutions.



**5.1.3.5.1 Enablers of Innovation in Privacy Design** We describe enablers of innovation in privacy design below:

**New privacy features were supported by qualitative and quantitative UX research.** UX stakeholders (n=4) working at companies A and B adopted a mixed qualitative-quantitative approach to build new features that addressed user privacy (e.g., concerns, pain points, expectations) during the design phase. To design features related to camera monitoring, UX Designer A2 conducted qualitative interviews with users as well as observed users in their homes to address any privacy concerns. UX Director A6 conducted quantitative research by collecting and analyzing survey data to design a visible indicator that showed whether a camera was turned on or off. A6 also used existing quantitative data from Google Analytics to prioritize which privacy features to implement. Experience Designer B9 created detailed storyboards and personas to visualize how their doorbell would be used in users' homes and whether it would be intrusive.

**New privacy features were evaluated through usability testing.** UX stakeholders (n=2) conducted usability testing of new privacy features introduced by company B. This was used to ensure that new privacy features did not negatively affect customer experience. UX Designer B11 delivered usability testing results to the *Product Design Team* based on the analysis of mobile application prototypes. B11 mentioned that among these prototypes, some requirements were related to privacy features. B11 explained that users were observed interacting with and changing privacy settings. Similarly, Experience Designer B9 conducted usability testing of the doorbell privacy features and was able to identify issues that prompted design considerations.

**5.1.3.5.2 Barriers to Innovation in Security Design** We describe barriers to innovation in security design below:

**Security solutions were tried-and-tested.** Security experts (n=3) mentioned that their companies' *Information Security Team* did not design their own security solutions. Instead, they used existing security solutions in their company's security protection paradigms, a practice known as *tried-and-tested* security. Additionally, non-experts also made security design choices supported by their own understanding of common security solutions. Product Manager A1, who worked with the *Design Team* that did not include security experts, chose the "username and password" authentication mechanism since it was familiar, widely-used, and accepted in industry. **New security solutions increased uncertainty.** Participants (n=2) explained that incorporating tried-and-tested security solutions avoided uncertainties that

arose out of the introduction of new security features. Product Manager C18 mentioned that new security solutions were likely to create usability concerns due to lacking information on how users would interact with such features. Similarly, Security Engineer C19 mentioned that attempts to introduce new security features were discouraged in the *Security Team*. C19 explained that introducing new security features would increase security risks due to lacking the knowledge required to design these features.

### 5.1.3.6 Trust

We found that trust heavily influenced UX design choices: product teams aimed to build customer trust through better privacy experiences, and also aimed to protect trust relationships with their customers through data protection policies.

**Building and nurturing trust through privacy experiences.** We found concerted efforts in the companies that aimed to build a culture of fostering trust. In company C, Product Counsel C15 explained that employees were encouraged to take an interest in and care about protecting user privacy. Similarly, in company B, Legal Counsel B7 described efforts put into creating a customer-first culture, where user privacy was not only seen in development processes but also discussed and encouraged culturally among product teams.

**Protecting trust relationships through data protection policies.** Product teams (n=5) used data protection policies to protect their company's reputation and build user trust. Many companies had established policies to deal with security vulnerabilities and attacks. For example, Security Manager A3 reported that his company adopted an incident response plan in case of a breach, in order to maintain its reputation, which we identified as a powerful motivator for companies to take security measures. Similarly, Security Architect B12 reported that their *Security Team* had invested in "*developing well-founded requirements*" for responding to security incidents, even when incidents resulted from users' incompetence (e.g., falling for a phishing attack, a compromised home router). Security Engineer C19 said their company drafted a "*responsible disclosure policy*" which dealt with managing security vulnerabilities reported by users.

Overall, our interview participants identified that customer trust was strongly linked to data protection: security was needed to mitigate loss of trust arising from exploiting security vulnerabilities. Further, user privacy was used by product teams to build and nurture trust relationships.

### 5.1.3.7 Summary

All product teams used an agile methodology to drive the development of their smart home products. We found that the practice of using tried-and-tested security solutions inhibited innovation in security design. In addition, the perception of security being only a technical problem, for which there were ‘best-practice’ technical solutions, limited the consideration of social and interactive aspects of security. In particular, it created a gap between UX considerations and security design (e.g., UX designers had no sight of security requirements).

Despite the gaps that we found in security design, our results show companies innovated in the privacy design space (e.g., company B created a novel geographic-based privacy feature). Our data shows that UX stakeholders in design teams elicited and handled privacy requirements. The practice of using UX design principles to respect user privacy (e.g., giving users control, avoiding creepiness and intrusiveness) seemed to encourage innovation in the privacy space. Moreover, we found that companies were motivated to preserve a trust relationship and build trust with their customers, as privacy or security failures (e.g., intrusive or vulnerable products) would undermine that relationship. Finally, regulations (e.g., GDPR) legally required design teams to consider data protection by design in their requirements.

### 5.1.4 Discussion

Our results uncover complex challenges and limitations that product designers faced: challenges arising from complying with GDPR; the importance and role of building trust; barriers to factoring UX into security design solutions. In this section, we use our findings to discuss the wider role of innovation in designing security and privacy solutions, as well as the implications of adopting a user-centered agile approach to data protection. We also highlight areas for future work.

#### 5.1.4.1 Need for Fostering Innovation

The current efforts of innovation in privacy design are a good first step, but more is needed. For example, the challenge of communicating and obtaining user consent in smart homes needs to be systematic (e.g., within the same device ecosystem) and coordinated (e.g., among device ecosystems). However, this is currently not the case and highlights the need for better communication and coordination between stakeholders and product teams.

While data protection regulations (e.g., GDPR) appear to be consistent with better UX design for privacy in smart homes, these regulations remain unclear

as to whether the same could be true with regards to UX for security design. Security and privacy qualities of smart homes are not the same; however, both are qualities of data protection. It is not clear how much responsibility users should have to ensure the secure operation of their devices. However, some manufacturers blame breaches on users who do not adopt secure practices (e.g., failing to change default passwords). Regardless of where responsibility lies, manufacturers could put effort into improving security experience, making it easier for users to achieve their desired security outcomes. One option would be for data protection legislation to explicitly cover security experiences, as currently there are very few incentives for manufacturers to put additional effort into enhancing the UX of security.

Regardless of whether regulations should encompass UX aspects of both security and privacy, design standards, guidelines, frameworks, and APIs are other options which have not been explored from an innovation perspective. The tensions that exist between regulators and UX designers over communicating the use of data (e.g., despite being required by GDPR, UX designers do not typically ask users to consent to all uses of their data because—otherwise—it would be detrimental to UX) should invite us to find innovative solutions that satisfy both parties: regulators and users.

#### 5.1.4.2 Security Design in Agile Development

Agile teams have historically treated security as a technical problem, ignoring its social and interaction aspects [400]. With that in mind, we argue that in an agile setting, security would still not be considered during the design stage and would, hence, remain an implementation problem. In company A, Security Manager A3 described their *Information Security Team* as “*the department of ‘no’ when it comes to enforcing security.*” This problem has been common in the past where security teams blocked progress in agile environments with the attitude of “security says no” [401].

Moreover, agile development does not have built-in steps for explicitly dealing with security issues because it was not designed with security in mind [402]. This might explain our results which show that product design teams who used an agile development process did not explicitly consider security issues during the design phase. However, our results show that GDPR required design teams to follow DPbD requirements, in order to build legally-compliant products. We argue that this is a promising step toward better considerations of security design in agile teams, but this is accompanied with noteworthy challenges and barriers, especially in the context of smart home ecosystems.

## 5.2 User Experience of Data Protection

### 5.2.1 Motivation

Data protection user experiences (e.g., consent interactions) have been widely studied in the literature. However, the user experience of data protection is a designed encounter, the modalities of which arise out of a process that encompasses contextual, economic, compliance and strategic business priorities. As a result, our research aims to expand the consideration of data protection user experience to encompass the perspectives of designers and business leaders to gain a wider understanding of the complexities and nuances. To understand and address the challenges of data protection compliance, our research qualitatively investigates smart home experiences by bridging the perspectives of smart home users (n=7), designers (n=6) and manufacturers (n=6).

### 5.2.2 Methods

We designed and conducted a qualitative user study of smart home users, designers and business leaders following similar approaches used in previous qualitative studies [289, 349, 350]. We interviewed 20 participants in the United Kingdom, focusing on understanding smart home data protection experiences and practices from the perspectives of users (n=7), designers (n=6), and business leaders (n=6). We concentrated on smart home products because they (i) have a growing adoption rate [383] and (ii) are seen as particularly invasive by end-users [385, 386].

A trained researcher conducted qualitative semi-structured interviews in the UK in English between October 2020 and June 2021.

#### 5.2.2.1 Recruitment

**5.2.2.1.1 Recruitment of Users** To recruit our user participants, we posted flyers and distributed leaflets in the UK, and advertised the study on online platforms (e.g., Twitter, LinkedIn). We asked interested participants to complete an online screening questionnaire, which about 30 completed. We aimed to recruit a demographically-diverse sample of participants. Hence, we included a number of demographic questions about gender, age, educational level, occupation and work field. In addition, we asked participants to specify the smart home devices they use and whether they share them with other users. We aimed to recruit smart home users that (i) were in favor of technology adoption [371], (ii) had previous experiences in data protection (e.g., consent or right of access), and (iii) were technically competent.

We defined different levels of technical competence (novice, competence, proficiency, expertise, and mastery) using Dreyfus' model of skill acquisition [372]. Dreyfus' model has been widely used to define levels for assessing one's competence.

**5.2.2.1.2 Recruitment of Designers and Business Leaders** To recruit designers and business leaders, we also advertised the study in the UK. However, we experienced difficulties finding designers and business leaders willing to share their experiences with data protection. Data protection in many organizations is considered a strictly confidential [403–405], sensitive and/or 'taboo' topic [406]. In addition, many potential participants could not participate due to being bound by non-disclosure and confidentiality obligations.

To address this limitation, we used the snowball sampling method [407], which is commonly used when investigating hard-to-reach groups [408–410]. We also recruited a smart home consultant advisor who had wider access to smart home designers and business leaders working in a professional capacity in the United Kingdom. The consultant facilitated referrals to around 25 smart home designers and 25 smart home business leaders contacts. We reached out to all referred participants by email to arrange interviews, and interested participants were asked to fill a screening questionnaire.

All designers and business leaders were working at different companies, and were not connected to each other in any way. In total, we recruited six designers and six business leaders that represented twelve different companies.

### **5.2.2.2 Participant Demographics**

The demographics of our user participants (see Table 5.4) consisted of seven participants from seven households. Participants were composed of five male and two female participants. Two reported having an undergraduate degree, and five a graduate degree. Three were expert smart home users and four were proficient. As for business leaders (see Table 5.5), all were male (n=6) and leading small and medium-sized enterprises (SMEs). Four came from a technical background while two came from an arts and communication background. Their SMEs sold a wide range of smart home products such as smart locks, smart doorbells and smart vacuum cleaners. Our designer participants (see Table 5.6) consisted of three male and three female participants, all working in different companies. Four worked as UX designers and two as UX consultants. Three participants worked in a flexible team structure, two worked in cross-functional teams, and one in a centralized team.

**Table 5.4:** Demographics of Users

P#	Gender	Age (Degree)	Field	Occupation	Competence	Sharing Devices	Devices Used
U01	Male	35-49 (M.Sc.)	Commercial Insurance	Commercial Finance Analyst	Expert	Multiple Users	Amazon Echo Dot, Hue Smart Light
U02	Male	25-34 (B.Eng.)	Railway Transport	Senior Mechanical Engineer	Expert	Single User	Google Home, Nest Audio, Nest Hub
U03	Female	35-49 (M.Sc.)	Information Technology	Senior Engineering Manager	Proficient	Single User	Google Home Mini, Echo Show 5
U04	Male	25-34 (M.Sc.)	Information Technology	Database Administrator	Proficient	Multiple Users	Google Home Hub, Hue Smart Light
U05	Male	18-24 (P.h.D)	Computer Security	Doctoral Researcher	Expert	Multiple Users	Amazon Echo, Google Home
U06	Male	35-49 (B.Sc.)	Education Leadership	Academic Administrator	Proficient	Single User	Nest Thermostat, Nest Hub Max
U07	Female	35-49 (M.Sc.)	Professional Services	Chief Financial Officer	Proficient	Multiple Users	Ring Doorbell, Nest Thermostat

**Table 5.5:** Demographics of Business Leaders

P#	Gender	Age (Degree)	Background	Executive Role	Team Size	Company Type	Devices Sold
B01	Male	25-34 (B.A.)	Graphic and Media Design	CTO & Founder	18	SME	smart baby monitors, smart alarms, smart trackers
B02	Male	45-54 (M.Sc.)	Computer Science & Digital Electronics	Technology Lead	5	SME	smart cups, smart food containers, smart mugs
B03	Male	35-44 (B.Sc.)	Mechanical Engineering	CTO & Founder	3	SME	smart robots, smart vacuum cleaners, smart mops
B04	Male	35-44 (P.h.D)	Electrical & Electronic Engineering	Co-Founder	25	SME	smart adult toys, smart vibrators, remote vibrators
B05	Male	45-54 (M.A.)	Virtual Communication	CEO & Founder	11	SME	smart doorbells, smart door chimes, smart cameras
B06	Male	45-54 (M.Sc.)	Electronic & Hardware Security	CEO & Founder	7	SME	smart locks, smart digital door locks, smart padlocks

### 5.2.2.3 Interview Procedure

**5.2.2.3.1 Interview Process** To address our research questions, we conducted semi-structured interviews with 20 smart home participants: users (n=7), designers (n=6) and business leaders (n=6). We conducted all our interviews remotely using Skype, Zoom and Microsoft Teams. We also audio-recorded the interviews

**Table 5.6:** Demographics of Designers

P#	Gender	Age (Degree)	Team Structure	Occupation	Experience	Company Size	Devices Worked On
D01	Female	35-44 (B.Sc.)	Flexible	UX Consultant	7 years	50-100	activity trackers, smart cameras, smart speakers
D02	Female	45-54 (B.Des.)	Centralized	UX Designer	5 years	01-50	smart thermometer, smart grill thermometer
D03	Male	25-34 (M.Des.)	Cross-Functional (Embedded)	UX Designer	4 years	100-500	smart locks, smart security sensors, smart alarms
D04	Male	45-54 (M.Sc.)	Flexible	UX Consultant	6 years	50-100	smart speakers, smart displays, baby monitors
D05	Female	35-44 (M.Arch.)	Flexible	UX Designer	8 years	100-500	smart intelligent sensors, smart home automation,
D06	Male	45-54 (M.Sc.)	Cross-Functional (Embedded)	UX Designer	10 years	500-1000	smart indoor/outdoor cameras, smart doorbells,

and took notes to document noticeable events. No participant was compensated for the interviews.

We allowed participants to elaborate, share their thoughts, and ask any clarification questions. We also asked follow-up questions and probed participants when appropriate. This is a common practice in semi-structured interviews, in which the interviewer primarily uses a list of questions, but has the discretion to ask follow-ups or skip questions that have already been covered. The value of conducting qualitative research lies in providing a holistic understanding of the phenomenon under inquiry using predominantly subjective qualitative data, which can be supplemented by observational and other quantitative data [411]. Our interview guide can be found in Section C.2.1.

**5.2.2.3.2 User Interviews** We started with general questions asking users to describe the smart home devices they own, how they use them, and what apps or automation they have installed. We also asked them to describe any previous experiences dealing with or understanding data protection regulation (e.g., exercising their online rights, experiencing consent interactions). In addition, we asked participants to describe their understanding of their data use by smart home companies. To avoid participant response bias [412, 413], we began by querying more general questions that could elicit security or privacy concerns but did not explicitly mention them.



**5.2.2.3.3 Designer Interviews** We started with general questions characterizing the designers' role at the company (e.g., responsibilities, duration of employment), the type of products they designed or developed, and their experiences with UX and data protection regulation. We then asked questions related to requirements gathering and specification in the design phase, as well as questions about how UX was factored into the design process (e.g., data protection design decisions, UX design methods, techniques, and artifacts). Our designer participants referred to different groups of people (e.g., device purchaser, device administrator, and device user in the house) as 'users' without distinction.

**5.2.2.3.4 Business Leader Interviews** With business leaders, we started asking general questions regarding their executive role, their leadership approach, and how they attain business goals and objectives. We also asked them about the products they sold and marketed, their plans for expansion, their customer base, their markets, and innovative industry developments and standards. In addition, we asked business leaders about their experience with GDPR data protection compliance, which included questions regarding their role in implementing a data protection strategy or program, strategic experience in guiding the organization through a process of continuous compliance, and their internal organizational challenges and mismatches with data protection law.

#### **5.2.2.4 Pilot Study**

We conducted a pilot study of three semi-structured interviews to check that the questions for all stakeholders could be understood, and identify any potential problems in the script (e.g., cost, time, adverse events) in advance, so that the methodology could be fine-tuned before launching into the main study. We used the common practice of convenience sampling [414] by selecting three employees (with a background relevant to each user group) in our organization for the pilot study. In addition to the three sessions, we asked two researchers to review the study. No considerable changes were made to the study.

#### **5.2.2.5 Data Analysis**

We transcribed and analyzed all 20 semi-structured interviews using Grounded Theory as described in Section 3.2.2.1. To make our consolidated analysis feasible, we derived a core set of questions linking all interviews together. However, we observed data saturation separately for all our three participant groups. We observed data saturation [388–390] between the 6<sup>th</sup> and the 7<sup>th</sup> interview for users, the 5<sup>th</sup>

and the 6<sup>th</sup> interview for business leaders, and the 5<sup>th</sup> and the 6<sup>th</sup> interview for designers. Data saturation has attained widespread acceptance as a methodological principle in qualitative research. It is commonly taken to indicate, on the basis of the data that has been collected and analyzed, that further data collection and analysis are unnecessary.

After creating the final codebook, we tested for inter-rater reliability for each user group. The average Cohen's kappa coefficient ( $\kappa$ ) is 0.86 for users, 0.80 for business leaders, and 0.83 for designers. Cohen's kappa values over 0.80 indicate almost perfect agreement [370].

In total, the analyzed material interviews consisted of 10 hours and 28 minutes for users (average of 1 hour and 29 minutes per interview), 10 hours and 18 minutes for business leaders (average of 1 hour and 43 minutes per interview) and 8 hours and 19 minutes (average of 1 hour and 23 minutes per interview) for designers.

#### **5.2.2.6 Limitations**

Our study has a number of limitations common to all qualitative research studies. First, research quality depends on the researchers' individual skills and might be influenced by their personal biases. Inexperienced interviewers may not be able to ask prompt questions or probe into situations that would result in missing gathering relevant data [415]. For instance, the depth of data collected is dependent on the interviewer's skill [416] and the quality of the questions asked [417]. To address this limitation, one researcher, who was trained to conduct the interviews consistently and ask questions in an open and neutral way in order not to influence participants, conducted all 20 interviews.

Second, self-reporting bias is common in interview studies [391]. Some participants might have not responded accurately to our questions because they did not remember specific details. Other participants could have been concerned about the interviewer's perception of them and, therefore could have changed their answers in line with how they like to be perceived. For instance, social factors such as ethnicity may influence the answers that different social groups are willing to give [418]. To maximize validity and minimize self-reporting bias, we avoided leading questions and relied on open-ended questions, inviting participants to provide in-depth answers in their own words. Some of our participant answers were less detailed, however, we prompted participants to give full answers to all questions.

Third, as we note in our recruitment section, finding designers and business leaders willing to share their experiences in data protection (e.g., GDPR) is challenging due to legal matters being sensitive and confidential. As a result,

despite numerous efforts, we were unable to recruit any business leaders from large companies. As such, our qualitative work is limited by the size and diversity of our sample. Following recommendations from prior work to interview between 12 and 20 participants [392], we interviewed users, designers and business leaders until new codes stopped emerging.

Fourth, security, privacy, and regulatory matters are sensitive issues in organizations. Our participants' corporate responsibilities, as well as their company's reputation, might have biased their responses. Some participants (e.g., business leaders) were not able to share sensitive and confidential information, and could have stripped essential and valuable research data. To mitigate this, we briefed our participants about our security and privacy measures, focusing on how we will encrypt their data and process it in accordance with the General Data Protection Regulation (GDPR).

Fifth, we note that ours is a qualitative study. We do not attempt to quantify our findings or draw conclusions or generalizable findings about a larger or a wider population of users, business leaders and designers. The focus of our qualitative work is about the richness of understanding rather than the generalizability to a population. Since our methodology was qualitative and exploratory in nature, the hypotheses we formulated based on our findings, emerging themes and discussion coming from the grounded-theoretic analysis, would need to be tested in a follow-up confirmatory study to assess their broader applicability and generalizability.

### **5.2.3 Results**

In this section, we present our findings. We discuss our key themes: the experience of users (Section 5.2.3.1), the experience of business leaders (Section 5.2.3.2) and the experience of UX designers (Section 5.2.3.3).

#### **5.2.3.1 Experience of Users**

Users experienced dark patterns when consenting to personal data processing (e.g., tracking) or giving access to device permissions (e.g., location services). In addition, they experienced dark patterns when exercising their data protection rights (e.g., right of data access). As a result, they perceived the data-value exchange with smart home companies to be imbalanced, confusing, and untrustworthy.

**5.2.3.1.1 Dark Patterns when Providing Consent** Smart home users (n=4) reported experiencing dark patterns when consenting to providing access to their audio recordings, web cookies and device permissions. They experienced four categories of dark patterns: intrusive privacy defaults, difficulty rejecting consent, unexpected detriment and punishment, and forced interactions.

**Obscured and hidden privacy-intrusive selected defaults:** User participants (n=3) experienced hidden privacy defaults that felt intrusive while setting up and using smart home products. U05 reportedly found pre-selected defaults enabled on their Amazon Echo after checking their ‘Alexa Privacy’ settings. U05 expressed disappointment after finding the “*use of voice recordings*” feature activated by default. The feature allowed Amazon Alexa to use customer voice recordings to develop new features as well as enable contractors to manually review the voice recordings. Similarly, U03 said they were shocked after discovering a privacy-invasive feature enabled by default on their Echo Show 5 called ‘Amazon Hunches’. The feature allows Alexa to observe users’ interactions with connected smart home devices like locks, lights and electricity outlets. In turn, Alexa would detect regular patterns and proactively offer to complete tasks around the house, such as turning off lights, based on habits and frequent requests. U03 said they found it ‘*creepy*’ and ‘*disturbing*’ that their detailed home activities were being analyzed and turned into patterns.

**Frustration and difficulty in rejecting consent:** Users (n=3) experienced difficulty while attempting to reject or withhold consent from cookies and device permissions. As a result, privacy-preserving options were more cumbersome. For instance, U02 reported that their Google Home constantly nudged them to give Bluetooth permissions to be able to easily set up the device. U02 said: “*As I was installing the app from the App Store, it kept on asking me to turn on Bluetooth to set up the device even though I was clearly uncomfortable giving that to Google. They even said it can set the device quicker if I turn on Bluetooth.*” Similarly, U04 couldn’t set up their Google Home Hub because it required consent to ‘*location services*’.

**Facing unexpected detriment and punishment:** Users (n=2) have reportedly experienced unexpected detriment from refusing to consent to specific permissions and services. Users facing privacy-invasive permissions said that permissions they attempted to reject turned into roadblocks (e.g., inability to set up the device). Those permissions are known as ‘do-or-die’ or ‘take-it-or-leave-it’ permissions, but do not always make it clear they are necessary. For instance, U04 could not play music on their Google Home Hub without consenting to ‘*Web and Tracking*’ activity monitoring. U04 explained: ‘*I don’t understand why it needs my Google browsing history to play music.*’

**Pressured consent interactions and limited timing:** User participants (n=3) experienced consent interactions that pressured them to make consent decisions before using smart home products. Those interactions prohibited users from postponing their choices, giving impressions that users would be blocked from using the service. For instance U03, who was setting up their Google Home Mini, was presented with privacy preferences (e.g., location, activity tracking, personalisation) before proceeding with the installation of the Google Home. U03 said they were in a hurry and did not see a clear option to postpone their choices to a more convenient time. This added unnecessary urgency and gave little time for U03 to reflect on the choices provided.

**5.2.3.1.2 Dark Patterns when Exercising Legal Rights** Smart home users (n=2) experienced dark patterns when exercising their data protection rights (e.g., right of access). They found the process to be confusing, frustrating and couldn't easily authenticate or prove their identity. As such, they expressed a preference for automated data subject requests.

**Frustration when making data subject access requests:** Some users (n=2) who made data subject access requests found the process to be confusing or frustrating. They were not given any specific instructions for how to exercise their data access rights. U01 reported sending data subject access requests in the past, by making use of letter templates found online to facilitate the process. U01 said that the process of submitting and receiving data access requests was frustrating as they had to wait for weeks to receive an answer. Similarly, U05 who wanted to send data subject access requests found it difficult to get the contact details of the data protection officer. U05 said: *“It would be nice if organizations, for example, had the equivalent of a robots.txt file on their websites that would just list the data protection officer and their email address.”*

**Difficulty authenticating when making data access requests:** Users who reported making data access requests experienced difficulty. For example, U05 who sent different data access requests in the past described their difficulties in authenticating. U05 expressed frustration over having to register new online accounts with third parties to exercise their data access requests. They explained: *“I found that often I have to create a special account on a proprietary or a contracted out GDPR access type system to make requests [...], or I'd have to share documents with some third-party document server in order to prove my identity. There were often a lot of steps in the actual process from wanting to make a request to executing the request and then getting an answer.”*

### 5.2.3.1.3 Preference for automated data subject access requests

Users who exercised their data right of access reported a strong preference for using automated data subject access requests. Users reported a positive experience over using automated platforms that made the experience smooth and efficient. For example, U05 found Google's data subject access request smooth. U05 explained: "*Google's right of access process is really smooth. I can press a single button and execute my right of access request whenever I want.*" Similarly, U01 who wanted to exercise their data access rights for Alexa and Echo devices described Amazon's automated '*Request My Data*' web page as '*convenient*' and '*easy to use*'.

### 5.2.3.1.4 Poor Data-Value Exchange

Users experienced an imbalance in the perceived data-value exchange with smart home companies. They did not know which data was collected about them, how it was used or how much it was worth. As a result, they were not comfortable with sharing data and did not trust the exchange process.

**Not knowing what data is collected and why:** Smart home users (n=3) did not know what data was being collected about them; others (n=2) did not know why some data was collected. For instance, U06 stated that they wanted to know what data is collected by their Nest thermostat but they were unable to find out how to get that information. U06 said that there is no easy way to find out which data is collected and the only available information was Google's Privacy Policy which applies to Google's connected home devices and services. Moreover, some users who were worried about their privacy struggled to find concise, transparent, intelligible and accessible information. U01 explained that they were concerned about how audio interactions were being stored on their Amazon Echo. U01 visited Amazon's FAQ to find more details but they found the information vague. U01 said: '*Their FAQ only told me how to review recordings Alexa has about me and delete them. But nothing shows me how and if the data is stored on my own device and how long it is stored for.*' Similarly, U07 expressed concerns over the lack of knowledge of motion data collected by Ring doorbells. In particular, they were unsure what kind of metadata is collected with every motion and what kind of interactions with the camera are recorded.

**Not understanding how their data is being used:** Interviewees (n=2) said that they don't understand how their data and information was being used by smart home companies. U07 who experienced annoyance over what happens with their Amazon Echo data stated that the company has been unhelpful in providing

any type of personal information. Similarly, U07 said they don't understand how Google Assistant is using their location and making predictions. U07 said: "*I'd really like to know how Google is able to use my location, calendar or whatever to tell me when I should leave the house and which route I should take.*" Users experienced dissatisfaction in understanding how algorithmic decision-making works. It was difficult for them to understand where data comes from, how it is used by algorithms powering smart homes, and where algorithms send data. For instance, U05 experienced frustration over their device 'waking up' without them saying the wake word which caused serious concerns. U05 wanted to access more information about how Amazon detects and processes wake words but they couldn't find any helpful information through official documentation.

**Not knowing how much their data is actually worth:** Interviewees (n=2) said that they aren't aware of the true value of their personal data, but they believed it was worth more than what they are getting in exchange. Specifically, data that is not used to improve smart products is seen as offering a poor value exchange. For instance, U02 who shares their video footage, audio recordings and home environment sensor readings with Google said they would be curious to know how much their data is worth. U02 also said that they don't receive enough benefits for providing sensitive data which could be used for home personalization. Similarly, U06 who shared video footage with third-party apps and services within existing Google Home devices said they wanted to know the true value of their video footage to Google. U03 described receiving '*minimal value*' from their products and expressed the need for visualizations that can summarize all the data collected and how much Google is deriving profits from it.

**Lack of trust in the exchange process:** Interviewees (n=4) reported a lack of trust for major smart home product manufacturers (e.g., Google, Amazon). U01 referred to Amazon as untrustworthy and said they were not sure whether they could fully trust if Amazon Alexa would be collecting more data than agreed. Similarly, U07 who uses a Ring camera said they don't trust the company not to sell their personal data to third parties. U07 explained: "*I've always been wary of our Ring camera. It is quite funny. Going through their privacy page they clearly say they don't sell my personal data to third parties, I don't believe them.*"

### 5.2.3.2 Experience of Business Leaders

Business leaders found the costs of data protection to be unfair to smaller businesses and they lacked the necessary resources (e.g., labor) to address compliance needs. They were also confused due to a lack of consistency and clarity in data protection compliance. As such, they took 'necessary shortcuts' to comply with data protection.

### 5.2.3.2.1 Unfair Data Protection Costs

**Data protection ‘fundamentally unfair’ to small businesses due to lack of resources:** Participants (n=3) argued that data protection regulation is ‘fundamentally unfair’ to their businesses (e.g., small, mid-size) because larger companies have significantly more resources (e.g., time, labor and wealth) to face the data protection regulation challenges. For instance, B04 said that their lack of resources makes it challenging to overhaul their compliance processes and invest in appropriate long-term solutions. Other participants argued that data protection fines are unfair towards businesses because larger companies can afford fines whereas smaller ones would go bankrupt. For instance, B02 said: *“Companies just get away with way too much and there’s no disincentive. [...] And I think that is why you need absolutely huge fines, but you need them to actually be used, because otherwise the companies will just treat it as the cost of doing business.”* B05 said that going through GDPR requirements was difficult for them because they’re a small company with limited resources. He said: *“We went through this and the requirements and so on. It is quite difficult for a very, very small company to understand it and understand what the requirements are actually, but we did make an effort to go through that and to try and make sure we complied.”*

**Fines and penalties applied unfairly across different sized businesses:** Some participants state that data protection fines (e.g., GDPR) are unfair towards smaller businesses. In particular, fines projected against bigger companies tend to be too low. Technology lead B02 who runs a small company expressed disappointment over small fines imposed against big companies. He said: *“I think the enforcement in the UK is poor. The ICO is just pathetic. They just announced their Marriott Fine today. Marriott lost 340 million people’s records. The ICO said they were going to charge them £100,000,000 and they’ve finally come through today and said they were actually only charging them £18,000,000. That’s 5p per person. So then you can just kind of see the Marriott people going: ‘Hey, it only cost us 5p to just do what the hell we like with people’s data. That’s fine, cost of doing business.’ ”* Moreover, business lead B01 claimed that his company can be fined as high as £20,000,000 which he described as *‘nonsensical’*.

**The cost of data protection compliance is unrecognized:** Participants (n=3) stressed that the focus has been on the cost of fines and penalties; leaving little focus on the cost of compliance. The cost of compliance is reported as being prohibitive and unfair: while fines and penalties are proportional to the company turnover, the cost of compliance is not. Unrecognized compliance costs were reported



originating from: educating staff, personal data mapping, reviewing data protection documentation, appointing a data protection officer (DPO), creating privacy notices, and facilitating data access requests and procedures. For instance, B01 expressed dissatisfaction over the high cost of compliance associated with complying with the ‘right of access’. B01 invested in tools to comply with data access requests and described high costs associated with authenticating users, reviewing the legitimacy of requests, gathering data securely and communicating to users.

#### 5.2.3.2.2 Compliance Practices

Business leaders found data protection inconsistent across countries, and lacked information over the implications of non-compliance. They were also confused whether compliance was needed in some cases. As a result, they took ‘necessary shortcuts’ to comply with data protection and outsourced responsibilities to third party vendors.

**Lack of consistency in data protection regulation across countries:** Our participants noted the lack of consistency in data protection regulation across different countries, and more specifically across Europe. B02 who sells smart cup technology in the UK and US described difficulties navigating data protection compliance in both countries citing inconsistencies between CCPA and GDPR. Specifically, B02 said that GDPR limits their capability from processing personal data when there is a legal ground (e.g., consent, contractual obligation), unlike CCPA, which requires consent only when there is a ‘financial incentive’ out of personal data. Moreover, the ‘right to opt out’ in CCPA is an absolute right which means B02 cannot reject an opt-out request on the basis of their compelling legitimate grounds; unlike GDPR where legitimate grounds can be used to continue processing information. This finding is in line with Future of Privacy forum’s [419] report which reports numerous inconsistencies amongst CCPA and GDPR.

**Lack of clarity over legal implications of non-compliance:** Participants (n=2) reported a lack of knowledge over the implication of non-compliance (e.g., amount of fines and type of penalties). For instance, B05 said while GDPR requirements are generally clear, the implications of breaching these regulations aren’t. B05 explains: “*I also had the opportunity to read through the DSGVO, which was the German Data Protection Law before the GDPR. In general, it’s very clear. The actors in the system, what their responsibilities and roles are, and what you need to do offering a product or service. I think what’s not clear is the legal implications. That’s still being sorted out in the courts and in the various jurisdictions.*”

**Confusion whether data protection compliance is needed:** Some participants (n=2) were unsure whether they are liable for GDPR compliance because they were not collecting personal data. For instance, B06, a business leader of a smart lock manufacturer in the UK, explained that GDPR compliance wasn't too relevant since his company did not collect or store personal data. B06 said: *“From a GDPR perspective, we don't gather personally identifiable information. We don't store any of that information that is recognizable to the individual. From that perspective, while we do comply with all of the regulations that are in place, they are less relevant to us because of the way that we don't actually gather data in the first place.”*

**Taking ‘necessary shortcuts’ to comply with data protection:** Some participants (n=3) struggled to find suitable processes and practices to address data protection. As a result, they reported taking ‘necessary shortcuts’ and cutting corners to comply with data protection. For example, B03 complied with data protection through his own judgment and reasoning instead of going through the official documentation. He explained: *“Probably complying with them is the easy part actually. The difficult part is almost certainly just reading and wading through the regulations and working out exactly what you have to do. Once you've done that, doing it is probably easy. We've decided that we'd shortcut our process and do what seems reasonable, which is not selling anyone's data, to keep it secure, to keep the minimum amount of data that we need to do the job.”*

**Using third parties to comply with GDPR:** Participants (n=6) engaged with third-party suppliers to process or access personal data on their behalf which made their experience of dealing with GDPR easier. For instance, B04 reportedly chose to use Shopify to sell smart products in the UK citing GDPR-compliant features are built into Shopify's platform. B04 explained: *“Now, everything which is standard, for example, with Shopify, mail platforms, Amazon web services, everything complies. As long as you're using the standard builds of a lot of functions, and you have a very good legal counsel in-house, it is quite easy to comply with GDPR.”*

### 5.2.3.3 Experience of Designers

Designers managed data protection requirements through balancing user needs with business goals. However, they experienced challenges achieving that balance due to poor communication with business leaders. To manage the challenge of data protection design, they developed heuristics (i.e., rules of thumb) to navigate the complexity and constraints of data protection design. Moreover, they recommended that users should be better educated on business models.

### 5.2.3.3.1 Balancing User and Business Needs

Designers balanced user needs with business goals to address data protection designs needs. However, they faced challenges due to difficulties aligning UX efforts with business goals and communicating to business leaders privacy issues and UX needs. **Obstacle in sensitizing business representatives towards privacy issues:** UX Designers (n=3) faced obstacles communicating the security and privacy impacts of smart homes to business leaders. D05 said that they tend to research and provide summaries of privacy issues that might occur from the design of some features. D06, who worked in smart home product teams, said that privacy and security conversations are often “*sailed away with one privacy or security expert*”. As such, security and privacy topics are not part of the regular conversations. D06 said that they make an effort to inform all stakeholders (specifically to business leaders) on possible security and privacy issues they are aware of.

**Difficulty in explicitly aligning UX efforts with business goals:** UX designers (n=2) said that business leaders often do not see the value of some investments in UX. In addition, explicitly translating the benefits of UX designs with business requirements (e.g., user retention, increased sales, conversation, and reduced costs) is not straightforward. For instance, UX designer D06 faced challenges in getting prototypes for a smart camera application approved by business executives. As such, they often identify selective design issues in their prototype that, if fixed, would help business executives better improve business goals (e.g., users purchasing a cloud storage solution for the video recordings). D06 said: “*The reality is that if you work as part of a large product team and your prototype does not move the needle, it will likely be thrown away.*” This finding adds more context to Lallemand et al.’s survey [420] which found that UX experts consider UX goals to extend beyond ones typically held by business leaders.

**Frustration when involving business leaders in UX:** UX Designers (n=4) stressed that involving business and product stakeholders in UX is critical to balancing user and business goals. However, this can be a laborious and frustrating task. D01 explained that connecting business stakeholders into UX research and design is not always possible. This would lead to less commitment within teams and result in uncreative ideas. D01 said: “*The worst thing is people building stuff and designing stuff in isolation.*” Similarly, D04 said that enabling business leaders to experience the customer and to facilitate the cross-functional conversation about the experience is difficult. D04 strongly encourages product teams and business leaders within a team to learn and be involved in UX. D04 explains: “*UX is not exclusively a UX designers’ job. Everyone is responsible for learning and connecting from customers, including CEOs and ultimate decision-makers. They should experience the customer and really have a sense of how they are interacting with the product.*”

### 5.2.3.3.2 Managing Challenges

To manage the challenges and complexity of data protection regulation, designers used heuristics (e.g., rules of thumb, tried-and-tested solutions, learning in production) to find a cheap and fast way to achieve data protection compliance. In addition, they balanced different stakeholder interests (e.g., through visualizations, arranging meetings) to reduce problems and maximize benefits.

**Using rules of thumb to overcome data protection design challenges:** UX designers (n=3) reported using rules of thumb to address data protection design challenges. The rules of thumb aided designers with ‘*mental shortcuts*’ when faced with time pressure or complex conditions. For instance, D06 introduced ‘*just-in-time*’ privacy notices, a rule of thumb from an online UX practice guide for GDPR compliance, into a number of interactions (e.g., the registration page of a smart camera product). Similarly, D02 used two rules of thumb (clearly separating terms and conditions from consent requests, allowing users to separately consent for different types of data collection) to introduce GDPR-compliant privacy notices for a smart heating mobile application. This allowed D02 to introduce a new privacy design without the need to conduct user testing and research.

**Representing and visualizing business and user viewpoints:** UX Designers (n=2) stressed that representing and visualizing user and business viewpoints can be crucial in finding a balanced solution experience, while being aligned with project constraints and business goals. D01 uses their visualization skills to sketch and paint an image that can help business leaders see different users’ viewpoints within a project. Similarly, D02 said they regularly spend time representing and understanding different business goals and perspectives within a project. They stressed that business goals which help grow the company size and revenue improve the product experience for users in the long run. This finding confirms Schaffer and Lahiri’s argument [421] that UX teams participate in practices of organizations developing new products or business ideas.

**Relying on tried-and-tested techniques to move past strong opinions:** UX Designers (n=3) relied on tried-and-tested techniques (e.g., usability testing) to move past subjective and conflicting opinions. These solutions reportedly raised awareness of user needs as they focus on gathering empirical user data instead of subjective opinions. When faced with strong and conflicting opinions, D01 raised the awareness of user needs through usability testing with the whole project team as observers. Similarly, D05 stated that they tend to demonstrate usability videos to business leaders when faced with opposition.

**Balancing stakeholder interests to minimize problems and maximize benefits:** UX designers (n=5) said that competing interests in a project can arise where stakeholders are not on the same page on data protection regulation or have disagreements over its implementation. As such, they resolve conflicts through ‘*satisficing*’ (aiming for a satisfactory result, rather than an optimal solution) or balancing the conflicting opinions of stakeholders. This would lead to a design approach that is pragmatic and, rather than maximizing the benefits and minimizing the drawbacks for all stakeholders, it aims to provide a good enough solution. For example, D06 held structured meetings to address disagreements occurring due to lack of consensus during the product design phase. D06 described organizing meetings with key stakeholders (e.g., business, development, regulatory) where they discussed their conflicts. Similarly, D03 explained that they feel responsible in participating in prioritization discussions where they bring their skills and offer a ‘balanced perspective’ that factors different stakeholder perspectives.

**Continuous improvement of smart products (learning in production):** UX designers (n=3) adopted an on-going design approach where they continuously measure, learn and improve from smart products that are released in production. In particular, UX designers are involved in continuous integration, deployment and improvement of smart home products. Designers set up feedback loops in production where they established a dialog with users and extracted insights and improved understanding of users. In return, they shared their insights with other stakeholders. As such, designers improve and change product features, and introduce new deliverables consistently over time. For instance, D04 who follows a ‘*continuous design*’ approach when designing smart home products ensures that released smart products are over-provisioned to allow for features to be introduced in the future. He explained: “*You have this propensity to over-provision these initial hardware devices. That may mean additional sensors, that may mean additional processing power, additional things like microphones, things like that. Even if you’re not using them in the beginning because it’s much more expensive to do an exchange of those devices than it is to just put those things on the initial device and not use them.*”

**5.2.3.3.3 Educating Users** Designers reported that educating users about the value proposition and business models (e.g., through conversational interfaces) is crucial in smart homes. However, this can be challenging due to the inability of some users to understand how technology works.

**Users should be taught data monetization business models:** UX designers stressed that users should have a clear understanding over business models and

how their data is monetized, especially when the service is free. D01 explains that understanding business models is part of a user's experience: *"This might not necessarily be user experience designer's job, but the fairness or otherwise of the business model, and how well users understand it, and how they perceive value exchange is part of a person's experience of that product or service. If someone's monetizing your data for other things, it might allow them to charge you less as a customer. But then your data is being used in ways that you may not really have any control over."*

**Users should be educated through more conversational interfaces:** Instead of communicating to users through text, UX designers (n=2) suggested that making smart home interfaces more conversational is likely to improve users' understanding of data use. D01 explains: *"This is off the top of my head, but let's say: 'It looks like you're out, but you haven't set the burglar alarm.' or 'It looks like you're out, maybe we should put the security cameras into motion detection mode. We can do that with your electricity data, but are you happy for us to use your electricity data to infer when you're at home or not?'"*

**Difficulty for users to understand how technology works:** Users who are unable to understand how technology works in general might struggle to understand how their data is processed. As a result, it is difficult to know if users are paying for a well-designed system or not. D05 explained: *"I came from an architectural background, and for me programming is secondary, my second life that I've come to be in contact with. One of the things that I could empathize very well is the fact that if you don't know technology yourself, it seems like a huge barrier to mentally understand what lies beyond the surface of it."* Moreover, D06 stated that users who purchase smart speakers might not be aware that they might not work without a cloud back-end. He explained: *"If you buy an Amazon Echo, it's a peripheral for a piece of software running in a data center really, isn't it? I don't think people (a), realize that; then (b), realize they have an object in their home. They don't realize how connected it is to the servers and what data is being transmitted backwards and forwards."* Further, D04 explained that some users might be unable to assess whether the price they are paying is fair and represents good value. D04 explained: *"I think the issue here is that there's no way for an end consumer to know if I am considering purchasing or using a well-designed system? Or is this the cheapest possible thing that could be brought to the market?"*

## 5.2.4 Discussion

In this section, we first discuss how our findings relate to the wider context of ethics, in particular how dark patterns evolved to fill a gap in regulation, and the role of *honesty* as a means of building trust in the relationship between users and companies. We then focus on UX data protection practices, exploring the principles behind discount data protection among designers and business leaders, and discussing the wider applicability of this concept. Finally, we discuss how our findings can lead to new implications for the design of data protection experiences.

### 5.2.4.1 Implications for Ethics and Data Protection

**5.2.4.1.1 Dark Patterns arise from Conflicts of Interest:** Users experienced a wide range of dark patterns (e.g., magnified sense of urgency and scarcity, manipulation to trick users into action, toying with emotions). As a result, users reported wanting companies to demonstrate more accountability and transparency (e.g., U02 wanted to know what data they are giving away). In addition to experiencing dark patterns, users wanting to exercise their data rights online found the process to be frustrating (e.g., data rights requiring time and effort). Data protection regulation lacks explicit instructions over how easy it should be for users to exercise data rights online: while the exercise of legal rights is protected, the ease with which they can be exercised should be seen as an ethical choice by the business and UX designer.

Dark patterns can be seen as an instance of unethical design practice that has become extremely commonplace since data protection regulation took effect. In addition to employing persuasive design techniques to make it easy for users to agree and difficult for them to object, there are some instances of companies that refuse to offer their services unless the user consents to all data uses. For companies that choose to employ them, the appeal of dark patterns is to minimize the number of users who choose to partially consent to data uses, which can in turn lead to a reduction in data monetization, but also lead to reduced functionality or worse user experiences. The prevailing perception of dark patterns is that they are objectionable and this has driven further regulation, e.g. California has legislated to outlaw their use under CCPA [175, 176].

Dark patterns are not accidental – they are deliberate acts of manipulative design. They have been described as ‘*willfully dishonest design*’ [422], ‘*asshole design*’ [423], ‘*diabolical*’ [424], ‘*deceptive*’ [425], ‘*unethical*’ [426, 427], and ‘*manipulative user interfaces*’ [428, 429]. We note that dark patterns arise out of a conflict of interest

where the business in charge of designing and implementing the consent exchange has a material interest (e.g. data monetisation) in one particular outcome. As a result, the appeal of dark patterns is to facilitate the preservation of business imperatives and interests (e.g., collecting and using more data) at the detriment of user needs (e.g., respecting the data rights of users). Our results show that dark patterns are only one example of what can happen when business needs aren't aligned with data protection requirements, where the responsibility for implementation of data protection can lead to conflicts of interest, and where the incentives for respecting users' needs are insufficient when matched against business drivers.

**5.2.4.1.2 Value Exchange:** With personal data being described as the “new oil” over the past decade (e.g., [177, 430]), we are entering an economy where personal information is the new currency (e.g., [431, 432]), however the value of this currency is not understood by many users [195, 199]. In addition, just like oil, we are witnessing the negative consequences and impacts arising from large-scale data mining of personal data [433].

Our results show that smart home users do not perceive the data-value exchange in the same way that businesses do. Users expect smart home products that are respectful of their security, privacy and safety. Business leaders conversely are expected to find new opportunities to collect customer data and to monetize it.

In addition, our results reveal that users do not have a detailed understanding of the value of their personal information. Our participants had minimal information over the value of their personal data and frequently interacted with products that failed to explain what data they were giving away. The only real source of information about the value of personal data comes from mass media (e.g., news stories about data breaches). For instance, our Amazon Echo participants had to pay separately for the price of the device, audio-book plans and music services. However, they had no clue how much personal data is shared with Amazon, how valuable it is, and precisely what they are getting in exchange.

While some experts advocate for the use of personal data marketplaces to address value exchange imbalances (e.g., [181, 182]), these might not be suitable for smart homes users. While data marketplaces are helpful in business-to-business relations, business-to-customer relations aren't best framed as a financial exchange. Instead, they could be better framed as an ethical positioning (e.g., companies being trustworthy and acting honestly), and framed according to the value that the personal data of users can have for the wider society or the public good.



Future technologies with business models that aim to collect, manage, and monetize personal data should explicitly demonstrate how user data is being monetized. For instance, companies can redesign consent interactions to clearly demonstrate to users how much their data is worth and what value they are getting – instead of simply requesting consent to data use. This would allow users to learn the value of their customer data and make more mindful decisions about data use. Another option in this space could include moving away from individual consent interactions and towards standard data usage models that represent transparently negotiated and ethical data usage practices. Although this could be seen as undermining individual choice and agency, there are arguably advantages to this for communal spaces such as smart homes where individual data use decisions may affect bystanders or other users.

**5.2.4.1.3 Outsourcing in Data Protection** As a common form of outsourcing, many product manufacturers use third-party Consent Management Platforms (CMP) to solicit consent to tracking cookies. Nouwens et al. [175] reported that 75% of top 10,000 websites in the UK outsource their cookie consent processes to use third-party CMPs. However, they found that the vast majority of websites outsourcing consent notifications through CMPs (e.g., QuantCast, OneTrust and Cookiebot) deployed dark patterns (e.g., rejecting all tracking was “substantially more difficult than accepting it”). Researchers noted that popular CMP implementation wizards allow their clients to configure consent preferences, which indicates that dark patterns configurations could have been created by business owners [434].

Data protection best practices are frequently reported and adopted by thousands of small businesses [435]. Data protection best practices often consist of checklists (e.g., [436, 437]), guides (e.g., [438, 439]), and frameworks (e.g., [440]). While best practices provide efficient or prudent courses of action, they are not universally applicable. Best practices tend to come from top performers in an industry, which prompts smaller companies to follow them [441]. Regulatory experts are skeptical over ‘best practices’ adopted as a law practice (e.g., data protection) [442]. Data protection best practices that have worked for certain companies wouldn’t necessarily work for all companies. As a result, we argue that business leaders should develop a very critical eye of whether best practices are appropriate beyond the fact they’re already in use [443]. Business leaders should avoid benchmarking and instead routinely test their best practices to check that they hold over time and address any problems that arise.

Our results reveal that many of our business leaders have outsourced aspects of data protection compliance. Reports show businesses are increasingly dependent on third parties to comply with data protection [444]. Outsourcing has been proven to be beneficial and sometimes essential for small business leaders. For instance, the appointment of a new employee to act as a Data Protection Officer (DPO) has been reported to be an unrealistic burden for small businesses. Business leaders with owner-operated businesses or small teams who act as their own DPO may not be effective in ensuring GDPR compliance due to “*conflict of interest with possible other tasks and duties.*” [445]. As such, outsourcing the role of DPO to third-parties would be beneficial for small business leaders.

However, outsourcing data protection duties to third parties should be addressed very carefully. Third party compliance vendors tend to market their products as a way to avoid GDPR compliance entirely [446]. However, data protection mandates that business leaders are responsible for their third-party vendors’ GDPR compliance and could be liable for third-party breaches. Moreover, they should define areas and activities in which the GDPR is in scope, and have third-party vendors agree and provide signed contractual assurances [447]. In the UK, the ICO mandates that third-party vendors cross-handling data with outsourcing businesses would find themselves equally liable for data breaches [448]. Some argue business leaders delegating data protection duties to third parties are in a more vulnerable position, as they are paying to outsource, as opposed to training their own staff [448].

The effectiveness of data protection practices is a critical aspect in successfully navigating the complex space of regulation and protection. While ‘best practices’ aim to help identify the most effective solutions, in reality they largely document the most common solutions, and moreover these tend to be contributed by companies that may not be representative of the wider industry. To help improve how business leaders gauge effectiveness, we argue (i) that data protection solutions need to clearly document their source and target industry, and that (ii) the scope of outsourced solutions and their relevance to data protection requirements need to be clearer and designed to help with comparison. While these need more research, both proposals arise from existing problems in judging effectiveness: (i) in evaluating the relevance of proposed solutions, and (ii) in comparing different offerings.

#### 5.2.4.2 Discount Practices

We found that *discount data protection practices* cut across all stakeholders. Our results confirm that all stakeholders (e.g., users, designers, business leaders) developed processes and practices to address the challenges of data protection regulation and had a strong preference for approaches that have a good cost-benefit value. The propensity for users to take shortcuts and apply heuristics for dealing with security and privacy is already known, and our findings confirm that users are indeed behaving in a similar manner for data protection choices, e.g., users were confused about how consent notices function, and perceived them to be manipulative and meaningless. As a result, they deployed coping strategies to address them: they ‘*clicked away*’ privacy notices or regularly ignored them. In addition to this, our findings also highlight that taking shortcuts and using heuristics also extend to other stakeholder groups: designers and business leaders.

Business leaders of SMEs found the costs of data protection to be strategically limiting and lacked proper resources to address the data protection demands. As such, they took ‘*necessary shortcuts*’ (e.g., workarounds, common sense interpretations, cutting corners) and outsourced data protection duties to third-parties. UX designers also faced challenges in balancing user needs with business goals and conducting formal extensive processes to keep up with the need for speedy development in smart homes. They used rules of thumb and relied on tried-and-tested techniques to navigate the complexity of data protection design needs (see Section 5.2.3.3.2). We build on this to discuss the wider concept of discount data protection and how this relates to the needs of designers and business leaders:

**5.2.4.2.1 Discount Practices for Designers:** Discount *usability* principles [449] have previously shown to provide a strong value proposition for usability designers. This allows them to perform quick, iterative, and cheap usability testing rather than full-on, expensive, or one-off user tests.

Our results demonstrate that the problems that inspired discount usability (e.g., lengthy, untimely, and expensive usability testing processes) are similar to the problems reported by our design participants dealing with data protection. As such, we argue that the principles that inspired *discount usability* can be used to frame discount data protection.

Discount usability design methods are highly compatible with Agile development principles [449]. For instance, the “*discount usability engineering*” movement has demonstrated that discount usability methods are the best way to increase UX because they are cheap and fast; and as a result designers can use them frequently

[450]. Given that all our design participants followed an agile product development process during the design of smart home products, data protection techniques that fit into an iterative, fast, and agile context are highly desirable.

Discount usability methods have a strong emphasis on techniques that are cost effective, and can outperform more expensive (or deluxe) usability by focusing on early and rapid iteration with frequent usability input [451]. For example, narrowed-down prototypes, such as paper low-fidelity prototyping, can give a faster way for smart home designers to simulate a holistic user experience (e.g., testing very early, iterating through many rounds of design) [452]. Our findings suggest that designers also favor solutions that demonstrate a clear value to their UX efforts (e.g., by helping resolve conflicts, either through usability testing or satisficing rather than optimizing different stakeholder needs). As a result, data protection techniques that demonstrate a strong value to the designer, helping them to resolve problems or to align their UX efforts to business needs are very desirable.

Based on this, our view of discount data protection encompasses pragmatic solutions that help designers to apply, evaluate, and iterate through different UX designs for data protection in an agile manner. While the benefits of early discount usability have become apparent, we believe that the benefits of early discount data protection will result in solutions that better suit the needs of different stakeholders and result in better data protection experiences.

To illustrate this, we propose the following example of a discount data protection method, which is inspired by the discount usability practice of using heuristic evaluation to assess user interface designs, instead of testing interfaces with users [75]. Heuristic evaluation allows designers to determine whether interfaces and interactions follow usability principles and achieves a high level of quality by combining the views of several designers to arrive at a consensus. This allows designers to gather early, quick and relatively inexpensive feedback to input into the design process [339]. We believe that a similar approach can be applied to the design of data protection experiences, and we propose the idea of a *heuristic evaluation of data protection experiences*. This technique would require several designers to reach a consensus in evaluating a data protection experience according to user, regulatory, and business perspectives. To do so, they would employ principles and apply heuristics to consider usability, honesty, fair data exchanges, and business alignment.

**5.2.4.2.2 Discount Practices for Business Leaders:** Reports and studies have demonstrated that bigger companies provide better data rights exercising experiences [453–456]. While larger companies (e.g., Google, Facebook) can afford to invest more into improving the experience of exercising data rights (e.g., enhanced privacy settings, increasing transparency with YouTube videos), small businesses leaders have reported lacking resources (e.g., labor, skills, budget) to facilitate the implementation of GDPR. With a clear emphasis on cost-effectiveness, discount data protection practices should help to introduce more tools and business-friendly solutions to facilitate the implementation of data protection by small businesses.

While a focus on suitability, efficiency and effectiveness are core to ensuring that techniques suit the budgets of all businesses, another facet offered by the concept of discount data protection lies in the possibility of using discounts to incentivise change. The current approach to data protection incentives is framed around using regulatory fines to punish breaches, however a more comprehensive approach could make use of discounts on the cost of compliance either to incentivise specific practices, or to address issues arising from the fixed overheads associated with compliance being too significant for small businesses. While the specifics of how such a funding model could be devised are beyond the scope of this thesis, given that data protection costs are usually not borne by those who benefit from data protection improvements, we believe that this could prove to be a fruitful area of future work.

Overall, the concept of discount data protection aims to support business and designers in addressing the data protection problems that matter most. We have described how designers and business leader perspectives can be taken into account, and outlined a series of recommendations aimed at supporting those stakeholders.

## 5.3 Discussion

### 5.3.1 Discount Practices

Both studies revealed that stakeholders (e.g., users, designers, business leaders) developed discount processes and practices to address the challenges of security, privacy and data protection in smart home products.

In the first study, UX designers used discount practices (e.g., used rules of thumb, heuristics, third parties) to address challenges of security design. In addition, software engineers made use of third-party products (e.g., Amazon Alexa) to outsource their requirements. In the second study, UX designers used rules of thumb and relied on tried-and-tested techniques to navigate the complexity of data protection design needs. In addition, business leaders took necessary shortcuts

(e.g., workarounds, common sense interpretations, cutting corners) and outsourced data protection duties to third-parties.

A key difference between the studies is that study 2 considered the economic interests of product manufacturers or business leaders, which revealed how the strategic interests of the business leaders conflict with the personal interests of the users (e.g., business leaders perceived that data protection costs to be unfair whereas users experienced dark patterns).

### **5.3.2 Lack of Security Innovation**

Both studies revealed that designers did not innovate in the design of their own security solutions. Instead, they used existing security solutions in their company's security protection paradigms, a practice known as tried-and-tested security.

In the first study, UX designers used established, tried-and-tested solutions (e.g., previous traditional security solutions that were seen as effective and reliable to fix certain design problems) to address challenges of security design. For instance, Product Manager A1, who worked with the Design Team that did not include security experts, chose the “*username and password*” authentication mechanism since it was familiar, widely-used, and accepted in industry. In study 2, designers and business leaders used tried-and-tested techniques rather than innovating to navigate the complexity of data protection design needs. For example, D01 raised the awareness of user needs through usability testing with the whole project team as observers. Similarly, D05 stated that they tend to demonstrate usability videos to business leaders.

A key difference between the studies is that study 1 found that UX was seen as helpful by UX designers in fostering innovation in the design of privacy solutions, but not the design of security solutions. In contrast, study 2 jointly factors the perspectives of users and business leaders.

### **5.3.3 Difficulty Navigating Data Protection**

Both studies revealed that designers and business leaders found difficulties navigating data protection design requirements. Data protection guidelines were found to be high-level and impractical. Moreover, they created a conflict between different stakeholders (e.g., users, business and regulation).

In the first study, our participants reported that GDPR touched on facets of product design but often failed to translate into specific requirements, which caused disparities in the design process. Moreover, different and conflicting design

goals arose during the design phase. Security Manager A3 reported dealing with a conflict between the legal and commercial department. In the second study, our participant balanced user needs with business goals to address data protection designs needs. However, they faced challenges due to difficulties aligning UX efforts with business goals and communicating to business leaders privacy issues and UX needs. Moreover, they faced time pressure or complex conditions when trying to address data protection design guidelines.

A key difference between the studies is that study 2 revealed that data protection was unfair to smaller businesses because they lacked the necessary resources (e.g., labor) to address compliance needs. Study 1 focused more on designer experiences and challenges.

## **5.4 Conclusion**

In this chapter, we explored the role of UX in the design of security, privacy and data protection in smart homes. To achieve our research goal, we conducted two studies. First, we conducted an interview-based study with 20 UX designers working in smart home companies; which resulted in a qualitative investigation and a Grounded Theory of UX design processes. Second, we conducted an interview-based study exploring data protection perspectives from users, designers and business leaders; which resulted in a qualitative investigation of data protection experiences. We summarized the key findings of our studies and discussed the implications.

*“A heuristic is a fast and practical way to solve problems or make decisions. In UX design, professional evaluators use heuristic evaluation to systematically determine a product’s usability. As experts, they go through a checklist of criteria to find flaws which design teams overlooked.”*

— Interaction Design Foundation

# 6

## Design Heuristics for Smart Homes

The purpose of this chapter is to explore how UX design principles can be factored into the design of security and privacy of smart home devices. Therefore, this chapter tackles our third and final research question: *RQ3: How can UX design be incorporated into the design of security and privacy of smart home devices?*

To address our research question, we used conceptual framework analysis from previously collected data and literature where we investigated the following research question: *How can we inform product design to incorporate UX practices into the security and privacy of smart home devices?* Our conceptual framework analysis resulted in a **design heuristics framework** that was aimed at participatory design environments and consisted of (i) a description of lifestyles, process models, repurposing, reuse and usage models in smart home environments, and (ii) a set of 32 heuristics for the design of security and privacy in smart home products. To evaluate our framework of design heuristics, we asked: *How can we apply and evaluate practices which factor UX in security and privacy in the product design process of smart home devices?* To address this, we engaged with groups of UX designers, developers, security engineers, and users in participatory design workshops to explore opportunities for their use, and we systematically analyzed the workshop transcripts in order to evaluate the use of the heuristics. We discuss the implications of this chapter in Section 5.3.

### 6.1 Motivation

Our results in Chapter 4, 5 and 6 demonstrate that privacy, security, and data protection challenges in smart homes require more involvement from users, designers,



bystanders, businesses and regulators. For example, data protection regulation has undergone significant changes over the past few years and is still evolving in the face of new technical developments, advocacy efforts, and legal rulings. The aim of such regulation is to provide greater protection and recognition for individual data rights, define how businesses and other organizations can handle information, and impose fines for breaches. Given the interconnection between business models for data use, data protection regulation, and user consent for data use, the problem of designing privacy and data protection in smart homes is not straightforward. Yet it is precisely this design challenge that needs to be addressed in order to ensure responsible and appropriate data use from smart home technology.

In this chapter, we focus on consent user experiences as they have been widely studied in the literature and consist of a clearly designed encounter, the nuances of which encompass contextual, economic, compliance and strategic business priorities. We aim to address this challenge by proposing a series of design heuristics grounded in User eXperience (UX) principles for consent in smart home devices and the previous literature.

## 6.2 Methods

Our literature review in Chapter 2 highlighted common smart home consent and permission problems as part of the UX of data protection with smart home devices. Although privacy-by-design principles are available, and researchers have proposed principles such as seamfulness, apparency, and mindfulness, designing for the UX of data protection in smart homes remains a challenge. In practice, the way UX designers engage with challenges of data protection is often not driven by methodological rigor and scientific curiosity. The various demands of their job require compromising for the most feasible approach. Discount UX methods such as design heuristics can inform the design process to generate innovative solutions which improve on the status quo of UX for data protection in smart homes.

Taking into account insights from our prior work on UX and data protection in smart homes reported in Chapter 4 and 5, we decided to *explore design heuristics for improving on UX for data protection in smart homes* following a three-step approach.

1. Constructing design heuristics using conceptual framework analysis from previously collected data and literature;
2. Engaging groups of UX designers, developers, security engineers, and users in participatory design workshops to explore opportunities for their use;
3. Systematically analyzing the workshop transcripts in order to evaluate the use of the heuristics.

## 6.2.1 Construction of Framework of Design Heuristics

Conceptual framework analysis [352] has been used widely to create conceptual frameworks. Jabareen proposes conceptual framework analysis based on Grounded Theory [389] as an alternative. All data for the analysis must relate to a specific phenomenon. Data sources include articles, books, essays, interviews, guidelines, standards, and practices. The approach involves eight main phases: (1) mapping the selected data sources; (2) extensive reading and categorizing of the selected data; (3) identifying and naming concepts; (4) deconstructing and categorizing the concepts; (5) integrating concepts; (6) synthesis, resynthesis, and making it all sensible; (7) validating the conceptual framework; and (8) rethinking the conceptual framework [354]. We used conceptual framework analysis (CFA) to generate heuristics of opportunities and challenges for the UX of consent processes and permission requests.

### 6.2.1.1 Data Analysis

Our conceptual framework analysis used data from previous studies, design workshops for heuristics, design heuristics, and best practices that have been developed targeting security and privacy in smart homes. This body of work was used to identify, integrate, conceptualize, and theorize core concepts from designing security and privacy related technologies in smart homes. Afterwards, we used these insights to systematically analyze a body of data collected from our prior investigations in smart homes security and privacy in Chapter 4 and 5 to derive a set of design heuristics.

In addition to our published work, artifacts were identified by searching for e.g. “smart homes”, “design [guidelines, heuristics, principles, practice]”, “consent [management, interaction, design]” in Google Search and Scholar, and ACM and IEEE libraries. We initially included work that focused on areas of consent, smart home context, and design, however the analysis drove new queries to explore areas which emerged from the coding. The process of gathering data and coding stopped once additional data had ceased generating new insight (theoretical saturation). The resulting body of work included 125 references which can be found in Appendix D.3.

Our study resulted in a design heuristics framework that was aimed at participatory design environments and consisted of:

1. A description of lifestyles, process models, repurposing, reuse and usage models in smart home environments.
2. A set of 32 heuristics for the design of security and privacy in smart home products.

The number of heuristics was driven by the CFA, and structured in three major themes: Knowledge, Consent and Communication. With approximately 10 heuristics per category, the categories provided structure for participants to explore and understand the heuristics sufficiently.

We present a detailed our framework below in Figure 6.1.

## 6.2.2 Applying the Framework in PD workshops

Following calls from previous contributions bridging the gap between privacy and design [457, 458], we adopted a participatory design (PD) approach to investigate our research question. Known as the “*third space in HCI*” [459], PD reinforces the role of end users as stakeholders in the design process and can be instrumental in understanding their values and expertise [458, 459]. Thereby, PD invites interpretation by users and focuses more on collectivism than individualism, with a heterogeneity of perspectives becoming the norm [459].

In electing to use PD, we intended to allow the interpersonal character of data protection in shared spaces to take center stage in our investigations, more fully exploring its contextual nature. Exploring data protection “*through the eyes of stakeholders*” [458] in this way allows us to investigate how stakeholders make sense of the proposed design heuristics and apply them for a specific design task.

### 6.2.2.1 Workshop Procedure

We first presented our framework and heuristics to participant groups and asked them to read, understand and examine the heuristics and the framework given to them. Second, we proposed the problem scenarios to the participants and monitored how they self-organized and addressed the problem. As part of our problem scenarios, we asked participants to (i) design for consent interactions and (ii) design for permission interactions in which users would be asked to consent. Participants were asked to look into permission design as a means of trying to understand how consent should be dealt with.

We tightly controlled the discussion to ensure that workshop participants were accentuating the identity assigned to them. For instance, participants with the role of ‘mobile developer’ were focused on deriving mobile application prototypes whereas participants with the role of ‘security engineer’ were analyzing security problems that could have occurred.

We started gathering design ideas from participants addressing these design problems, and asked their feedback about the heuristics given to them, noting down

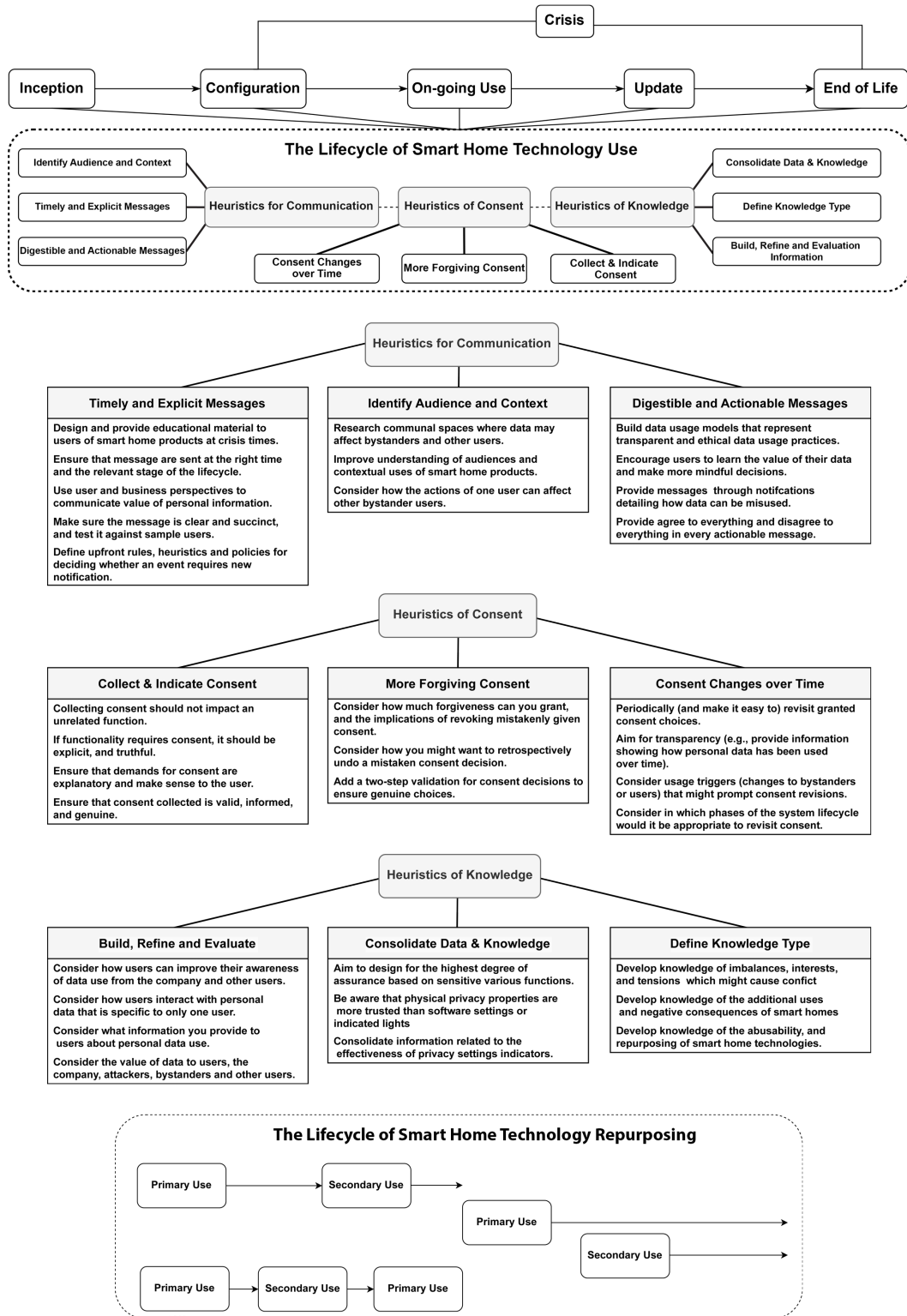


Figure 6.1: Framework of design heuristics that resulted from our conceptual framework analysis

what worked well and what didn't. Third, we conducted collective feedback sessions with the participants where we collected general feedback about the workshop, focusing on the utility and the use of heuristics.

#### **6.2.2.2 Participant Recruitment**

To recruit our participants, we posted flyers and distributed leaflets in the United Kingdom, and advertised the study on online platforms (e.g., LinkedIn). The participants were selected carefully whereby they all were tied to roles for which they had experience.

#### **6.2.2.3 Pilot Study**

We conducted a pilot study of our workshop to make sure that the questions for all stakeholders could be understood and to identify any potential problems in the script (e.g., cost, time, adverse events) in advance, so that the methodology could be fine-tuned before launching into the main study. We used the common practice of convenience sampling by selecting one member in our organization for the pilot study. No considerable changes were made to the study.

#### **6.2.2.4 Data Collection and Analysis**

We conducted the workshops, from which the data collected included participants' notes, pictures of any sketches (context and design solutions), and audio-recording of the workshop itself. At the beginning of each workshop session, we presented the same induction to all participants summarizing the heuristics and their use. After every session, we came together to reflect on the session and adapt the approach as required. Audio recordings were transcribed verbatim by a transcription service and proof-read. Participants and groups are assigned unique identifiers, shown in Table 6.1 that are used throughout the chapter.

The thesis author and the principal investigator then inductively and thematically analyzed the transcribed recordings. An open coding approach was applied to allow themes to emerge from the data. The thematic analysis also included participants notes and any produced sketches. We triangulated between these data as presented in the results section. Some discussions and design features were driven by information we introduced deliberately.

### 6.2.3 Evaluation of the Framework of Heuristics

To evaluate the usefulness and the application of the heuristics, we looked at the heuristics, the models, and descriptions of reuse and lifecycle. Due to the nature of our participatory design workshops, participants were more focused on heuristics, rather than the description of lifecycle and reuse of our design framework. As such, we focused exclusively on evaluating the security and privacy design heuristics individually rather than the framework holistically. We provide more details about this limitation in Section 6.2.5.

#### 6.2.3.1 Heuristics Evaluation

The purpose of our evaluation and analysis was to identify how heuristics are used in design workshops and hence how they can be useful to designers of consent interactions and inform privacy by design. Furthermore, since this was a co-design space, every participant brought their own background and previous experiences. We chose to analyze the design discussions that explicitly mention our heuristics in order to rule out factors related only to the participants.

#### 6.2.3.2 Data Analysis

Two researchers analyzed the design workshops with thematic analysis in order to evaluate the framework of heuristics. Evaluation of the heuristics was based on (i) whether the heuristics were understood or not, (ii) the number of times the heuristics were referenced, (iii) the reception (i.e., sentiment) of participants' responses for heuristics according to a simple closed-coding scheme: positive, neutral, negative, or indeterminable, (iv) the goals of the participants when trying to use the heuristics.

The thesis author and the principal investigator independently completed an initial coding of all transcripts. The initial coding had an agreement of 0.68 (average Cohen's kappa coefficient ( $\kappa$ ) for all codes in our data). After cross-reviewing coding decisions, clarifying coding rules, and independently re-coding the utterances, inter-rater reliability increased to an acceptable level (average Cohen's  $\kappa$  was 0.85) [370]. The remaining disagreements were individually negotiated and resolved.

### 6.2.4 Demographics

Table 6.1 summarizes the demographics of our sample (n=14). Our sample consisted of 10 male and 4 female participants. Ages ranged from 18 to 44. Ten participants had a college degree. We divided our participants (n=14) into four workshop groups.

<b>G#</b>	<b>P#</b>	<b>Age</b>	<b>Gender</b>	<b>Degree</b>	<b>Workshop Role</b>
<b>G01</b>	P1	25-34	M	BSc.	UX Designer
	P2	35-44	F	BSc.	Ordinary User
	P3	18-24	M	BSc.	Mobile Developer
	P4	25-34	F	BSc.	Security Engineer
<b>G02</b>	P5	25-34	M	B.S.	Ordinary User
	P6	35-44	M	BA	UX Designer
	P7	25-34	F	B.Eng.	Security Engineer
<b>G03</b>	P8	25-34	M	BSc.	Ordinary User
	P9	25-34	M	BSc.	Security Engineer
	P10	35-44	M	BSc.	UX Designer
	P11	18-24	M	BSc.	Ordinary User
<b>G04</b>	P12	18-24	M	BSc.	Ordinary User
	P13	35-44	F	BA	UX Designer
	P14	25-34	M	BSc.	Mobile Developer

**Table 6.1:** Demographics of workshop participants.

We also categorized participants based on their workshop role: UX Designer (n=4), Ordinary User (n=5), Security Engineer (n=3) and Mobile Developer (n=2).

While each participant was assigned a workshop role based on their background, their workshop role does not preclude bias (Mobile Developers could also be Ordinary Users).

### 6.2.5 Limitations

A major limitation of our study is that workshop design was more articulated around heuristics. As a result, during our open-ended qualitative analysis, we couldn't identify significant quality fact evidence from how the framework was articulated. Therefore, we could not evaluate whether the description of lifecycle and reuse of our design framework were particularly helpful. To address this limitation, we performed a detailed evaluation of the heuristics which allowed us to give recommendations for future design improvements.

Moreover, while the workshops uncovered useful insights into security and privacy design in smart home products, the number of exploratory workshops (n=4) we conducted was limited. Furthermore, the number of our sample is limited (n=14) and our selection of participants was not representative, and although from diverse cultures, all were resident in the UK.

In addition, we demonstrated and evaluated a framework based on given scenarios. However, we do not have data showing what users would do without the framework given the same scenarios. Nonetheless, the purpose of this study was not comparing

our framework against a benchmark, but seeing how it gets used. While we cannot claim that this study is better than other approaches, we can use the results of this study to suggest that the framework of design heuristics is fit for purpose. Moreover, how the heuristics were used in this study was influenced by how our experiment was run. Another limitation of our workshop study is that we are shaping the problem according to how it fits the proposed solution, rather than having a problem in investigating solutions.

## 6.3 Results

In presenting the results of the workshops, we first report the experiences of our participant groups as case studies. We then evaluate how the heuristics were used based on their effectiveness, use and value.

### 6.3.1 Framework of Design Heuristics

Our framework of design heuristics can be found in Figure 6.1.

### 6.3.2 Case Studies

#### 6.3.2.1 Consent as an on-going Relationship

Using the framework and the heuristics given to participants, we asked them to design for consent as an on-going relationship over time for smart speakers. We collected design ideas from participant groups addressing the problem space.

**Group 1:** Tasked with designing for consent as an on-going relationship over time, group 1 used our framework and design heuristics to derive, prototype and iterate new ideas. During the workshop, participants designed two additional consent features for smart speakers. First, they designed audio interactions where the smart speaker assistant asked users to revisit their audio recordings every Sunday. Second, they designed a two-step feature for mobile application of smart speakers where the smart speaker assistant added an extra validation option to ask for contact details and voice recordings, as well as providing an undo button. The heuristics strongly helped participants in deriving new design ideas for the problem posted. Most importantly, it helped engagement and facilitated discussion from diverse and different backgrounds.

**Group 2:** Faced with the same design challenge given to the previous group, group 2 used our framework and design heuristics to derive, prototype and iterate new ideas. During the workshop, participants designed one feature for smart speakers, and



suggested improvement of other features. First, they created a privacy feature for sharing smart speaker accounts among households. The feature added an automated setting where all users heard notifications from linked accounts once a new account is added to the mobile application of the smart speaker. The setting also allowed users to deny and control consent permissions when new users are added. Second, they suggested that more effective communication should be provided over the physical mute buttons in smart speakers. Especially since it wasn't clear to participants whether the mute button in smart speakers physically disconnects to the device.

### 6.3.2.2 Designing Family-friendly Permission Models

Using the framework and the heuristics given to participants, we asked them to design for family-friendly permission models for external and internal smart cameras. We collected design ideas from participant groups addressing the problem space.

**Group 3:** Tasked with designing for family-friendly permission models for smart home cameras, group 3 used our framework and design heuristics to derive, prototype and iterate new ideas. During the workshop, participants designed two additional permission features for smart cameras. First, they designed a communal privacy zone feature for families where all family members specify an area within the smart home camera's field-of-view which can be defined as an off-limits area. The feature broadcasted to all households that anything in the area won't be video recorded. Second, they designed a communal privacy permissions feature in smart cameras that allowed all families in a household to control when and what the device recorded in the home. The framework and accompanying heuristics strongly helped participants in deriving new design ideas for the problem posted. Most importantly, it demonstrated value in the design communications among stakeholders.

**Group 4:** Faced with the same design challenge given to group 3, group 4 used our framework and design heuristics to derive, prototype, iterate new ideas. During the workshop, participants designed one feature for smart cameras, and suggested the development of offline smart cameras. First, they designed a hibernate mode feature for households using a smart camera that could be triggered by anyone in the household. This would allow households to have more autonomy and control over their privacy. Some participants suggested that it can be used in situations where household members experience domestic or external abuse. However, researchers argue that such features won't necessarily be helpful to victims (e.g., an offender would find out if a feature was switched off). More challenges have been discussed by Thomas et al.'s research on hate and harassment [460]. Second, the households proposed that offline smart cameras should be developed in order to be used solely

for the purpose of security monitoring. As such, the workshop participants argued that while offline smart cameras would not benefit from advanced features (e.g., cloud storage, phone alerts), it would nearly eliminate privacy and safety risks that come from connected security cameras.

### 6.3.3 Heuristics Evaluation

Based on our analysis of the workshops, we present how the heuristics were used during the design workshop; how heuristics were helpful in facilitating communication and discussion of different design perspectives; what the underlying goals were behind the use of the heuristics; and how effective the heuristics were according to the design outcomes.

#### 6.3.3.1 The Use of Heuristics

**6.3.3.1.1 Heuristics used alongside other heuristics** Participant groups (n=4) combined multiple heuristics (often from different themes) in order to derive design solutions for the design challenges posed. Participants naturally were able to combine multiple heuristics in order to solve solutions. For example, group G1 combined three heuristics to design an audio interaction feature where the smart assistant asked users to revisit their settings regularly. UX Designer P1, Ordinary User P2 and Mobile Developer P3 used the *“design and provide educational material to users of smart home products at crisis times”* heuristic, the *“provide messages through notifications detailing how data can be misused”* heuristic, and the *“periodically revisit granted consent choices”* heuristic to design the feature. Similarly, group G3 combined the *“consider usage triggers that might prompt consent revision”* and the *“research communal spaces where data may affect bystanders and other users”* heuristics in order to design an automated setting that notifies all households once a new member is added.

**6.3.3.1.2 Heuristics used as a guide for do’s and don’ts** Participant groups (n=2) used heuristics as a guide for do’s and don’ts of a particular situation, and used them as an advice on what they should or should not design in particular situations. For example, the heuristic *“ensure that consent collected is valid, informed, and genuine”* was used as a rule and a custom when designing interactions for collecting consent by group G1 and G3. UX Design P10 referred to the heuristic when Ordinary User P11 proposed a new feature that did not explicitly collect consent from the user. UX Designer P10 said: *“You can’t do that because if you look at the fourth point under Collect & Indicate consent, it says that consent collected should be informed.”*

**6.3.3.1.3 Heuristics used to directly justify an opinion** To convince other workshop participants, participant groups (n=3) used heuristics as an acceptable and logical reason or to justify and defend their opinion in a design setting. In G4, Ordinary User P12 was arguing that smart home manufacturers should consider more than the legitimate interest and consent for the legal basis of processing consent, they should consider whether their practices impact human rights or individual values. However, Mobile Developer P14 disagreed with P12 saying that this is the role of regulations. To defend his opinion, P14 cited the “*develop knowledge of the additional uses and negative consequences of smart homes*” heuristic. P14 said: “*As you see in the figure, developers should develop knowledge of additional uses and negative consequences of smart home usage.*”

**6.3.3.1.4 Storytelling was used in the context of heuristics** Participants groups (n=4) used heuristics to think about important experiences in their real life and used heuristics to derive personal anecdotes and tell stories based on their personal experiences. Participants used anecdotes in two different contexts:

**Using anecdotes to expand and contextualize the heuristic:** Participants groups (n=4) used anecdotal evidence to justify an opinion or to provide greater information about a particular problem. It was trying to expand the heuristic, apply it and demonstrate it. For example, Ordinary User P5 recalled a personal anecdote that closely aligns with the heuristic “*consider how you might retrospectively undo a mistaken consent decision*”. P5 said: “*I remember adding a friend to my Alexa by mistake, and I couldn’t figure out how to undo that. It would be very useful if we can add a two-step validation for these kind of interactions.*”

**Using anecdotes was used to support and backup the heuristic:** Participants groups (n=2) used anecdotes to provide evidence, backup or justify heuristic. For example, UX Designer P10 used vicarious and fictitious storytelling imagined in the eyes of ordinary users to back up the heuristic “*periodically (and make it easy to) revisit granted consent choices.*” P10 said: “*I’d imagine many users are unaware that Google Homes are tracking them in many ways like analyzing their audio recordings. Revisiting their choices and reminding them of what is being collected is crucial.*”

### 6.3.3.2 Design Discussion Context

Heuristics helped participants talk about different design perspectives and problem spaces in different contexts.

**6.3.3.2.1 Heuristics used in a privacy design interaction context** Participant groups (n=3) used heuristics when solving design problems in the context of user interaction design. Most notably, UX Designers in participant groups G1, G2 and G3 in our workshops discussed heuristics in the context of UX and usability guidelines, focusing on user needs and interests. For example, UX Designer P1 argued that heuristics related to consent should never be overwhelming to the user and should try to be as simple as possible. Similarly, UX Designer P6 said that heuristics concerning misuse of personal data could scare users and should be done very carefully.

**6.3.3.2.2 Heuristics used in a regulatory and data protection context** Participant groups (n=4) used heuristics when solving design problems in the context of regulation and data protection. Participants focused mostly on the data protection rights of users in the workshops such as providing and withdrawing consent. For example, Participants P7 and P13 aligned some of our consent-related heuristics with data protection regulation when addressing our design challenges. P7 contrasted the “*consider how you might want to retrospectively undo a mistaken consent decision*” heuristic with the right to withdraw consent. Similarly, P13 contrasted the “*ensure that consent collected is valid, informed, and genuine*” heuristic with informed consent principles in medical ethics.

**6.3.3.2.3 Heuristics used in a technical privacy context** Participant groups (n=3) used heuristics when solving design problems in a technical context. Participants focused on improving design problems such as designing privacy controls by addressing technical aspects of smart home products (e.g., designing better permissions and technical physical privacy control). For example, Security Engineer P4 used the “*be aware that physical privacy properties are more trusted than software settings or indicated lights*” heuristic to discuss the technical difficulties designing physical privacy indicators. Similarly, Mobile Developer P3 used the “*aim for transparency (e.g., provide information showing how personal data has been used over time)*” to tackle the challenge of controlling or knowing what personal data is collected by third party services.

**6.3.3.2.4 Heuristics used outside of privacy design discussions** Participant groups (n=2) also used heuristics outside of privacy design discussions mostly focusing on the lifecycle of systems and use, and the reuse and proposing of smart home devices. For example, UX designer P13 used the “*develop knowledge of the additional uses and negative consequences of smart homes*” heuristic to discuss how the repurposing of smart home products can be more efficient and useful for smart home users. Moreover, UX Designer P6 used our smart home lifecycle map (e.g., Inception, Configuration, On-going, Update) to suggest more user-friendly smart home lifecycle experiences. This finding shows that our heuristics were also useful outside of a data protection or privacy perspective.

### 6.3.3.3 The Goals of Heuristics

**6.3.3.3.1 Problem Understanding** Participants groups (n=4) used the heuristics (n=12) to understand the design problem given to them. The heuristics helped participants take a step back and make sure they understood the design task that was given to them. For example, in Group 4, Mobile Developer P14 used heuristics from the ‘*Define Knowledge Type*’ box to understand the problem space before designing a hibernate mode for smart cameras that protects households from privacy breaches, misuse, or abuse. UX designer P13 argued it is important to understand the imbalances, and tensions in the home that can cause conflict. Ordinary User P12 added that it is also important to understand how smart home technologies can be misused or abused.

**6.3.3.3.2 Problem Resolution** Participants groups (n=4) used heuristics to resolve the design problem given to them. The heuristics helped participants determine essential challenges in design problems, identify, prioritize or select alternatives for a solution. For instance, participants in group G2 used three heuristics to address the problem of multi-sharing in smart speakers. UX Designer P6 added that researching communal spaces affecting bystanders and non-users in the home is crucial for solving the problems. Security Engineer P7 added that it is critical to be able to understand what kind of users can be added to a household. Ordinary User P5 said they would be more comfortable if they had full control over who can be added to their device (e.g., Amazon Household). These participants designed an automated notification setting that gets triggered when a new account is added to a smart speaker.

**6.3.3.3.3 Problem-Solving Discussion** Participants groups (n=4) used problem-solving discussion to resolve the design problem given to them. The heuristics helped participants discuss unsatisfactory situations, design goals, and obstacles that must be surmounted in order to address the design challenge. For example, participants in group G1 had different opinions about the “*be aware that physical privacy properties are more trusted than software settings or indicated lights*” heuristic which has been used for addressing the design challenge of privacy controls around smart speakers. Security engineer P4 argued that the mute button in smart speakers such as Amazon Echo is a hardware button (physical switch) according to various sources, and as a result, there is no need for design changes. In return, Ordinary User P2 said that despite what P4 has mentioned, they still cannot trust that the device will protect their privacy. The group resolved the problem by recommending to provide more effective communication over the physical muting button of smart speakers.

#### 6.3.3.4 The Effectiveness of Heuristics

**6.3.3.4.1 Successful design outcomes** We define satisfactory design outcomes as a situation where the understanding, solution and discussion of the result lead to a clear resolution that satisfies all parties who were present in the workshop. Most design outcomes (n=8) that were tackled in the workshop by the participants were successful. In Groups 1 and 2, participant groups successfully used the heuristics to design outcomes to address the challenge of consent in smart speakers. They designed a two-step feature for providing consent, a consent revisiting feature and a privacy sharing feature. Similarly, in groups 3 and 4, participant groups successfully used the heuristics to design outcomes to address the challenge of permissions in smart cameras. They designed a communal privacy zone feature, a permission alerting feature, and a hibernate safety mode feature.

**6.3.3.4.2 Unsatisfactory design outcomes** We define unsatisfactory design outcomes as a situation that arises when problem understanding, and problem discussion do not result in a clear resolution that satisfies all parties who were present in a workshop. While most design outcomes were successful, some design outcomes (n=2) were unsuccessful. In Group 2, participants disagreed over how privacy features in smart speakers can be effective, mostly whether changing the privacy features (e.g., physical mute button) can improve the privacy assurance. While the participants couldn't use the heuristics to come up with a design solution, they were able to use them to facilitate a discussion around more effective communication concerning the privacy features of smart speakers.

## 6.4 Discussion

### 6.4.1 Prominent Heuristics

We highlight and summarize the design heuristics that had the biggest influence on the design discussions and decisions below:

#### 6.4.1.1 **Ensure that demands for consent are explanatory and make sense to the user**

This was the most used heuristic and was referenced 16 times in the participatory design workshops. This heuristic prompted workshop participants to consider more user-friendly consent experiences that go beyond the minimum legal requirements and ensure that consent requests are fully understandable and clear to the user. For instance, this heuristic was used by Groups 1, 2 and 3 to go beyond what is being required by data protection regulation when designing privacy and security features for smart home products.

#### 6.4.1.2 **Provide messages through notifications detailing how data can be misused**

This was the second most used heuristic and was referenced 14 times in the participatory design workshops. This heuristic prompted workshop participants to improve the transparency of smart home interactions by looking at innovative areas such as conversational interfaces. For example, this heuristic was used by Group 1 when designing a two-step validation feature while users are providing consent for their personal data use. Workshop participants used the heuristic to add or include messages (e.g., risks of consenting to personal data) when two-step validation interactions are triggered.

#### 6.4.1.3 **Periodically (and make it easy to) revisit granted consent choices**

This was the third most used heuristic and was referenced 11 times in the participatory design workshops. This heuristic prompted workshop participants to design for consent as a relationship that can change over time and require updates. For instance, this heuristic was used by Group 2 to examine frequent situations where users might need to revisit their consent preferences and design for appropriate interactions. For example, workshop participants designed a feature that helped users easily revisit their consent permissions once a new user is added to the environment of a smart home application. The heuristic was also used by Group 1 to design a smart speaker assistant feature that makes it easy for them to control their privacy choices through audio interactions.

#### **6.4.1.4 Consider the value of data to users, the company, attackers, bystanders and other users**

This was the fourth most used heuristic and was referenced 10 times in the participatory design workshops. This heuristic prompted workshop participants to relate to the perceptions of value of personal data from all various stakeholders, instead of having narrow views of the dimensions and the value of personal data. For instance, it was used by Group 2 to improve the UX of privacy controls of smart speakers (e.g., physical mute buttons). Workshop participants considered the value of smart speaker audio recordings from the perspective of users (e.g., ability of users to fully control their audio recordings) and business leaders (e.g., ability of the manufacturer to improve the voice recognition service).

#### **6.4.1.5 Develop knowledge of the abusability, and repurposing of smart home**

This was the fifth most used heuristic and was referenced 10 times in the participatory design workshops. This heuristic prompted workshop participants to consider all discoverability features of smart homes that improve security and privacy of the devices but also can be exploited and misused by adversaries. For example, this heuristic was used by Group 4 to design a hibernate mode for smart cameras that can instantly turn off smart cameras in situations of suspected misuse, and also by Group 3 to design a privacy feature which allows household members to restrict sensitive areas of the home from being recorded (e.g., bedrooms).

### **6.4.2 The interplay between Consent and Permissions**

Heuristics, as described in our framework, focused broadly on consent, however it is interesting to note the relationship between consent interactions and permission design. For smart home interactions which are consensual or egalitarian, participants used the consent heuristics to help design permissions models that were well suited to that domestic environment. This would suggest a wider benefit in applying principles of responsible consent management to help design, configure, and manage the permissions for data use in unregulated domestic spaces. More work is needed to fully explore this, however we believe that it is a promising approach for embedding the principle of responsibility into how smart devices are designed and used in communal domestic settings.



### **6.4.3 Problems of Designing for Permissions**

The model underpinning smart home permissions tends to concentrate on authority, and doesn't tackle the problem of decision-making (e.g. helping users decide on appropriate data use for themselves, other users, or bystanders) nor help evaluate the implications of those design decisions. In the absence of permission and administration models which are more consensual or more democratic, our results show that consent heuristics can be helpful in exploring this space.

Furthermore, participants brought many of their own values into the participatory design workshops such as fairness, equality, and agency. Our design heuristics also brought some other values (such as transparency and accountability). While the values of the participants and those embodied in the heuristics were well aligned, we can anticipate that this may not hold for all situations and all cultural contexts. While it is beyond the scope of this thesis to explore it in more detail, that points to a wider problem in the design of technology which aims to operate in less regulated spaces, where different contextual norms and values may conflict with those that are embodied in its design.

### **6.4.4 Why Are Heuristics Useful**

#### **6.4.4.1 Heuristics demonstrated value in communicating design**

Participant groups (n=2) used heuristics to communicate design compellingly. In particular, heuristics gave participants the ability to articulate design decisions which helped to convey to other stakeholders that they can be trusted and have the expertise necessary to address the design challenge. Heuristics also allowed participants to prove purpose, validating that they have thought about their solutions and that there is logic to their approach.

In addition, heuristics elicited and fostered discussions through storytelling and by facilitating communication of specific issues. Heuristics helped participant groups (n=4) in fostering participatory engagement and discussion within different stakeholders, enabling conversation and active skills.

#### **6.4.4.2 Heuristics helped avoid profound analysis needed for complex problems**

Participants groups (n=3) found heuristics to be an effective method for identifying, defining, and potentially solving complex design problems that involved ambiguity, had a lot of unknowns, and had ill defined boundaries of the problem space. They helped to resolve a problem without doing further analysis.

Our results also show that there are more contentious heuristics which were unsuitable for stakeholders and were not used. This may be due to a smaller sample of design workshops and participants, a lack of clarity in the heuristic, disagreement with the intent or values embodied by the heuristic, or due to how the workshops were designed. Overall, we believe that these heuristics are best used to enrich the understanding of designers and to facilitate the communication among the stakeholders rather than providing a solution.

## 6.5 Conclusion

In this chapter, we presented our thesis framework of design heuristics as a useful design technique for smart home consent interactions based on a conceptual framework analysis of data collected from studies in Chapter 4 and 5 and the UX design literature. We demonstrated its application through a series of four workshops exploring how consent interactions can be designed and how consent principles influence the design of permissions models in smart homes.

Based on a detailed analysis of the workshop transcripts, we evaluated the heuristics and identified how these are used in the design setting, and can also be used to foster innovative thinking around consent in smart home devices.

We concluded with a discussion of the heuristics that were most used by our participants, discussed the wider issues surrounding heuristics for consent, and pointed to their role in helping navigate the design of permissions in a domestic communal setting.

*“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.”*

— Edward Snowden

# 7

## Discussion

In this Chapter, we present a discussion of the findings presented in Chapters 4, 5 and 6. The discussion forms our understanding and analysis of the core challenges presented in these Chapters. First, we discussed how consent could be conceptualized as a relationship between users and service providers (see Section 7.1). Then, we discussed how UX can help data protection interactions be more transparent and more broadly supported (see Section 7.2). Finally, we discussed how innovation can help users, designers and business leaders in the design of security, privacy and data protection (see Section 7.3).

### 7.1 Consent is Conceptualized as a Relationship

In this thesis, we exclusively tackle consent which is different from informed consent. Consent is defined <sup>1</sup> as “*any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*” On the other hand, informed consent is defined as “*the process by which a fully informed user participates in decisions about his or her personal data*” [461] and can be achieved by upholding five principles: disclosure, competence, comprehension, voluntariness, and agreement. Informed consent practices are sometimes criticized [462] (e.g., some fail to inform data subjects about the use of personal data).

---

<sup>1</sup><https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent>

In the field of usable security and privacy, consent is conceptualized as a relationship between the *user* using a service and the *company* or service provider providing a product. In Chapter 4, we demonstrated that there are signs that the relationship is not always healthy (e.g., the presence of dark patterns in consent interactions). Healthy relationships involve honesty, trust, respect and open communication between parties who put effort and compromise without imbalance of power. Results from Chapter 4 show that user consent is sometimes coerced and extracted from users. While smart home companies are obliged to give users consent choices, through the evident use of dark patterns, users are having more difficulty to refuse to provide consent and sometimes are tricked to provide consent. We illustrate key points below which conceptualizes consent as an on-going relationship.

### 7.1.1 The Lifecycle of Consent

Our results in Chapter 4 and 6 show that different consent relationships in the context of smart homes from the lifecycle of consent can be based upon four possible scenarios:

- Consent was properly given and both parties were satisfied.
- Consent was erroneously given by the user.
- Consent was granted but needs to be revoked with retrospective effect.
- Consent was granted but needs to be revoked without retrospective effect.

All the possible scenarios provided for the lifecycle of consent highlight the importance of improving the design of consent management. Not all smart home consent management interfaces factor these scenarios. We argue that the lifecycle of consent should be explicitly factored in the design of security and privacy technologies in smart home products.

### 7.1.2 Consent is Dynamic not Static

Our scenarios, results and framework reveal that the life cycle of consent can change over time (see our framework in Chapter 6): users can withhold - grant - revoke - amend consent as they see fit at different times of product use and for different reasons and purposes (e.g., in Chapter 4, Carrie H3a temporarily granted access to her location). Users' consent requirements and preferences can change based on learning about new events becoming evident around the world, becoming aware of new facts relating to technology, or experiencing life events or major transitions – e.g., serious illness, relationship breakdown. User needs are usually not static and final; an unwanted service today can become critical tomorrow. The

dimension of time should be explicitly designed for privacy consent management and allow users to revisit granted permissions (e.g., breach notifications can invite users to revisit their privacy settings).

### 7.1.3 Withholding Consent can be Unpleasant

Our results show that consent can be an unpleasant experience, particularly in cases where users are given options to either grant consent wholesale or be denied services; or be allowed to withhold consent, but have broken features in a device/service. For example, in Chapter 4, Carrie H3a could not play music on her Google Home because she withheld consent to ‘*Web & Activity*’ tracking: a feature that collects queries and device activity across Google apps and services. As such, Carrie H3a perceived the option to consent to ‘*Web & Activity*’ tracking as a false choice. Consent options should give users genuine choice and control; data protection regulation asserts that consent should not be bundled up as a condition of service unless it is necessary [463]. Google Home users have reported that ‘*Web & Activity*’ tracking must be enabled to stream music on the device [464]. It was not clear to Carrie H3a why tracking was necessary for streaming, and moreover this was neither explained upfront in the consent interface nor was the failure to stream music clearly explained as consequence of withholding consent in the Google Home.

### 7.1.4 Consent Changes Should be More Forgiving

Our results show that in the context of smart home products, consent management is perceived to be highly unforgiving and not a safe space in which to make mistakes. In Chapter 4, Tobias H6a in H6 synced his contacts with his Echo device; but regretted his decision. He believed his action could not be undone since Amazon had already received all his contact details, and that this was irrevocable. This is fundamentally tied to the question of what happens to data that was collected when users agreed by mistake, and whether there are options for deleting this retrospectively. While the right to erasure is covered by data protection regulation [465], the process is typically cumbersome and detached from the consent management process. Moreover, in Chapter 4, we show that in Tobias’ H6a experience using smart home products, there were few indicators that explain what would happen to his contact details if he were to withhold his consent. We recommend for smart home designers to offer a time-limited window following consent being granted during which data that has been collected by mistake is automatically erased should the consent be revoked or amended. This approach would help to provide more forgiveness in the case of mistakenly granting consent to data use.

## 7.2 Data Protection Practitioners

In this section, we discuss why designing honest and transparent smart home interactions is important. We then discussed how UX can help practitioners (users, designers and business leaders) in data protection. Finally, we discuss how data protection design interactions could be supported more broadly.

### 7.2.1 Data Protection Interactions in Smart Homes

Previous research in smart home security and privacy strongly advocates for building ‘trusting relationships’ with users [228, 263, 330, 466, 467]. However many smart tech companies have regularly failed to adequately gain the trust of users [468]. When Facebook released an AI-powered Smart Camera, Mozilla Foundation released a report stating ‘*given Facebook’s terrible track record on privacy, we’re worried a lot.*’ [469] Research that has explored the impact of long-term customer-company relationships reported a ‘*trust crisis*’ that costs companies \$2.5 Trillion per year [470, 471].

Some of our interviewees in Chapters 4, 5 and 6 who consented to providing data perceived smart home interactions to be dishonest, poor and lacking transparency. Dishonest and non-transparent practices are harmful to a healthy and trusting relationship between users and service providers. In order for smart home companies to gain consumer trust and build affinity, they will need to consistently demonstrate their social responsibility and develop core values such as honesty and trustworthiness. Designing honest and transparent smart home interactions is critical as honesty is a precursor to building trust, which cannot be designed or bought.

Our interviews with business leaders reveal that smart home manufacturers have little incentive to go beyond the bare minimum to comply with data protection regulation. Our participants described data protection regulation as a ‘*checklist*’ and a ‘*box ticking exercise*’ describing an evident lack of care and prioritization. For instance, B06 said: “*I think what it only does is it leads to a tick box exercise, because ultimately, what you want to show as an organization is that your software is complying with particular GDPR requirements, but does it actually lead to an improvement in privacy practices in software?*” We argue that smart home manufacturers should align more explicitly with transparent and demonstrably honest practices when complying with data protection. This would motivate all stakeholders to go beyond the minimum to develop honest interactions around data protection.

### 7.2.2 UX can Help Data Protection Interaction Design

Our results in Chapter 5 and 6 strongly support the suitability of UX expertise and practices in tackling the challenges that we face in data protection, such as trust and honesty, alignment with business and regulatory goals, and the necessity of integrating data protection into established development processes. Hence, we have proposed a number of recommendations: discount data protection as a collection of techniques and practices aimed at pragmatic, cost-effective solutions; formulating a code of practice to help build a solid foundation of trust in the data relationships between users and businesses; and working towards economically viable solutions that fit the business realities and budgets of enterprises of all sizes.

We believe that these recommendations offer several key benefits over existing approaches:

1. By combining user, regulatory and business needs, a more positive culture can be developed where UX designers and others can raise issues and address them proactively without fear of reprisals. For instance, the ethical aspects of data protection could be made part of a code of conduct for data protection professionals, similar to how chartered professionals have ethical standards to which they are expected to adhere to. This would have the additional benefit of providing a new mechanism for building trust between users and businesses (e.g., an opportunity to address the conflicts of interest, which drive solutions that favor businesses over the needs of users).
2. By placing a strong emphasis on cost effectiveness and pragmatic solutions, discount data protection techniques will help UX designers in identifying and resolving potential conflicts early and effectively;
3. By aligning to agile principles, discount data protection will provide appropriate techniques to support designers in crafting better experiences of data protection in ways that fit their existing ways of working.
4. Finally, by working to offer competitive, cost-effective, or even subsidized solutions to fit the budgets of even the smallest companies, we can start to address the issue of large overheads associated with data protection compliance.

### 7.2.3 Supporting Data Protection Design More Broadly

Our results in Chapter 5 demonstrate a desire for data protection to be more friendly and honest for users, easier to navigate for designers, and cheaper and fairer for smaller business leaders. As such, we argue for the identification and adoption of future data protection practices that are safe, efficient and ethical which

can support data protection design more broadly. Such practices need to embody informed and valid consent from users without killing business models. Moreover, valid discount practices need to have manageable costs for business leaders and introduce solutions that can be safely outsourced to third parties.

Many industries with potential to cause harm (e.g., environmental harm) have a regulatory or voluntary code of conduct for the field. Just like the Medical Code of Ethics, we argue that the smart home industry should develop an ethical code of conduct with honesty, respect, and privacy as the core values. These values should be reflected in any data protection practices, project goals, and product features. Framing this ethical code of conduct would also be very useful for designers during all phases of UX design (e.g., research, analysis, design and testing). Similarly, it would be useful for business leaders making executive or strategic decisions.

Moreover, in Chapter 6, we demonstrate that some UX principles, such as heuristics are helpful in facilitating co-design workshops and to elicit perspectives from users, designers, business leaders and using those to improve design more broadly of data protection. In addition, our designer interviews in Chapter 5 demonstrated that UX designers experienced challenges in finding the right balance between user needs and business goals. Limited resources and competing objectives in organizations were previously reported by Becker et al. [337, 338, 472–474]. UX designers act as the user’s advocate in the design space. As a result, while they have to fulfill the business objectives, they are also empowered to maximize user needs (e.g., respect, satisfaction, positive ethical engagement), and act as a focal point for interventions in this space. UX designers often come across tight deadlines and limited resources to complete projects. They are sometimes pressured to design interactions that are not compliant with their own values or practices. Having a clearly framed ethical code of conduct can liberate UX designers to challenge situations where business imperatives are unfairly disadvantageous to the user’s best interests. We argue that UX designers are key to building a trusting relationship with users: they are able to reflect ethical and honest user values that are consistent with business goals and requirements.

Just like business leaders, designers need tools and support to help navigate data protection requirements. For instance, in Chapter 5, D01 and D02 hoped for more concrete UX guidelines for addressing GDPR requirements. Business lead B02 expressed the need to make GDPR easier for designers: “*We also need to make it easier for designers and developers to really implement the provisions of GDPR within software, rather than just making it a tick box exercise.*” Tools and solutions could be in the form of best practices, common APIs, third party



solutions, visualizations and automation tools. Such tools should allow designers the means to respect the ethical dimensions of data protection and value exchange perspectives. For instance, our results showed that users favored automated data subject access experiences. UX-friendly tools that are able to guarantee repeatable, scalable (to small businesses), secure, and positive UX data access interactions, are likely to be helpful for UX designers.

Rapid product life cycles in smart home products create challenges for designers – especially when navigating data protection requirements. UX designers have to balance user and business needs, and design data protection solutions in an iterative rapid development process. More tools and guidelines should be developed to assist UX designers to comply with data protection regulation in ways that enhance the user experience and facilitate ethical business practices.

Finally, users expressed a preference for automation as it allowed them to easily exercise their data protection rights. Automation is also likely to reduce data protection costs for business leaders, and help address some challenges of data protection regulation. A report by McKinsey Company stated that automated data protection solutions would result in reduced costs in the long run [475]. As such, we argue that automation should be further explored as it is easier for users, a market differentiator for business leaders. Future work should also explore how to provide users more agency over their data protection rights.

At the current moment, it is difficult to distinguish companies that have effective (e.g., ethical, useful) data protection practices from those that merely claim to. Moreover, given the desire to rely on third parties for data protection, there is a question mark over whether a subcontracted interaction that seems unethical to a user (e.g., a dark pattern) is perceived as an indication of unethical data protection practices in the original company. As a result of the difficulty in identifying truly effective (e.g., ethical, useful, practice) data protection practices, there is a disincentive for companies to embrace these without further ways of signaling their authenticity.

We suggest that a voluntary code of practice for data protection could be developed. For instance, data protection organizations could provide certification schemes or indicators which can demonstrate that companies are behaving reasonably (e.g. ethically) with consumer privacy and regulatory needs. Such schemes would be more challenging in smart home contexts due to the various sectors of ecosystems, suppliers, manufacturers, and third parties. However, they would improve practices of transparency, freedom of information, and honesty in smart home companies. Moreover, certification schemes may have limitations and drawbacks. For instance,

some argue that companies are unlikely to participate in certification schemes due to the lack of details in existing schemes<sup>2</sup> (e.g., obligations, potential sanctions).

Moreover, such code of practice could help to address the issues arising where companies are in a conflict between the best interests of users and the best interests of the business. Having well-founded trust in data protection practices is necessary to ensure that users engage and businesses thrive, and having a code of practice which enshrines the importance of ethical behavior could provide a foundation from which data protection professionals would serve as guarantors of honest data protection practices – much in the same way that chartered professionals are trusted to deliver competence and ethical standards.

## 7.3 Innovation

Our thesis confirms that understanding innovation in a design space is really important: users, designers and business leaders can be innovative in the design of security, privacy and data protection, which can have an effect on the design of systems.

### 7.3.1 Implications of Innovative Repurposing

In this thesis, our results showed that users are willing to innovate when using smart home products, in cases such as repurposing smart home products. For example, in Chapter 4, we show that smart home products were repurposed in five households. Smart home cameras that were originally intended to protect the household from burglary and vandalism were repurposed for parenting and entertainment. Conversely, smart lights that were originally intended for lighting control were used as a deterrent against burglary (e.g., making the house appear to be occupied while inhabitants were away).

Smart lights have been previously susceptible to numerous attacks. For instance, a security attack was able to remotely leak data from smart lights from a distance of 100 meters using cheap and readily available equipment [476]. In contrast, the intrusive nature of smart cameras can make them susceptible to misuse and even abuse. Researchers have argued that smart home cameras can be exploited and facilitate domestic abuse by controlling and monitoring victims [262, 477]. In response to these on-going threats, smart home manufacturers (e.g., Google) have introduced large counter-abuse teams. Those teams are often reactive, relying largely on users to report misbehavior [478]. Given the diversity, immaturity, complexity of

---

<sup>2</sup><https://www.pinsentmasons.com/out-law/analysis/more-detail-on-workings-of-gdpr-certification-schemes-necessary-to-prompt-business-take-up-says-expert>

smart homes and the inconsistencies surrounding security and privacy experiences, we argue that a more proactive approach is also needed.

Designers should improve their understanding of audiences and contextual uses of smart home products to be able to ground and anticipate how their technologies might be repurposed. This would allow them to accommodate for the additional uses and negative consequences of smart home technologies. Designers should be aware of potential imbalances, interests, and tensions among co-cohabitants which might cause conflict (e.g., conflicts between parent and child or arising from an abusive partner).

In a typical household, smart home administration models provide total control and agency to individual users (e.g., often the ones who set up these devices) over other users. As a result, a power imbalance between users can be exploited which can curtail both the visibility of misuse and the opportunities for remedial action. This model of control may not be best suited to the home, and alternatives may prove to be fruitful areas of investigation. For example, some features of smart home products might be protected through a dual control process, which would require two users to cooperate in order to gain authorized access to a smart home product. These would require the cooperation of two individuals in the household and provide an impediment to a single individual misusing their access; however this comes at the cost of convenience and would only be suitable for infrequent and high-value access.

### 7.3.2 Privacy vs Security Innovation

In Chapter 5, we observed novel issues that are related to smart home security and privacy, which pointed to significant challenges where innovative solutions are necessary. Despite recognizing the importance of security in the design process, our results show design and security teams are less innovative due to existing practices and perceptions. These practices include favoring tried-and-tested security solutions or procuring security solutions from reputable vendors. This finding highlights a desire to avoid novelty and a preference to ‘*follow the crowd*’ in the design of security.

Further, the perception of security as only a technical problem, for which there are ‘*best-practice*’ technical solutions, limits design considerations for security solutions (e.g., authentication consisting of only username and password combinations). Many smart home devices are designed for operating in privacy-sensitive environments (e.g., personal spaces). Given the relative immaturity of the smart home device space, tried-and-tested solutions are not particularly suitable, and innovative solutions are required. For example, current designs do not accommodate the diversity of social aspects of smart home security and privacy (e.g., the nuance between

a device being in a shared space in a flat-share vs. being in a shared space in a single-family household).

While we found no evidence of innovation in security design, our results show that efforts have been made to innovate in the privacy space. For instance, company B created a geographic location privacy feature which could detect human activity and make their doorbell less intrusive. One reason for this was that companies wanted to preserve their trust relationship with their customers, and privacy failures were seen as potentially ‘*creepy*’ and ‘*intrusive*’, which would undermine this relationship.

### 7.3.3 Identifying Innovation Gaps for Business Leaders

Our results show that business leaders working in SMEs (small and medium-sized enterprises) desire for more innovation in smart home environments. In Chapter 5, we show that business leaders who worked in SMEs lacked resources (e.g., time, money, staff) to develop solutions that bigger companies had in-house capabilities to develop. We argue that innovation for business leaders is about identifying the gaps that are not filled at all, rather than those barely being filled.

Furthermore, our results have highlighted that smaller businesses are keen to outsource as a means of complying with data protection regulation. As a result, discount data protection should also be aiming to be consistent with third party services and offerings. Such solutions can potentially reduce overheads (e.g., costs of tooling, training, hiring, etc.), provide industry standard solutions to common data protection needs, or be embedded and provide added value to other services.

### 7.3.4 Responsible Innovation in the Design of Security and Privacy

Responsible innovation refers to a responsible approach towards innovation that involves taking into account the effects and potential impacts of innovation on the environment and society [479–482]. The European project RRI Tools defines Responsible Innovation [483] as:

“a dynamic, iterative process in which all stakeholders in research and innovation become mutually responsive and share responsibility for both the process and its outcomes.”

Our results in Chapter 4, 5 and 6 show that *responsibility* is a strong theme that cross-cut all chapters, hence creating considerable societal (e.g., health, demographic change and wellbeing) and ethical challenges of smart home products. Among these

challenges is the growth of these products in complexity, scale and power and their potential to put the security, privacy and well-being of users, households, and bystanders at serious risk.

We argue that responsible innovation is the next crucial wave of design thinking that is able to address these challenges. Responsible innovation is inherent in the design space, in particular under the design heuristics we have developed for smart home products. Our results in Chapter 4 and 5 show that responsible innovation is implicitly tied to our findings through the lifecycle of consent, interactions surrounding smart home security and privacy, and the lifecycle of technology repurposing. Similarly, our Framework of Design Heuristics in Section 6.3.1 shows that responsible innovation is implicitly tied to our design heuristics. The user-centricity of the heuristics enabled designers to better understand the context and the values of the users as well as their needs and limitations. As a result, they helped tackle responsibility in innovation and promote responsible thinking. For example, many of our heuristics for consent and communication are focused on improving the UX of smart home products, making them more user-centric, which is inherently more value sensitive, hence leading to more responsibility (e.g., consider how users interact with personal data that is specific to only one user). Furthermore, our Framework of Design Heuristics also showed that heuristics helped designers act more responsibly in tackling security, privacy and ethical challenges (e.g., UX designers in the workshop considered ethical and human right issues to design panic features). Explicitly taking user values into account and designing for them would achieve responsible behavior and responsible decisions from all stakeholders. This is evidenced in Chapter 5 where user experience is regarded as a shared responsibility among all stakeholders (e.g., users, designers and business leaders) who contribute to the development of a smart home product.

Since UX is useful for tackling user-centricity of smart home products, our research tackled two aspects of responsible innovation: the ethical and social implications. It also tackled the legal aspects of responsible innovation through data protection regulation. However, it did not tackle environmental aspects due to being out of scope of the primary thesis which is exploring user experience design. Future work addressing responsible innovation of smart home design should strongly consider their environmental impacts. Some of our designer interviewees strongly recognized the importance of environmental impacts in smart home design. For example, UX Designer D03 in Chapter 5 noted that some smart home products have to be physically disposed to prevent data leakage, which is harmful for the environment. They explained: *“There are some security aspects that we have: the devices are*

*disposable, they're not re-manufactured. It's not as nice for the environment as it could be, but it does ensure the old data doesn't leak out in some recycling scenario."* Future research could explore how data security and privacy practices of smart homes could be less harmful for the environment while achieving their function.

In addition, more work needs to be done to identify and explore responsible perspectives from our framework of design heuristics. In particular, future work should explore in more detail how to (i) identify more heuristics that tie to responsibility and (ii) identify existing heuristics for which there is a responsibility perspective. For instance, future work can categorize heuristics that seem to tie to responsibility from those that do not at all. In addition, future work can explore what constitutes a responsible design recommendation and develop frameworks or methods that can evaluate design recommendations for their responsibility.

Moreover, to facilitate the process of responsible innovation, we argue that smart home designers, researchers, business leaders, regulators and decision makers should continuously exercise the moral imagination to consider the socio-technical implications of smart home technologies. Since moral imagination takes time to build, we propose that designers, business leaders and companies should invest in developing tools, framework and methods that can facilitate moral imagination. For example, researchers at Microsoft have introduced a Responsible Innovation Practices Toolkit to help facilitate responsible innovation practices [484]. While these are not guaranteed to address all the challenges, they represent a good direction towards designing responsible smart home technologies with better intention.

*“It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it.”*

— Stephane Nappo

# 8

## Conclusion

The allure of the smart home is powerful: simple voice commands can raise window shades, change home temperatures, and turn on the coffee maker. Smart homes can save time, increase personal productivity, and provide a level of convenience for households. And yet the convenience comes at a cost: more data pertaining to private home spaces is created, processed, and shared outside the home [216].

In order to devise more appropriate and effective security, privacy and data protection solutions, we believe that these solutions should be designed with UX design principles from the ground. The UX of security, privacy and data protection is a designed encounter which encompasses contextual, economic, compliance and strategic business priorities [420, 421, 485]. The research reported in this dissertation took a step in that direction.

The research question addressed in this dissertation was: *How can UX design principles be well supported and understood to inform security and privacy design in the smart home?* The question was broken down into the following research questions:

- What is the relationship between UX, security, and privacy in the smart home?
- What is the role of UX in the design of security, privacy and data protection in smart home products?
- How can UX design be incorporated into the design of security and privacy of smart home devices?

To address our research questions, first, we explored how does UX relate to security, privacy and smart homes (see Chapter 4), second, we explored the role

of UX in the design of security and privacy in smart homes from designer and business leader perspectives (see Chapter 5), and third, we proposed and evaluated a framework of design heuristics for consent and permission (see Chapter 6).

## 8.1 Key Findings

This thesis aimed to research UX design principles and factors in order to inform and inspire the design of security and privacy in smart home devices. Through our identified research questions, we derived the following key findings:

### 8.1.1 UX can Deepen Understanding of Consent Relationships

In this thesis, we showed that consent is conceptualized as a relationship, where UX is part of the way in which people interact with security and privacy features. We listed different scenarios in which consent relationships are formed, illustrated how the life cycle of consent can change over time. We also demonstrated that consent can be an unpleasant experience, particularly in cases where users are experiencing dark patterns. Finally, we showed that consent management is perceived to be highly unforgiving and not a safe space in which to make mistakes.

### 8.1.2 Innovation in the UX Design of Security, Privacy and Data Protection

In this thesis, we also showed that users, designers and business leaders can be innovative in the UX design of security, privacy and data protection. Users are willing to innovate when using smart home products such as repurposing smart home products. Moreover, security design teams are less innovative due to existing practices and perceptions (e.g., favoring tried-and-tested security solutions), but privacy design teams have tended to be more innovative. Also, business leaders working in SMEs desire for more innovative solutions in data protection in order to address the challenges they are experiencing. Finally, we showed that responsible innovation is a critical part of the future of smart home design, and we pointed out how it can help deal with societal and ethical aspects of responsible innovation.



### 8.1.3 UX Design can Help Security and Privacy Practitioners

In this thesis, we also demonstrated that users perceived some smart home interactions to be dishonest, forced, persuasive and lacking transparency. On further investigation, we found some situations where these unfriendly interactions arose due a mismatch between customer priorities and business realities. We also showed that some smart home manufacturers fail to comply with data protection regulation due to lacking resources such as time and labor, and experiencing an unrecognized cost of compliance. In those specific cases, we illustrated how UX and heuristics can help with data protection interaction design through discount practices, a collection of techniques and practices aimed at pragmatic, low effort, cost-effective solutions. Finally, we showed that heuristics can help in three areas: (i) improved user-centricity (more satisfied users), (ii) supporting data protection practices and (iii) helping with responsibility and responsible innovation.

## 8.2 Critical Review

We identify areas of weaknesses and limitations (e.g., flaws or shortcomings) of the research presented in this thesis. We list eight major limitations below:

First, we have selected smart home participants in this thesis who clearly chose to use and adopt smart home products. Deliberate users of smart home devices are not representatives of all users. Non-users and bystanders of smart home products are likely to have different views, experiences and perceptions over the use of smart home products. Furthermore, it is possible that users with security and privacy concerns elect not to use smart home products. Future work should explore the concerns of bystanders and non-users of smart home devices.

Second, security, privacy and data protection are sensitive issues for designers and business leaders (especially participants working in big organizations). Our participants' corporate responsibilities as well as their company's reputation might have biased their responses. To mitigate this, we briefed our participants about our security and privacy measures, focusing on how we will encrypt their data and process it in accordance with the General Data Protection Regulation (GDPR). We provide more details over how we addressed these limitations in Section 4.2.2.5 and Section 5.2.2.6.

Third, in Chapter 4, we performed a secondary data analysis of a dataset that was collected as part of a large study. A major limitation in secondary analyses is that the data used was not collected to address our research questions

[367, 369]. To address this limitation, we followed a process of careful reflective examination and critical evaluation of the data to ensure a match between our research questions and the existing data. We provide more details over how we addressed this limitation in Section 4.2.2.5.

Fourth, self-reporting bias is common in user (e.g., interview) studies [391]. Some participants in Chapter 4, 5 and 6 might not have responded accurately to our questions because they did not remember specific details or wanted to be viewed as socially acceptable. Other participants could have been concerned about the interviewer's perception of them and, therefore could have changed their answers in line with how they like to be perceived. For instance, social factors such as ethnicity may influence the answers that different social groups are willing to give [418]. To maximize validity and minimize self-reporting bias, we avoided leading questions and relied on open-ended questions, inviting participants to provide in-depth answers in their own words. We provide more details over how we addressed self-reporting bias limitations in Section 5.1.2.5 and Section 5.2.2.6.

Fifth, our qualitative studies reported in Chapter 4, 5 and 6 are limited by the size and diversity of our sample. For instance, finding designers and business leaders willing to share their experiences in security, privacy and data protection (e.g., GDPR) is challenging due to legal matters being sensitive and confidential. As a result, despite numerous efforts, we were unable to recruit any business leaders from large companies in this thesis. As such, our qualitative work is limited by the size and diversity of our sample. Following recommendations from prior work to interview between 12 and 20 participants [392], we interviewed 20 participants until new codes stopped emerging. We provide more details over how we addressed these limitations in Section 5.1.2.5 and Section 5.2.2.6 and Section 6.2.5.

Sixth, research quality depends on the thesis author's individual skills and might be influenced by their personal biases. Inexperienced interviewers may not be able to ask prompt questions or probe into situations that would result in missing gathering relevant data [415]. For instance, the depth of data collected is dependent on the interviewer's skill [416] and the quality of the questions asked [417]. To address this limitation, one researcher, who was trained to conduct the interviews consistently and ask questions in an open and neutral way in order not to influence participants, conducted all studies in this thesis. We provided more details over how we addressed this limitation in Section 5.2.2.6.

Seventh, we note that our thesis is purely of qualitative nature. We do not attempt to quantify our findings or draw conclusions or generalizable findings about a larger or a wider population of users, business leaders and designers. The focus

of our qualitative work is about the richness of understanding rather than the generalizability to a population. Since our thesis methodology was qualitative and exploratory in nature, the hypotheses we formulated based on our findings, emerging themes and discussion coming from the grounded-theoretic analyses in Chapter 4, 5 and 6, would need to be tested in a follow-up confirmatory study to assess their broader applicability and generalizability. We provided more details over how we addressed this limitation in Section 5.2.2.6.

Eighth, we couldn't evaluate whether the description of lifecycle and reuse of our framework were particularly helpful because our workshops were articulated around heuristics. To address this limitation, we performed a detailed evaluation of the heuristics which allowed us to give recommendations for future design improvements. We described how we addressed this limitation in more detail in Section 6.2.5.

## 8.3 Directions For Future Work

Our research key findings motivate research areas that are ripe for future evaluation and investigation. We outline these areas below:

### 8.3.1 Understanding the Effectiveness of Privacy Controls

Our results in Chapter 4 showed that the ability to give users full control over their personal information is crucial to providing assurance: tangible privacy controls (e.g., physically taping a camera) provided more assurance than other more abstract controls (e.g., data use policies). Visual cues have historically provided privacy assurance to web users [466], however more research is needed to understand whether this is applicable, and more fundamentally how effectiveness of privacy controls is perceived in smart products.

### 8.3.2 Forecasting the Consequences of Technology Repurposing

Our results in Chapter 4 showed that technology repurposing can bring benefits, but can also introduce new security and privacy threats. Our results highlight the role of responsible innovation which has been discussed in Section 7.3.4. Designers and researchers should develop knowledge of the risks and threats of repurposing and improve the transparency of sensitive features (e.g., cameras). Users should be able to easily find accessible usage logs and should be reminded (e.g., notifications, visual indicators) when sensitive features are enabled.

### 8.3.3 Making Consent Choices More Forgiving

Our results in Chapter 4 showed that the design of consent needs to consider the experience of changes over time (e.g., granting, revoking and amending consent). More research should explore the experience of withholding consent, and how the experience of making mistakes can be made more forgiving.

### 8.3.4 Innovating without Hindering Security

Our results in Chapter 5 demonstrated that tried-and-tested solutions were highly demanded in companies A, B, and C which preferred reliability and assurance (e.g., reusing best-security practices). Those practices were shown to hinder innovation; however, we believe more research is needed to explore the relationship between UX, innovation, and security. A key issue to uncover would incite us to wonder what aspects of security design can be safely innovated, and how UX can be used to design more effective security experiences?

### 8.3.5 Creating UX-aware Data Protection Guidelines

Our results in Chapter 5 showed that data protection regulations (e.g., GDPR) influenced the design phase. Our participants reported that GDPR touched on facets of product design but often failed to translate into specific requirements, which caused disparities in the design process. While GDPR requires practitioners to factor security and privacy into the design process, it can bring more confusion to the design table: regulatory requirements have been reported to be high-level and impractical [486]. New techniques and tools are needed to address how data protection regulations and practices can factor the application of UX design principles.

### 8.3.6 Improving Communication Among Different Stakeholders

Our results in Chapter 5 show poor communication among multi-stakeholder teams where security design happens. In the absence of regular communication among stakeholders, the number of implicit assumptions made increases (e.g., in our study, Product Manager A1 selecting security features based on their own knowledge of common practices) [487]. Similarly, tensions among stakeholders also increase. For example, in Company B, UX Designer B11 was frustrated that they could not make UX-aware decisions. Expecting largely autonomous groups of stakeholders (e.g.,

security, legal, design, UX) with different goals, motivations, and constraints to speak the same language is unrealistic. Therefore, more research into this area should explore how to make different teams communicate effectively about factoring UX into the security and privacy design of smart home products.

### **8.3.7 Identifying Heuristics for Individuals**

Our results in Chapter 6 demonstrated the application of heuristics in focus group design setting; targeting teams and organizations, rather than individuals. Identifying a repertoire of heuristics on which individual experts can also rely, is crucial. Future work should explore how useful the heuristics are for individual experts through an expert-driven solitary design process.

# Appendices

*“People ignore design that ignores people.”*

— Frank Chimero



# Thesis Definitions

## **A.1 Definitions**

In this section, we provide definitions for key concepts that are the focus of this thesis. We provide a definition for UX, Security, Privacy, Design Process and Innovation.

### **A.1.1 User Experience**

User Experience (UX) has gained enormous traction in Human-Computer Interaction (HCI) over the past years which led to significant efforts that aim to provide a uniform definition of UX [488]. Although many researchers explore UX, its definition and characteristics are repeatedly debated [78]. As a result, there is no general agreement on what is the meaning of UX. Mäkelä and Fulton Suri [489] defined UX as the “result of motivated action in a certain context” which is broad. Hassenzahl and Tractinsky [16] provide a more appropriate definition of UX as “a consequence of a user’s internal state (e.g., predispositions, expectations, needs, motivation, mood, etc.), the characteristics of the designed system (e.g., complexity, purpose, usability, functionality, etc.) and the context (or the environment) in which the interaction occurs (e.g., organizational/social setting, meaningfulness of the activity, voluntariness of use, etc.)”. Nielsen-Norman Group offered a concise definition of UX [490]: “All aspects of the end-user’s interaction with the company, its services, and its products.” Finally, Alben [491]’s definition puts strong emphasis on feelings: “All the aspects of how people use an interactive product: the way it feels in their hands, how well they understand how it works, how they feel about it while

they're using it, how well it serves their purposes, and how well it fits into the entire context in which they are using it.”

In this thesis, we adopt the most widely accepted and referenced definition of UX which was proposed by the international standard of human-system interaction ISO 9241-210 [492]:

“a person’s perceptions and responses that result from the use or anticipated use of a product, system or service.”

This definition was chosen because it factors people’s emotions, preferences, behaviors, perceptions, beliefs, psychological responses, and accomplishments during service or product use. UX has three dimensions: user, system, and context [80]. Each dimension of UX is accompanied with sub-dimensions [493]. The sub-dimensions of the *user* dimension are: ‘affect’, emotion, feelings and psychological needs. Hedonic and pragmatic (e.g., usability and utility) product quality are the sub-dimensions of the *system* dimension. Time and situatedness are the sub-dimensions of the *context* dimension.

### A.1.2 Security

There is a lack of a concise or broadly acceptable definition of security. Existing definitions have been variable, subjective, and sometimes, uninformative. An early definition of security can be tracked to the Committee on National Security System [494] definition in 2003: “the ability to protect or defend the use of cyberspace from cyber-attacks.” However, Public Safety Canada proposed a more informative definition [495]: “The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.” Some experts provide political definitions of security such as Canongia & Mandarino [496]: “The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure.” An accepted definition of security is provided by Oxford Dictionaries [497]: “The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.” However, it is not too detailed for the context of this thesis. A well-known definition is provided by the US Department of Homeland Security (DHS) [498]: “The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”

In this thesis, we adopt Craigen’s definition of security due to its considerations for security’s multidimensionality [499]:



“the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.”

This definition highlights three important factors in security (i) its multidisciplinary socio-technical nature, (ii) its scale-free network, and (iii) its high degrees of change, speed and connectivity. The definition also factors the three well-known *security mechanisms*: (i) confidentiality, (ii) integrity, and (iii) availability [500]. The rating methodology, OWASP RRM, adds (iv) accountability [501].

### A.1.3 Privacy

Privacy is a human right that had historically motivated security and privacy researchers to research techniques to protect it. Being strongly related to information technology (IT), privacy is a broad term with meanings rooted in larger cultural practices and understandings in law, ethics, and social theory. In 1890, privacy was defined by Brandeis and Warren as the “right to be let alone” with a detailed analysis of the meaning of being “let alone” [502]. A more comprehensive definition of privacy appeared in 1880 by Godkin as “the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion” [502, 503]. Richard Posner defined privacy as the right to have secrecy: “conceal information about themselves that others might use to their disadvantage” [502, 504]. Privacy is sometimes defined as controlling over one’s personal data: “privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” [502, 505] For some, privacy is defined and composed through different states. Westin defined privacy as being composed of four states: reserve, intimacy, anonymity, and solitude. [505]. Rouse [506] defines privacy as “the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.” Privacy factors (i) data collection and distribution, (ii) technology, (iii) user expectations, and (iv) regulatory issues [507]. Privacy is also referred to as information or data privacy, [233] and sometimes data protection [109].

### A.1.4 Smart Home

The first smart home definition [508] was proposed 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, home intelligence is not factored in this definition; Berlo [509]’s definition adds home intelligence: “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 define smart homes as a group of products and skills based on networks in the home [510]. But, the definition is too broad.

Intertek’s smart home project provided a more detailed interpretation in 2003 [511]: “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 [512] provides even a more comprehensive definition: “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.” There is agreement that smart homes are the application of ubiquitous or pervasive computing or environments. However, as described in this section, there is no agreement on the definition of smart homes. In this thesis, we use Alam’s [513] definition:

“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.”

According to Aldrish [514], smart homes respond to households’ needs to ensure their safety, privacy and peace of mind. Smart homes also are known as intelligent houses, home automation, and aware houses [513].

### A.1.5 Product Design

Product design also does not have a widely accepted definition. Luchs and Swan [515] propose two discrete, yet interdependent, definitions: “product design” and “product design process”. For the purpose of this thesis, we will use Luchs and Swan [515]’s definitions:

“the set of properties of an artifact, consisting of the discrete properties 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.”

To complement the previous definition, Luchs and Swan [515] define “product design process”:

“the set of strategic and tactical activities, from idea generation to commercialization, used to create a product design.”

### **A.1.6 Innovation**

Innovation means “a new idea, creative thoughts, new imaginations in form of device or method” [516]. Innovation is seen as building solutions to address novel challenges and market needs that are not coherently expressed [517]. In this thesis, we adopt Crossan and Apaydin’s definition [518] of innovation:

“Innovation is the production or adoption, assimilation, and exploitation of a value-added novelty in economic and social spheres; renewal and enlargement of products, services, and markets; development of new methods of production; and the establishment of new management systems. It is both a process and an outcome.”

We chose this definition because it encompasses the delivery of effective products. Successful innovations provide effective and novel solutions, which “break into” markets and societies [519].

# B

## Chapter 4 Supplementary Material

We present in this appendix supplementary material relating to Chapter 4.

### **B.1 Study One**

#### **B.1.1 Interview Questions**

##### **B.1.1.1 Characterizations**

- Can you tell us a bit about yourself?
- Which smart speaker do you use? Why did you choose it?
- Where is your smart speaker placed? Why did you place it there?
- Are you the sole user of the smart speaker or is it used with others?

##### **B.1.1.2 General Perceptions**

- What made you decide to get smart speakers? Did you consider any features or characteristics?
- And why did you decide to choose this particular model?
- Did you purchase the smart speaker? If not, how did you acquire it?
- Do you think you'll use your smart speaker in the next year?

##### **B.1.1.3 Interactions with Device**

- How would you describe your experience with smart speakers in general?
- What do you use smart speakers for? What about the other uses?
- Do you think smart speakers save time for you?

- Do you have any ‘apps’ or ‘skills’ with your smart speaker?
- Are you using your smart speaker for any automations?
- Do you have any concerns or worries when you are using your smart speaker?
- Has the device ever made you uncomfortable? How did you deal with the situation?

#### **B.1.1.4 Sharing with Others**

- How many people live in your home? Does everyone get equal access around the smart speaker? Do they have their own profile or use yours?
- Have you had one instance where a house guest interacted with your smart speaker? On your profiles? How did you feel about it?

#### **B.1.1.5 Understanding Technology**

- Could you briefly explain your understanding of smart speaker technology?
- Can you describe how smart speakers are able to respond to your commands? How do you feel about the always-listening mode? Do you have any concerns?
- Do you sometimes mute your smart speakers? If so, how? Do you use any features in the device? How do you feel about them?
- Do you ever manage your voice command activity? If so, how? Do you use any features in the device? How do you feel about them?

#### **B.1.1.6 Security and Privacy**

- Do you have any security or privacy concerns when using smart speakers? If so, can you provide more details?
- How do you feel about your personal data being handled by product manufacturers? Do you have any concerns?
- Do you feel that you have adequate security and privacy controls?
- Do you take any measures to protect your security or privacy?

#### **B.1.1.7 Concluding Interview**

- We have reached the end of this interview. Do you have any questions or comments?

## B.2 Study Two

### B.2.1 Recruitment Form

#### Household Information

Please provide information on all persons in your household

	pseudonym (nickname) <i>Optional</i>	age <i>Optional</i>	gender <i>Optional</i>	highest level of education <i>Optional</i>	skills with smart devices <i>Optional</i>	profe
person 1	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 2	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 3	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 4	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 5	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 6	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 7	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 8	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>
person 9	<input type="text"/>	Please select ▾	Please select ▾	Please select ▾	Please select ▾	<input type="text"/>

total household income \* Required

post code \* Required

### Internet-Connected Technology

Which internet-connected devices does your household own and who uses them? Think of your computers, smart phones, fitness trackers, TVs, Amazon Alexa, and so on \* Required

Do you intend to purchase any other devices in the near future? If so, which, why, and when? \* Required

Have you heard of any other internet-connected (smart) devices that you thought were interesting? \* Required

**Administrative**

Do you have any travel longer than 2 weeks planned (including all your household)? \* *Required*

Why would you like to participate in this study? \* *Required*



Final page

Thank you for filling in the survey. We will be in touch within two weeks.

---

### Key for selection options

**4.1.b - age**

<18  
18-34  
35-64  
65+

**4.1.c - gender**

male  
female  
prefer not to disclose

**4.1.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.1.e - skills with smart devices**

novice  
competent  
expert

**4.2.b - age**

<18  
18-34  
35-64  
65+

**4.2.c - gender**

male  
female  
prefer not to disclose

**4.2.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.2.e - skills with smart devices**

novice  
competent  
expert

**4.3.b - age**

<18  
18-34  
35-64

65+

**4.3.c - gender**

male  
female  
prefer not to disclose

**4.3.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.3.e - skills with smart devices**

novice  
competent  
expert

**4.4.b - age**

<18  
18-34  
35-64  
65+

**4.4.c - gender**

male  
female  
prefer not to disclose

**4.4.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.4.e - skills with smart devices**

novice  
competent  
expert

**4.5.b - age**

<18  
18-34  
35-64  
65+

**4.5.c - gender**

male  
female  
prefer not to disclose

**4.5.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training

Undergraduate studies  
Postgraduate studies

**4.5.e - skills with smart devices**

novice  
competent  
expert

**4.6.b - age**

<18  
18-34  
35-64  
65+

**4.6.c - gender**

male  
female  
prefer not to disclose

**4.6.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.6.e - skills with smart devices**

novice  
competent  
expert

**4.7.b - age**

<18  
18-34  
35-64  
65+

**4.7.c - gender**

male  
female  
prefer not to disclose

**4.7.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.7.e - skills with smart devices**

novice  
competent  
expert

**4.8.b - age**

<18  
18-34  
35-64

65+

**4.8.c - gender**

male  
female  
prefer not to disclose

**4.8.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.8.e - skills with smart devices**

novice  
competent  
expert

**4.9.b - age**

<18  
18-34  
35-64  
65+

**4.9.c - gender**

male  
female  
prefer not to disclose

**4.9.d - highest level of education**

no school completed  
Nursery  
High School  
Trade/technical/vocational training  
Undergraduate studies  
Postgraduate studies

**4.9.e - skills with smart devices**

novice  
competent  
expert

**5 - total household income**

less than £10,000  
£10,001 – £20,000  
£20,001 – £30,000  
£30,001 – £40,000  
£40,001 – £50,000  
£50,001 – £60,000  
£60,001 – £70,000  
£70,001 – £80,000  
£80,001 – £90,000  
£90,001 – £100,000  
£100,001 – £150,000  
more than £150,000

---

### B.2.2 Diary Template

This is your personal study diary, and you are invited to write down thoughts and notes related to the study as you please.

We encourage you to tell your diary (and thereby us) about your **experiences with using internet connected technology** in your home.

We ask you to fill in the **following template** using one of the free pages in this notebook **twice a week**.

#### **My experience**

When?	Day, time of the day
Where?	Which room
Goal?	What were you doing/ aiming to do, e.g. relax, do homework...
With whom?	Were you doing it alone or was someone else doing this with you?
Others?	Were other people around? What did they want to do?
Device?	Which devices (computer, phone, TV) did you use?
Discussion/Conversation?	Was there a conversation around using the device?
Positives/negatives?	Anything you particularly liked about the situation (with regards to use of the device)? Anything that you didn't like about it?

Answer the questions above on an empty page in this notebook. Provide information as you see fit. Don't provide anything you are not comfortable with sharing.

Figure B.1: Diary Template

### B.2.3 Deployment Picture and Notes

## Deployment Pictures and Notes

Taking pictures of the devices was entirely voluntary and optional. Hence, we only have picture of some devices in some households.

### Household 1

Household 1 installed their smart security cameras outside the building, overlooking their own property and the public foot path / school path in front of their house. The household also received an Amazon Alexa which was placed in the kitchen and used by all household members; the teenage daughter exclusively used an Amazon Echo Dot in her room.

Figure 1: All smart security cameras were positioned outside the house



### Household 2

One Google Home Mini was placed in the living room, and another Home Mini was placed in the parents' bedroom. A Home Hub was used in the kitchen. Only the device in the kitchen was used on a regular basis, and the two Home Minis remained frequently unplugged for several days. An Arlo Smart Doorbell and a security camera overlooking the front door approach were installed and configured for use by both adults.

### Household 3

At the beginning of the study, it became apparent that household 3 required a more recent smart phone to use any of the companion apps that came with smart home devices. Household 3 then chose a Hive Smart Thermostat that was installed professionally (the internet connection bridge was later unplugged) and a Google Home Hub Max. The household members decided later on to get a Google Home Mini and a Google Chromecast.

### Household 4

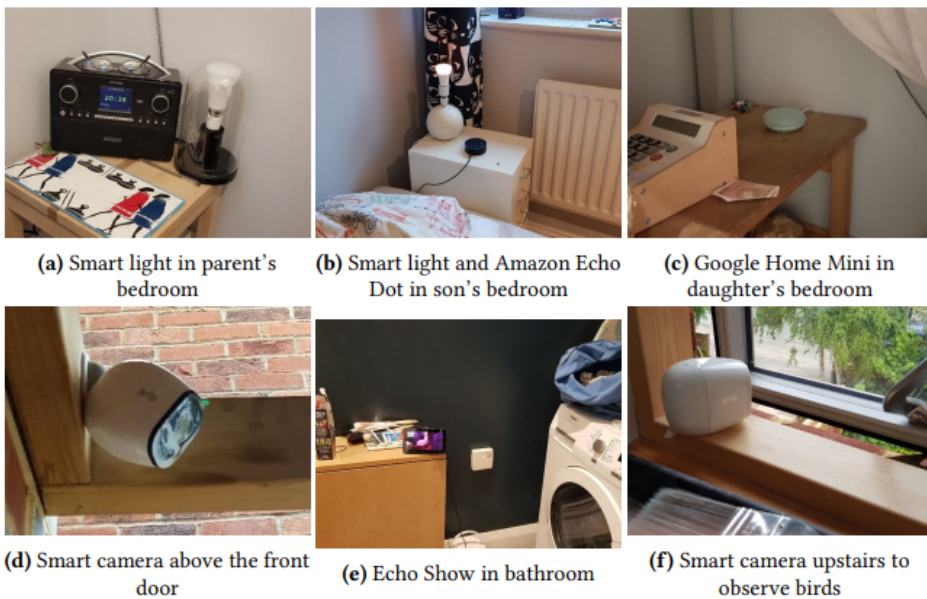
Household 4 chose a Google Home Mini for the daughter, an Echo Show for the living room which later was used in the bathroom, a smart camera with doorbell and chime for the front door to keep track of their son, and smart lights for their son.

Figure B.2: Deployment Notes (Part 1)

**Figure 2: Devices in Household 3**



**Figure 3: Pictures of deployed devices in Household 4**



### Household 6

The household members built their smart home system with Apple's Homekit as central control unit. Hence, they chose a new Apple TV, a bridge to their existing smart thermostat, a smart switch for a lighting system, and a set of lights for their landing. During the study, they purchased a ring doorbell off their own account.

**Figure B.3:** Deployment Notes (Part 2)

## B.2.4 Relation to previous work

**Table B.1:** Comparison of our major contribution with existing work

Finding	Comparison
The experience of consent management was uneven: consent to data collection was easy to grant, but difficult to withhold and revoke.	This is a novel finding and our research provides a rich ethnographic account of consent experiences. Other work [221, 225, 336] has explored, through surveys and a 1-week in-situ study (where participants wore a lifelogging device), the importance of consent and the modalities of consenting to data use in smart homes, however they have neither identified the disparity nor provided much information about the wider context of such consent experiences.
Smart home device use changed over time (for parenting and entertainment) which led to new security and privacy tensions from others both within and neighboring the home (e.g., intrusiveness, loss of control).	Prior work explores potential misuse [477, 478] of smart devices in the context of domestic abuse, more work [219, 230, 520] has identified that issues can arise from the imbalance between active and passive users (i.e., those that configure smart devices and those that do not). Our work provides examples and insights into how use changes over time and not just that it does. It aligns with the call for future work in Geeng and Roesner [230] to consider the concerns of children and passive users in smart homes, as well as how interactions change over longer periods of time.
Access control management was poorly suited to the needs of the households, and resulted in account sharing instead of permission delegation.	Smart home access control features have been reported to be poorly usable and inconsistent (e.g., [239, 262, 521, 522]). We corroborate earlier findings and provide additional detail pertaining to situations where access control does not fit the needs of the user (e.g., multiple accounts in smart speakers are too difficult to use). We also expand on this area by exploring access control experiences resulting from prolonged use of an ecosystem of more and less invasive commercial devices.
Participants exercised control over their private data through both designed controls and workarounds (e.g., physical taping a camera). However, security behavior involved only designed controls use.	Previous work has widely reported how smart home users control their personal information (e.g., [221, 223, 336, 523, 524]). Our research uses longitudinal data to study unsolicited security and privacy behaviors over time. We corroborate earlier findings and note that behavior observed over shorter periods of time is consistent with behaviors over longer periods of time. We also identify that home users commonly augment their use of designed controls with workarounds to protect their privacy (e.g., taping cameras, unplugging or moving devices), however they do not do this to protect their security and rely only on the designed controls.
Privacy and security concerns arose from media and online sources. While privacy concerns also arose from device use, security concerns did not.	Previous work widely reported smart home security and privacy concerns in smart homes (e.g., [215, 219, 222, 263, 377, 525, 526]). We corroborate earlier findings and expand them by providing a richer account of unsolicited privacy and security concerns and where they originate from. We confirm earlier findings that security and privacy concerns arise from online and media sources, however we make the novel observation that using devices led to new privacy concerns but not to security concerns.



# C

## Chapter 5 Supplementary Material

We present in this appendix supplementary material relating to Chapter 5.

### C.1 Study One

#### C.1.1 Screening Questionnaire

1. Select your gender:
  - Male
  - Female
  - Other
  - Prefer not to answer
2. Select your age group:
  - 18-24
  - 25-34
  - 35-44
  - 45-54
  - 55-64
  - 65-74
  - 75 or older
  - Prefer not to answer
3. What best describes your job at the company?
  - UI Designer
  - UX Designer
  - UX Director

- Interaction Designer
  - Sales Manager
  - Software Developer
  - Security Officer
  - Legal Officer
  - Hardware Designer
  - Hardware Engineer
  - Product Manager
  - Other:
4. How long have you been working at your company?
- No Experience
  - Less than 1 year
  - More than 1 year and less than 3 years
  - More than 3 years and less than 5 years
  - More than 5 years and less than 7 years
  - More than 7 years
5. What best describes your company?
- Consultant Company
  - Product Company
  - Service Company
  - Platform Company
  - Other:
6. Select the smart-home product category (or categories) that your company deals with:
- Phone Systems
  - Smart Lights and Dimmers
  - Temperature and Climate Control Systems
  - Security Access Control Systems
  - Other:
7. Select the type of device(s) that your company deals with:
- Cameras
  - Door Locks
  - Home Theaters
  - Hubs

- Voice Assistants
  - Leak Detectors
  - Lights
  - Motion Sensors
  - Power Outlets and Switches
  - Smoke Detectors
  - Thermostats
  - Other:
8. How many employees does your company have?
- less than 25
  - 26-50
  - 51-100
  - 101-250
  - 251-500
  - 501-1000
  - More than 1000

### **C.1.2 Pilot Interview Questions**

1. What company do you work for? What does the company do? What is your role in the company?
2. Can you describe your product design process?
3. Do you consider UX when designing security and privacy solutions for your smart home products? If so, how?
4. What are the typical challenges that you face when designing smart home products? Are there any challenges specific to factoring UX into security and privacy design?
5. Is there anything in the design process that could help address user-centered security and privacy challenges in smart homes? If so, please elaborate.

### **C.1.3 Main Interview Questions**

Our interviews were semi-structured. We below describe our study script (divided into several sections). The last four sections describe specific questions that we asked to employees who had different responsibilities.

### **C.1.3.1 Characterizations**

1. Would you tell us about your role in the company that you work at?
  - (a) When did you join the company?
  - (b) What are your responsibilities?
  - (c) What is your specific role in the development or design process of smart home devices?
2. Would you tell us about the products that you develop?
  - (a) Is there a specific product that you focus on developing?
3. Would you tell us about your users (or customers)?
  - (a) How would you describe the typical customers that use your products?

### **C.1.3.2 Introductory Questions**

1. How would you describe User Experience (UX)?
  - (a) What UX characteristics do you regard as important?
  - (b) What do you think the role of security/privacy in UX is?
2. Do you think there is a relation between UX and security/privacy?
  - (a) (if yes) Could you describe this relation?
  - (b) (if no) Could you explain why not?

### **C.1.3.3 Requirements Gathering and Specification**

1. How do you identify or specify the requirements of a smart home camera before you design it?
  - (a) What kind of requirements do you consider?
  - (b) How do you prioritize requirements?
2. Do you handle any security/privacy requirements during the requirements gathering or specification process?
  - (a) (if yes) How do you handle these requirements?
  - (b) (if yes) Do you consider UX when addressing security or privacy requirements in the design process?
  - (c) (if no) What do you think of designers who do so?

### **C.1.3.4 UX Design Process**

1. Do you consider UX to be an important factor in the design process of smart home devices?
  - (a) Where in the design process do you apply UX techniques?
  - (b) Is there a specific UX team or role in a specific department?

- (c) How are decisions made when it comes to UX?
  - (d) Do you factor UX into the security and privacy design of smart home cameras? If so, could you give us more details?
2. Does security or privacy play a role in the UX development process that you take part of?
  - (a) (if yes) Could you explain the role?
  - (b) (if no) What type of effect would it have if it did?
3. Do you collect user data for UX development?
  - (a) (if yes) What type of user data do you collect? How do you collect it?
  - (b) (if yes) What sort of data-driven methods do you use?
  - (c) (if yes) Have you ever handled UX requirements within the context of security and privacy? Can you give us more details?
4. Do you have a UX requirements gathering process?
  - (a) (if yes) Could you give us more details?
5. What design processes—including methods, techniques (e.g., storyboards), and artifacts (e.g., personas)—do you use in the context of data protection?
6. Regardless of whether you have a UX requirements gathering process, what do you think the best design practices are (e.g., programming patterns, artifacts)?

#### **C.1.3.5 End-user Involvement**

1. Do you engage end-users in the development of smart camera products or features?
2. (if yes) How do you involve end-users in the design phase?
  - (a) To which extent do you involve end-users?
  - (b) Do you consider data security or user privacy during the process? Why/Why not?
  - (c) Does the type of product influence whether end-users can be involved? What about security or privacy risks?
3. (if no) What are your thoughts on involving end-users in the design of smart home cameras?

#### **C.1.3.6 Ecosystem Considerations**

1. Is your product part of an ecosystem of products used in smart home environments?
2. (if yes) Have you faced any obstacles when considering the ecosystem?
  - (a) (if yes) What were they? Could you describe the main obstacles? How did you deal with them?

3. (if security/privacy was mentioned) Can you describe how do you deal with security and privacy?
4. (if security/privacy was not mentioned) What do you think of the role of security and privacy in a smart home ecosystem?

#### **C.1.3.7 UX Challenges**

1. What were the UX challenges that you faced during the design of smart cameras?
  - (a) How did you overcome those challenges?
  - (b) Were there any challenges without any solutions in sight?
2. (if security/privacy was mentioned) Could you give us more details of the security or privacy challenges?
  - (a) How did you address those challenges?
3. (if security/privacy was not mentioned) Smart homes are associated with security/privacy threats. Have you ever experienced challenges specific to UX during the security/privacy design process of smart cameras?
  - (a) (if yes) Could you describe the challenges you faced, and how did you address them?
  - (b) (if no) What do you think of the role(s) of security/privacy and UX in smart home environments?

#### **C.1.3.8 Security Stakeholder Questions**

1. Can you tell us how security is taken into consideration at your company?
2. How do you ensure that your product is secure? Is there a process? How does it look like?
3. How do you identify security requirements?
4. Do you work/communicate with the design team? Do you get involved in the security and privacy design of smart cameras?
5. In general, who is responsible for designing the security/privacy features of smart cameras?
6. How do you update the firmware of smart cameras that you sell? Who is responsible for this task?
7. How often does security need to be maintained?
8. If a security breach happens in the physical products sold to clients, who will take responsibility?
9. If your company suffers from a data breach, how will you address this? Do you notify users?

10. How do you make sure that users who use your products are protected when it comes to breaches?

#### **C.1.3.9 Regulatory Stakeholder Questions**

1. Who deals with GDPR and Product Liability?
2. Do you deal with legislation?
3. How is data protection represented in your organization?
4. Do you interact with any regulatory bodies (e.g., ICO) when it comes to matters of data protection?
  - (a) (if yes) What are these matters?
  - (b) (if no) Do you think it would be useful to do so?

#### **C.1.3.10 Management Stakeholder Questions**

1. Are there any restrictions (e.g., , legal, security, privacy) that make it harder for you to use customer data for product design or making decisions?
2. What data protection roles/responsibilities are there for:
  - (a) Product management (and data management)?
  - (b) Product design and development?
  - (c) UX, usability, and experience-centered jobs?
  - (d) Marketing and sales?
3. What does privacy mean in terms of your products?
4. How do you design for data protection when devices are shared among multiple users?

#### **C.1.3.11 Concluding Remarks**

1. Do you think there is anything in the design/development process that makes it easier to address user-centered security and privacy challenges in cameras?
2. We have reached the end of the interview. Thank you for talking to us!
  - (a) Do you have any questions?
  - (b) Do you have any comments you want to add?

## C.1.4 Codebook

<b>Development</b>	Stakeholder Limitations	Internal Security Audits	Obtaining Consent
AB Testing	Stakeholder Responsibilities	Low-Priority Security	Opt-Out Services
Acceptability	Storyboarding	No One's Responsibility	Privacy by Design
Agile Development	Surveys	No Sight of Security Requirements	Privacy Mode
Agile Sprint Reviews	Technical Requirements	Reactive Security	Privacy Requirements
Agile User Stories	Tensions Between Stakeholders	Security by Design	Privacy Settings
Analyzing Requirements	The Complexity of Smart Home Devices	Security Maintenance	Privacy Threats
Company Policies	Time Constraints	Security Mode	Privacy Vulnerabilities
Conceptual Sketches	Usability Testing	Security not Factored into Design	Putting Users in Control
Conflicts Between Stakeholders	Usefulness	Security Practices	Security Management Frameworks
Convenience Aspects	User Cases	Security Requirements	Subjective Awareness of Privacy
Cost Constraints	User Frustration	Security Settings	Transparency
Design Process	User Integrity	Security Threats	UX in Privacy Requirements
Development Process	User Interviews	Security Vulnerabilities	UX of Consent
Development Teams	User Involvement in Design	Subjective Awareness of Security	UX of Privacy
Diffusion of Responsibilities	User Observation	Subjective Security Decisions	Withdrawing Consent
End-User Incompetence	User Personas	Technical-Only Security	<b>Innovation</b>
End-User Tests	User Research	Understanding User Behavior	Best Practices
Focus Group Interviews	User Respect	Usable Security	Common Practices
Functional Requirements	Utility	Usable Security Experts	Designing New Devices
GDPR Vagueness	UX Best Practices	UX in Security Requirements	Designing New Features
Hardware Design	UX Challenges	Vulnerability Reporting Programs	Designing New Solutions
Heterogeneous Devices	UX Departments	<b>Privacy</b>	Lack of Innovation
Indirect User Feedback	UX Design Process	Collecting/Processing Data (GDPR)	Novel Security Uncertainty
Industrial Design	UX Guidelines	Creepiness	Privacy Innovation
Interoperability	UX Pain Points	Creepiness-Convenience Trade-off	Security Innovation
Legal Compliance	UX Policies	Data Protection by Design	Security Uncertainty
Less Time for Hardware Design	UX Requirements Gathering	Data Protection Practices	Tried-And-Tested Security
No Flexibility to Upgrade Hardware	UX Research	Data Protection Requirements	<b>Trust</b>
Non-Functional Requirements	UX Roles	Data Protection Responsibilities	Culture of Trust
Not Enough Hardware Sprints	<b>Security</b>	Data Protection Roles	Data Breach Response Plan
Product Liabilities	Ad-hoc Security	End-User Compliance	Experience of Harm
Project Constraints	Afterthought Security	Explicit Consent	Incident Response Plan
Requirements Gathering	Awareness Based on Outside Sources	GDPR Consent	Increasing Trust
Requirements Specification	Awareness Based on Social Influences	GDPR Impracticality	Informing Users of Their Rights
Scope Constraints	Encryption Between Devices	GDPR Delayed Effect	Motivation for Privacy
Stakeholder Authority	Evidence-Based Security Decisions	Handling Sensitive Data	Motivation for Security
Stakeholder Characteristics	External Security Audits	Help Pages and FAQs	Motivation for Trust
Stakeholder Communication	Fit-and-Forget Security	Making Devices not Creepy	Preserving Trust
Stakeholder Knowledge	Incidents	No Sight of Privacy Requirements	Trust Relationship

Table C.1: Codebook (Grounded Theory) for Study 1.



## C.2 Study 2

### C.2.1 Main Interview Questions

#### C.2.1.1 Users

- Can you tell us about yourself?
- Can you describe the smart devices you own? How do you use them?
- Do you have any skills/apps/automations installed on your smart home products? If so, can you give more details?
- Have you ever had experiences (e.g., providing consent or exercising your online rights) with data protection or GDPR? Can you give more details?
- Have you ever consented to providing your data to a service provider? How was your experience? Did you experience any difficulties?
- Have you ever exercised your legal rights online (e.g., right to erasure)? How was your experience? Did you experience any difficulties?
- Can you describe which data you are providing to smart home companies?
- Can you describe your understanding of data sharing and use by smart home companies?
- Do you think you are receiving enough value/benefits from giving out your data to smart home companies?
- Do you trust the companies that collect and process your data? Why?

#### C.2.1.2 Designers

- Can you tell us about yourself at the company that you work for? Can you give us more details about your job?
- What kind of products does your company sell/manufacture? Which team are you part of?
- Can you describe your customer base or market?
- Can you tell us about the type of products that you design or develop?
- What are the most common challenges that you experience in your job? How do you address them?
- Have you ever designed or prototyped features for data protection or GDPR? How do you make data protection design decisions? Can you give more details?
- Can you tell us about your requirements gathering and specification process?
- How do you factor UX into your design process?
- What UX design methods and techniques do you use? Can you give more details?

- Do you face any challenges when dealing with the design of data protection regulation features? Can you give more details?

### **C.2.1.3 Business Leaders**

- Can you tell us about yourself and your company? Can you tell us more details about your executive role?
- Can you tell us what products you sell/manufacture?
- Can you describe your customer base or market? Which countries do you operate in?
- What are your business goals and objectives? Do you have any plans to expand?
- What business standards do you follow?
- Have you ever dealt with GDPR or any data protection regulation? Can you give us more details?
- Do you have a data protection strategy or program implemented? How was it derived? How is it enforced?
- How do you comply with data protection regulations? Can you give us more details?
- Do you use any third-party or outsourcing tools to comply with data protection regulations?
- Do you experience any difficulties, challenges, or limitations when complying with data protection regulations? How do you address the difficulties you experience?

## C.2.2 Codebook

Users	Designers	Business Leaders
automated data access requests	agile product development	amount of fines of non-compliance
awareness of company practices	arranging structured meetings	appointing a data protection officer
awareness of data collection practices	communicating UX benefits	automated decision
becoming more aware of data rights	communicating user behaviors	automatically authenticating users
blurring privacy	communicating user needs	collecting personal data
comprehension of requested permissions	communicating user privacy concerns	communicating to users
consumer privacy preferences	communicating with stakeholders	compliance overhead
cumbersome privacy options	conducting heuristic evaluation	cost of compliance is high
data breach concerns	conducting user research	cost of compliance is manageable
data privacy concerns	conducting design workshops	cost of compliance is unknown
device installation	conducting user interviews	cost of compliance is unrecognized
difficulty authenticating	recruiting users	creating privacy notices
difficulty rejecting consent	prototyping products	cutting corners
distrust of data collection practices	testing products	data protection by design
distrust of data processing practices	safeguarding individual rights	data protection compliance
distrust of smart home manufacturers	understanding technical limitations	data protection inconsistent in EU
erosion of trust	understanding organizational limitations	data protection inconsistent in UK/US
excessive permission requests	continuously improving smart products	data protection not applicable
exercising data rights	continuously conducting user research	data protection not relevant
experiencing dark patterns	improving user trust	data protection practices
experiencing detriment	improve consent interactions	data protection requirements
experiencing forced interactions	improve transparency	data protection roles
experiencing 'creepy' interactions	data protection compliance	data protection tools
fearing personal data will be sold	data protection features	educating staff
fear over collected personal data	data protection by design	facilitating data access procedures
feeling confused	data protection requirements	facilitating data access requests
feeling disappointed	privacy requirements	fines and penalties
feeling frustrated	privacy settings	gathering data securely
feeling overwhelmed	privacy threats	good judgment
feeling tricked	data protection responsibilities	hiring regulatory staff
hidden privacy defaults	determining a product's usability	implications of non-compliance
inaccessible privacy information	difficulty communicating with business leaders	in-house legal counsel
intrusive privacy defaults	difficulty balancing user/business requirements	lacking expertise
lack of awareness	difficulty conducting extensive UX processes	lacking funding
lack of awareness of worth of personal data	communicating UX efforts	lacking human labor
lack of concise privacy policies	communicating with business stakeholders	lacking knowledge
lack of transparent practices	educating users about business models	lacking resources
lack of transparent privacy policies	educating users about data monetization	lacking time
lack of trust	educating users about technology	manually authenticating users
learning about data rights	educating users about privacy	need for clear guidelines
making informed decisions	educating users about data protection	need for cost-effectiveness
managing consent	end-user compliance	need for government support
managing device permissions	experiencing complex conditions	not collecting personal data
manual data access requests	experiencing time pressure	outsourcing
need for anonymized data collection	experiencing work pressure	personal data mapping
need for brevity	feedback loops in production	prohibitive fines
need for personal data control	learning in production	purchasing services
need for transparency	learning about data protection guidance	regulatory fines
need for visualized privacy policies	making devices more conversational	responding to requests
not knowing how personal data was stored	on-going design approach	reviewing documentation
not understanding how smart homes work	over-provisioning devices	reviewing the legitimacy of requests
perceived ease of use	overcoming design challenges	right of access
perceived intrusion	raising awareness of user needs	right to be informed
perceived surveillance	raising awareness of privacy concerns	right to data portability
perceived usability	raising awareness of data protection requirements	right to erasure
perceived usefulness	representing and visualizing business viewpoints	right to object
perceived utility	representing and visualizing user viewpoints	right to rectification
positive experiences	researching data protection requirements	right to restrict processing
pressured consent interactions	researching privacy concerns	smaller businesses
privacy roadblocks	researching security concerns	strategic limitations
providing access to personal information	researching user pain points	taking necessary shortcuts
providing consent	satisficing conflicting opinions	tooling costs
security roadblocks	using design rules of thumb	training staff
unhelpful company responses	using heuristics	type of penalties non-compliance
unintelligible privacy information	using mental shortcuts	understanding requirements
unreliable smart home devices	using discount practices	unfair fines
using templates for data access requests	using best practices	using best practices
using third parties for data access requests	using tried-and-tested techniques	using common sense interpretations
vulnerable smart home devices	using usability testing	using own reasoning
withdrawing consent	using visualizations and graphs	using third parties

Table C.2: Codebook (Grounded Theory).

# D

## Chapter 6 Supplementary Material

### D.1 Conceptual Framework Analysis Codebook

<u>ux</u>	low authority	privacy management
usability	limited applications	privacy control
utility	high authority	privacy perceptions
product	specific design rules	privacy challenges
learnability	abstract design rules	privacy attacks
flexibility	high generability	privacy preferences
robustness	<b>security</b>	privacy concerns
branding	authentication	privacy threats
design	authorization	privacy behaviors
usability	account management	transparency
function	password management	privacy countermeasures
accessibility	security updates	trust
utility	security tools	<b>home tech</b>
credibility	security design	smart speakers
human factors	security vulnerabilities	smart cameras
design	security concerns	smart plugs
marketing	security breaches	smart bulbs
HCI	security behaviors	smart kitchen
user research	usable security	smart thermostats
<b>design guidelines</b>	unauthorized access	smart phones
guidelines	data theft	smart alarms
heuristics	access control	smart doorbells
principles	secure by design	smart hubs
practices	security threats	smart door locks
standards	security updates	smart ecosystem
rules	Privacy	home cameras
abstract rules	privacy by design	motion sensors
shortcuts	privacy design	microphones
rules of thumb	consent management	smart home assistants
guides	data protection	smart heaters
recommendations	tracking	smart displays
general applications	privacy tools	smart watches

**Table D.1:** Codebook (Conceptual Framework Analysis).

## D.2 Design Heuristics

In this appendix section, we list the design heuristics of our framework below:

- Research communal spaces where data may affect bystanders and other users
- Improve understanding of audiences and contextual uses of smart home products
- Consider how the actions of one user can affect other bystander users
- Build data usage models that represent transparent and ethical data usage practices
- Encourage users to learn the value of their data and make more mindful decisions
- Provide messages through notifications detailing how data can be misused
- Design and provide educational material to users of smart home products at crisis times
- Ensure that message are sent at the right time and the relevant stage of the life cycle
- Use user and business perspectives to communicate value of personal information
- Make sure the message is clear and succinct, and test it against sample users.
- Define upfront rules, heuristics and policies for deciding whether an event requires new notification.
- Periodically (and make it easy to) revisit granted consent choices
- Aim for transparency (e.g., provide information showing how personal data has been used over time)
- Consider usage triggers (changes to bystanders or users) that might prompt consent revisions
- Consider in which phases of the system life cycle would it be appropriate to revisit consent
- Consider how much forgiveness can you grant, and the implications of revoking mistakenly given consent.
- Consider how you might want to retrospectively undo a mistaken consent decision.
- Add a two-step validation for consent decisions to ensure genuine choices
- Collecting consent should not impact an unrelated function
- If functionality requires consent, it should be explicit, and truthful
- Ensure that demands for consent are explanatory and make sense to the user
- Ensure that consent collected is valid, informed, and genuine.

- Consider how users can improve their awareness of data use from the company and other users.
- Consider how users interact with personal data that is specific to only one user.
- Consider what information you provide to users about personal data use.
- Consider the value of data to users, the company, attackers, bystanders and other users.
- Develop knowledge of imbalances, interests, and tensions which might cause conflict
- Develop knowledge of the additional uses and negative consequences of smart homes
- Develop knowledge of the abusability, and repurposing of smart home technologies
- Aim to design for the highest degree of assurance based on sensitive various functions
- Be aware that physical privacy properties are more trusted than software settings or indicated lights
- Consolidate information related to the effectiveness of privacy settings indicators

## D.3 Conceptual Framework Analysis Papers

In this appendix section, we present the papers used in our Conceptual Framework Analysis. Each paper was categorized in one or more category from: user experience, design guidelines, user security, user privacy and home tech.

**Table D.2:** Conceptual Framework Analysis Papers

	user experience	design guidelines	user security	user privacy	home tech
More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. Noura Abdi, Kopo M. Ramokapane, and Jose M. Such.	✓		✓	✓	✓
A Review of Smart Homes—Past, Present, and Future. Muhammad Raisul Alam, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali.					✓
Noah Aphorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic.				✓	✓
Noah Aphorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity.				✓	✓
Gaurav Bansal, Fatemeh ‘Mariam’ Zahedi, and David Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern.	✓			✓	
Genevieve Bell and Paul Dourish. 2007. Yesterday’s tomorrows: notes on ubiquitous computing’s dominant vision.					✓
Victoria Bellotti and Abigail Sellen. 1993. Design for privacy in ubiquitous computing environments.			✓		
Asa Blomquist and Mattias Arvola. 2002. Personas in action: ethnography in an interaction design team.	✓	✓			
A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities.	✓				✓
Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. 2010. Who’s hogging the bandwidth: the consequences of revealing the invisible in the home.				✓	✓
Nielsen, J., and Molich, R. (1990). Heuristic evaluation of user interfaces.	✓	✓			
Experience, World Leaders in Research-Based User. "Heuristic Evaluation: How-To: Article by Jakob Nielsen".	✓	✓			
Molich, R., and Nielsen, J. (1990). Improving a human-computer dialogue.	✓	✓			
Nielsen, J. (1994). Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.).	✓	✓			
Nielsen, Jakob (1994). Usability Engineering.	✓	✓			
Gerhardt-Powals, Jill (1996). "Cognitive engineering principles for enhancing human – computer performance".	✓	✓			
Heuristic Evaluation – Usability Methods – What is a heuristic evaluation?	✓	✓			
Shneiderman (1998, p. 75); as cited in: "Eight Golden Rules of Interface Design"	✓	✓			
Malviya, Kartik (20 November 2020). "8 Golden Rules of Interface Design"	✓	✓			
Weinschenk, S and Barker,D. (2000) Designing Effective Speech Interfaces. Wiley.	✓	✓			
Jeff Sauro. "What’s the difference between a Heuristic Evaluation and a Cognitive Walkthrough?"	✓	✓			

	user experience	design guidelines	user security	user privacy	home tech
Nizamani, Sehrish; Khoumbati, Khalil; Nizamani, Sarwat; Memon, Shahzad; Nizamani, Saad; Laghari, Gulsher A methodology for domain and culture-oriented heuristics creation and validation".	✓	✓			
Nizamani, Sehrish; Nizamani, Saad; Basir, Nazish; Memon, Muhammad; Nizamani, Sarwat; Memon, Shahzad (5 April 2021). "Domain and culture-specific heuristic evaluation of the websites of universities of Pakistan".	✓	✓			
Marshini Chetty, Ja-Young Sung, and Rebecca E. Grinter. 2007. How Smart Homes Learn: The Evolution of the Networked Home and Household.					✓
Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a glass house: a survey of private moments in the home.				✓	✓
Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies.			✓	✓	✓
K. L. Courtney. 2008. Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities.				✓	✓
Scott Davidof, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. 2006. Principles of Smart Home Control.				✓	✓
George Demiris and Brian K. Hensel. 2008. Technologies for an aging society: a systematic review of "smart home" applications.					✓
Paul Dourish, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem.			✓		✓
Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On? Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms.				✓	✓
Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior.	✓		✓	✓	✓
Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes.	✓		✓	✓	✓
Esther Goernemann and Sarah Spiekermann. 2020. Moments of Truth with Conversational Agents: An Exploratory Quest for the Relevant Experiences of Alexa Users.	✓				✓
Manu Gupta, Stephen S. Intille, and Kent Larson. 2009. Adding GPS-Control to Traditional Thermostats: An Exploration of Potential Energy Savings and Design Challenges.		✓	✓		✓
Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earleence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT).			✓		✓
Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras.				✓	✓
Information Commissioner's Ofce. 2020. When is consent appropriate?				✓	
Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(es) with Smart Home: Experiences of a Living Lab Field Study.	✓				✓



	user experience	design guidelines	user security	user privacy	home tech
Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility.	✓		✓		✓
Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse.			✓	✓	✓
Brian Y. Lim, Anind K. Dey, and Daniel Avrahami. 2009. Why and why not explanations improve the intelligibility of context-aware intelligent systems.	✓				✓
Nathan Malkin, Joe Deatruck, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users.	✓			✓	✓
Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What Can't Data Be Used For?":				✓	✓
Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where WeAre and Where WeNeed toGo.					✓
Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices.			✓		✓
Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. 2011. Exploring reactive access control.			✓		
Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An Inthe-Wild Study of Smart Homes, Their Development, and the People Who Live in Them.	✓				✓
Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world.				✓	✓
David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An empirical investigation of concerns of everyday tracking and recording technologies.				✓	✓
Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices.			✓		✓
Norbert Nthala and Emilee Rader. 2020. Towards a Conceptual Model for Provoking Privacy Speculation.				✓	
Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term effects of ubiquitous surveillance in the home.				✓	✓
Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world.				✓	✓
Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management.	✓				✓
Dave Randall. 2003. Living Inside a Smart Home: A Case Study. In Inside the Smart Home, Richard Harper (Ed.).	✓				✓
Erika Shehan and W. Keith Edwards. 2007. Home networking and HCI: what hath god wrought?	✓				✓
Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2007. Making the home network at home: Digital housekeeping.					✓

	user experience	design guidelines	user security	user privacy	home tech
Daphne Townsend, Frank Knoefel, and Rafk Goubran. 2011. Privacy versus autonomy: A tradeoff model for smart home monitoring technologies.	✓				✓
Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes.			✓		✓
Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance.				✓	✓
Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2017. Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things.	✓			✓	✓
Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges.	✓				✓
Charlie Wilson, Tom Hargreaves, and Richard HauxwellBaldwin. Benefits and Risks of Smart Home Technologies.			✓	✓	✓
Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourselfstyle smart homes.	✓				✓
Allison Woodruff, Sally Augustin, and Brooke Foucault. 2007. Sabbath day home automation: 'it's like mixing technology and religion'.	✓				✓
Rayoung Yang and Mark W. Newman. 2013. Learning from a learning thermostat: lessons for intelligent systems for the home.	✓				✓
Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes.	✓		✓	✓	✓
Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study.	✓		✓	✓	✓
Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy.	✓			✓	✓
Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. Bringing Security Home: A Process for Developing Secure and Usable Systems.	✓	✓	✓		
Mary Ellen Zurko. User-Centered Security: Stepping Up to the Grand Challenge.	✓	✓	✓		
Lee A. Bygrave. Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements.		✓		✓	
Kambiz Ghazinour and Emil Shirima. Privacy for Security Monitoring Systems.				✓	✓
Rosa Yáñez Gómez, Daniel Cascado Caballero, and José-Luis Sevillano. Heuristic Evaluation on Mobile Interfaces: A New Checklist.		✓			
Timo Jokela. Assessments of Usability Engineering Processes: Experiences from Experiments.	✓				
Michael Onuoha Thomas, Beverly Amunga Onyimbo, and Rajasvaran Logeswaran. Usability Evaluation Criteria for Internet of Things.	✓	✓			
Claire Rowland. UX and Service Design for Connected Products.	✓				✓
Tyler W. Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. Security During Application Development: An Application Security Expert Perspective.	✓		✓		
Tayyaba Nafees, Natalie Coull, Ian Ferguson, and Adam Sampson. Vulnerability Anti-patterns: A Timeless Way to Capture Poor Software Practices (Vulnerabilities).			✓		
Hala Assal and Sonia Chiasson. Security in the Software Development Lifecycle.			✓		

	user experience	design guidelines	user security	user privacy	home tech
Johanna Bergman and Isabelle Johansson. The User Experience Perspective of Internet of Things Development.	✓				✓
Noura Aleisa and Karen Renaud. Privacy of the Internet of Things.				✓	✓
Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User Perceptions of Smart Home IoT Privacy.	✓			✓	✓
Panagiotis Zagouras, Christos Kalloniatis, and Stefanos Gritzalis. Managing User Experience: Usability and Security in a New Era of Software Supremacy.	✓		✓		
Niels Raabjerg Mathiasen and Susanne Bødker. Threats or Threads - From Usable Security to Secure Experience?	✓		✓		
Fungai Bhunu Shava and Darelle Van Greunen. Factors Affecting User Experience with Security Features: A Case Study of an Academic Institution in Namibia.	✓		✓		
Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. Understanding the Experience-Centeredness of Privacy and Security Technologies.	✓		✓	✓	
Julia Bernd, Alisa Frik, Maritza L. Johnson, and Nathan Malkin. Smart Home Bystanders: Further Complexifying a Complex Context.			✓	✓	✓
Yaxing Yao, Justin Reed Basdeo, Oriana Rosata McDonough, and Yang Wang. Privacy Perceptions and Designs of Bystanders in Smart Homes.	✓			✓	✓
Jeungmin Oh and Uichin Lee. Exploring UX Issues in Quantified Self Technologies.	✓				✓
Johanna Bergman, Thomas Olsson, Isabelle Johansson, and Kirsten Rasmus-Gröhn. An Exploratory Study on How Internet of Things Developing Companies Handle User Experience Requirements.	✓				✓
Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home.			✓	✓	✓
Andreas Jacobsson and Paul Davidsson. Towards a Model of Privacy and Security for Smart Homes.			✓	✓	✓
Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, and Alfred Lui. Designing Connected Products : UX for the Consumer Internet of Things.	✓				✓
Marc Hassenzahl and Noam Tractinsky. User experience — a research agenda.	✓				
Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach.			✓	✓	✓
Junia Valente, Matthew A. Wyn, and Alvaro A. Cardenas. Stealing, Spying, and Abusing: Consequences of Attacks on Internet of Things Devices. IEEE Security			✓	✓	✓
Sarah Spiekermann and Lorrie Faith Cranor. "Engineering Privacy".				✓	
Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. "A Design Space for Eective Privacy Notices".		✓		✓	
Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. "Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online".	✓			✓	
Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes".				✓	✓

	user experience	design guidelines	user security	user privacy	home tech
Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. "Playing the legal card: Using ideation cards to raise data protection issues within the design process".	✓	✓		✓	✓
Helen J. Richardson. "A 'smart house' is not a home: The domestication of ICTs".					✓
Jon O'Brien, Tom Rodden, Mark Rounceeld, and John Hughes. "At Home with the Technology : An Ethnographic Study of a Set-Top-Box Trial".	✓				✓
Sarah Mennicken, Jo Vermeulen, and Elaine M Huang. "From Today 's Augmented Houses to Tomorrow 's Smart Homes : New Directions for Home Automation Research".					✓
Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. "Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine".	✓				✓
Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steven Benford. "Making the Home Network at Home: Digital Housekeeping".	✓				✓
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".	✓			✓	✓
Sarah Mennicken and Elaine M Huang. "Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them".					✓
Ssara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "'She'll Just Grab Any Device That's Closer": A Study of Everyday Device & Account Sharing in Households".	✓		✓		✓
Roxanne Leitão. "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse".			✓	✓	
Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. "Protection, Productivity and Pleasure in the Smart Home".	✓				✓
Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. "I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios".	✓			✓	✓
Andy Crabtree, Richard Mortier, Toni Robertson, and Ina Wagner. "Human Data Interaction: Historical Lessons from Social Studies and CSCW".	✓				
Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. "'I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments".	✓			✓	✓
Vinay Koshy, Joon Sung Park, Ti-Chung Cheng, and Karrie Karahalios. "'We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes".	✓				✓
Liam J. Bannon. "From Human Factors to Human Actors: The Role of Psychology and Human-Computer Interaction Studies in System Design".	✓	✓			
Liam J Bannon. "Perspectives on CSCW: From HCI and CMC to CSCW".	✓				
Paul M. Aoki and Allison Woodru. "Making space for stories: ambiguity in the design of personal communication systems".	✓				

## D.4 Heuristics Evaluation

We present the evaluation of our heuristics in Table D.3 below.

**Table D.3:** Heuristic Evaluation Details

Design Heuristics	Used	Understood?	# of references?	Reception?	Goals?
Research communal spaces where data may affect bystanders and other users	✓	Yes	2	Positive	Problem Understanding
Improve understanding of audiences and contextual uses of smart home products	✓	Yes	3	Positive	Problem Understanding
Consider how the actions of one user can affect other bystander users	✓	Yes	5	Positive	Problem Understanding
Build data usage models that represent transparent and ethical data usage practices	✓	Yes	1	Neutral	Alternative Solution
Encourage users to learn the value of their data and make more mindful decisions	✓	Yes	3	Positive	Problem Resolution
Provide messages through notifications detailing how data can be misused	✓	Yes	14	Positive	Problem Resolution
Design and provide educational material to users of smart home products at crisis times		N/A	N/A	N/A	N/A
Ensure that message are sent at the right time and the relevant stage of the life cycle	✓	No	1	Negative	Eliciting Discussion
Use user and business perspectives to communicate value of personal information	✓	Yes	2	Positive	Problem Understanding
Make sure the message is clear and succinct, and test it against sample users.	✓	Yes	6	Positive	Problem Resolution
Define upfront rules, heuristics and policies for deciding whether an event requires new notification.	✓	Yes	2	Neutral	Alternative Solution
Periodically (and make it easy to) revisit granted consent choices	✓	Yes	11	Positive	Problem Resolution
Aim for transparency (e.g., provide information showing how personal data has been used over time)	✓	Yes	4	Positive	Eliciting Discussion
Consider usage triggers (changes to bystanders or users) that might prompt consent revisions	✓	Yes	7	Positive	Problem Understanding
Consider in which phases of the system life cycle would it be appropriate to revisit consent		N/A	N/A	N/A	N/A
Consider how much forgiveness can you grant, and the implications of revoking mistakenly given consent.	✓	Yes	4	Positive	Problem Understanding
Consider how you might want to retrospectively undo a mistaken consent decision.	✓	Yes	4	Positive	Problem Understanding
Add a two-step validation for consent decisions to ensure genuine choices	✓	Yes	8	Positive	Problem Resolution
Collecting consent should not impact an unrelated function	✓	No	2	Negative	Eliciting Discussion

Design Heuristics	Used	Understood?	# of references?	Reception?	Goals?
If functionality requires consent, it should be explicit, and truthful	✓	Yes	1	Positive	Eliciting Discussion
Ensure that demands for consent are explanatory and make sense to the user	✓	Yes	16	Positive	Problem Resolution
Ensure that consent collected is valid, informed, and genuine.	✓	Yes	12	Positive	Problem Resolution
Consider how users can improve their awareness of data use from the company and other users.	✓	Yes	8	Positive	Problem Understanding
Consider how users interact with personal data that is specific to only one user.		N/A	N/A	N/A	N/A
Consider what information you provide to users about personal data use.	✓	Yes	9	Positive	Problem Understanding
Consider the value of data to users, the company, attackers, bystanders and other users.	✓	Yes	10	Positive	Problem Resolution
Develop knowledge of imbalances, interests, and tensions which might cause conflict	✓	Yes	7	Positive	Problem Understanding
Develop knowledge of the additional uses and negative consequences of smart homes	✓	Yes	1	Positive	Problem Understanding
Develop knowledge of the abusability, and repurposing of smart home technologies	✓	Yes	10	Positive	Problem Resolution
Aim to design for the highest degree of assurance based on sensitive various functions	✓	Yes	4	Positive	Eliciting Discussion
Be aware that physical privacy properties are more trusted than software settings or indicated lights	✓	Yes	4	Neutral	Eliciting Discussion
Consolidate information related to the effectiveness of privacy settings indicators	✓	Yes	6	Neutral	Eliciting Discussion

# E

## Ethics Applications and Approval

As described in Section 3.3, all studies reported in this thesis were thoroughly reviewed and approved by the Central University Research Ethics Committee<sup>1</sup> (CUREC). CUREC has overall responsibility for the development of Oxford University’s Research Ethics Policy, and Oxford University’s ethical review process.

In this appendix, we provide the application material of the following CUREC-approved studies: CS\_C1A\_19\_024 (see Section E.1), CS\_C1A\_19\_049 (see Section E.2) and CS\_C1A\_021\_037 (see Section E.3).

For every CUREC application attached, we include the following: information sheets, interview question guides, consent forms, and poster advertisements.

Chapter	CUREC Approval Number	Appendix Index
Chapter 4	CUREC/CS_C1A_19_024	Section E.1
Chapter 5	CUREC/CS_C1A_19_049	Section E.2
Chapter 6	CUREC/CS_C1A_021_037	Section E.3

**Table E.1:** CUREC Applications Attached

<sup>1</sup><https://governance.admin.ox.ac.uk/central-university-research-ethics-committee>

## E.1 Ethics Application CUREC/CS\_C1A\_19\_024

### E.1.1 Application Material

#### 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 that the University is meeting its obligations as a responsible institution.

They start from the presumption that all members of the University will 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](mailto:ethics@socsci.ox.ac.uk) using your official [ox.ac.uk](mailto:ox.ac.uk) email address. **Only emailed applications will be accepted.**

#### WHAT THIS CHECKLIST IS DESIGNED FOR

This **CUREC 1A checklist** is designed largely for research that falls within the Divisions of Social Sciences and Humanities where ethical issues are relatively few and straightforward. Interviews, field work and oral history are also included in the CUREC process.

The **full CUREC 2 application** is only required where certain project characteristics (e.g. type of participants, or procedures) result in a more complex set of ethical issues. It is expected that only in a limited number of cases will it be necessary for researchers to complete a CUREC 2 application. The checklist below will direct you to a CUREC 2 application if needed.

#### WHAT THIS CHECKLIST WILL NOT ASSESS

This checklist does not cover research governance, satisfactory methodology, or compliance with the requirements of publishers when administering their tests or questionnaires. As **principal researcher (i.e. principal investigator)**, it is your responsibility to ensure that requirements in these areas are met.

CUREC does not review studies classed as **audit** (see [Glossary](#) and [Decision Flowchart for CUREC](#) on our website).

If your study involves **NHS patients, NHS staff / data / facilities, or human tissue**, please check the [Decision Flowchart for NHS approval](#) and contact the [Clinical Trials and Research Governance \(CTRG\) team](#) in the first instance.

Further information on the University's research ethics procedures is available from the [CUREC website](#).



<b>SECTION A: Filter for CUREC2 application</b>		
This section determines whether your study raises more complex issues which require the completion of a full application for ethical review, known as the CUREC 2 application.		
<b>(Please mark 'X' in the Yes/No column as appropriate to indicate your response.)</b>		
1. Are research participants classed as <a href="#">people whose ability to give free and informed consent is in question</a> ? (This may include those under 18 (though see " <a href="#">competent youths</a> "), prisoners, or adults "at risk".) Your attention is drawn to the University's <a href="#">Safeguarding Code of Practice</a> and its implications for researchers involving children or adults at risk, including the need for the work to be risk assessed and for researchers to undertake related training.  ( <b>Note:</b> If any of your participants are aged 16 or under, please answer 'Yes' here <b>and</b> also answer question 5 below.)		No
2. By taking part in the research, will participants be at serious risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)?		No
3. Does the research involve the <a href="#">deception</a> of participants?		No
4. Does your research raise issues relevant to the <b>Counter-Terrorism and Security Act (the Prevent duty)</b> , which seeks to prevent people from being drawn into terrorism? Please see advice on this on our <a href="#">Best Practice Guidance web page</a> .		No
If you have answered 'No' to all of the questions above please go to <b>Section B</b> . If you have answered 'Yes' to any question above continue to question 5 below.		
5. Is your project covered by a CUREC <a href="#">approved procedure</a> (formerly known as "CUREC Protocols")?		No
If yes, please give research procedure number(s):		
If you answered 'Yes' to ANY of questions 1-4, <b>and</b> answered 'No' to question 5, <b>please stop completing this checklist and do not submit it for ethical review</b> . Instead, please complete the <a href="#">CUREC 2 application form</a> from the CUREC website. Then submit the CUREC 2 form for ethical review. If you answered 'Yes' to ANY of questions 1-3, <b>and</b> answered 'Yes' to question 5, please go on to <b>Section B</b> .		
<b>SECTION B: Contact details and project description (NB: must be typed not handwritten)</b>		
<b>Contact details:</b>		
1. <b>Principal investigator</b> / supervisor (if student research (title and full name):	Dr. Ivan Flechais	
2. Name of student (if student research):	George Chalhoub	
3. Degree programme, e.g. DPhil, BA, MPhil, BSc, MSc (if student research):	DPhil Cyber Security	
4. Department or Institute name:	CDT Cyber Security	
5. Address for correspondence (if different from above):	Pembroke College, St. Aldates Oxford, OX1 1DW	
6. University e-mail ( <b>not</b> private email) and telephone:	<a href="mailto:george.chalhoub@pmb.ox.ac.uk">george.chalhoub@pmb.ox.ac.uk</a>	
7. Name and status of others taking part in the project, e.g. third year undergraduate; postdoctoral research assistant:	N/A	

SECTION B continued	
<b>Project description:</b>	
8. Title of research project:	User Experience and Security of Home Smart Speakers
9. List of location(s) where project will be conducted:	Oxford, United Kingdom
10. If your research involves overseas travel or fieldwork and your department requires a travel risk assessment, will you have completed and returned a risk assessment form beforehand? (This has to be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out <u>University travel insurance</u> .)	Not required in this instance
11. Anticipated duration of research project overall:	4 months
12. Anticipated start and end dates of the research project involving human participants:	From: (01/06/19) To: (13/09/19) Please note that you will need ethics approval <b>before</b> you start your research. CUREC 1As may take up to 30 days to process.
13. External organisation funding the research (if applicable): N/A	
14. Title and very brief and simple lay description of <b>research</b> (about 150 words), plus description (about 200 words) of the nature of participants.	
a) Title, brief description of research (150 words) in lay language. When describing the research, please include your methodology, how you are applying professional guidelines, and the use to which results/data will be put. <b>Please also declare any conflicts of interest here.</b>	
<p>The goal of this research project is to investigate how much do User Experience (UX) factors influence the security and privacy behaviour of users of home smart speakers (such as Amazon's Alexa, Google Home or Apple's HomePod). In order to accomplish the goals of this research, a qualitative study will be conducted. It will consist of (1) a literature review, (2) interviewing of participants and (3) qualitative analysis (likely thematic analysis). For the interview:</p> <ul style="list-style-type: none"> <li>• Interviewees will need to have owned and used smart home speakers.</li> <li>• I will aim to interview between 10 and 15 people for their use of smart speakers: The length of the interview will be around 30 minutes.</li> <li>• I will ask questions about user experience of smart speakers and security and privacy behaviour: Questions will be driven by the findings of the literature review (1).</li> <li>• Interviewees will be required to follow an informed consent process (participant information form, consent forms).</li> <li>• Names and contact details will not be kept on record. No sensitive, disturbing, suggestive or offensive questions will be asked.</li> <li>• I will follow <a href="#">Best Practice guide to Elite and expert interviewing</a> and the <a href="#">Oral History guidelines for interviewing</a>: the basic guidance applies to all interviews.</li> </ul>	

b) Description of participants and [obtaining informed consent](#) (200 words). When describing participants, please include

- criteria for inclusion/exclusion
- method of recruitment
- processes for consent to participate

Please ensure you attach as separate documents (if applicable, in English translation):

- your [recruitment and advertisement material](#) e.g. a poster or brief invitation letter/ email
- information for participants to read (or hear) before they agree to take part e.g. [written information sheets](#) or (only if applicable) [oral information scripts](#).
- 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
- a guide to interview questions (this may be a list of questions to be asked, or a preliminary scope of questions), or a sample of other instruments (such as a sample questionnaire)
- (if relevant) debriefing document after participants have taken part

In the process of recruiting interviewees, we will follow these criteria for inclusion:

- Owners of smart house speakers (Google Home, Amazon's Alexa and Apple's HomePod).
- Individuals aged 18 and above will be selected.
- Ability to give informed consent without special requirements.
- Fluency in the English language

The individuals will be asked if they are 18 and above before proceeding to the interview. No IDs will be checked unless the interviewees appear to look less than 18 years old.

Participants will be recruited via emails and connections/acquaintances. No posters are planned.

Participants will be thanked for their time with a £10 Amazon Gift Card. The gift card will be provided at the end of the interview.

Informed Consent forms will be printed and presented to the interviewees before the interview. Interviewees will be required to read and sign them before proceeding to the interview. While the informed consent form will clearly mention that the interviewees can opt out and withdraw their consent (stop the interview) at any time during the interview, I will verbally and clearly tell the interviewees that they can opt out and withdraw their consent (stop the interview) at any time.

The interviews are aimed to be conducted in person in an Oxford University building (Robert Hooke Building); however, if the interviewees cannot make it to the interview, the interview will be rescheduled on Skype (audio).

In the event where the interviewee decides to withdraw her or his consent, the recording will stop and be deleted immediately. The interviewee will be thanked for his or her time and will be informed that all data collected is removed.

The interviewees will be given a cut-off date to withdraw their consent after they have undertaken the study. The cut-off date will be the end of the project date: 13/09/19.

15. What are the ethical issues connected with your research and what steps have you taken to address them? Please do not answer 'none'. The committee needs to see evidence that you have identified potential ethical issues with respect to your research and have taken steps to address them. These issues could relate to:

<ul style="list-style-type: none"> <li>• your own physical and psychological safety as a researcher (please see the <a href="#">University's</a> and <a href="#">Social Science Division's Safety in Fieldwork</a> guidance</li> <li>• participant burdens and/or risks, and</li> <li>• data protection/ confidentiality (please also see section 18).</li> </ul> <p>For more guidance on ethical issues, please see <a href="http://researchsupport.admin.ox.ac.uk/governance/ethics/resources">http://researchsupport.admin.ox.ac.uk/governance/ethics/resources</a></p>		
<p>The ethical issues identified are listed below:</p> <ol style="list-style-type: none"> <li>Possibility of upsetting or embarrassing the interviewees <i>Mitigation: Avoiding the discussion of any sensitive topics. Informing the participants verbally and in writing that they can opt out at any time.</i></li> <li>Leaking of the audio recordings of the interviewees <i>Mitigation: Encryption of the audio recordings at rest and storing them offline only.</i></li> <li>Interviewees oversharing information <i>Mitigation: If the interviewees overshare information, it will be removed from the study and the transcription of the audio. Oversharing includes personal circumstances such as messy divorce, bankruptcy or death of a beloved pet. I will also follow the guidance for <a href="#">Elite and Expert Interviewing</a>.</i></li> <li>Researcher safety risks <i>Mitigation: Following <a href="#">CUREC's BPG 01 Researcher Safety</a> guidelines. Staying on university premises.</i></li> </ol>		
<p><b>Section B continued</b></p>		
<p>16. Will you obtain <a href="#">informed consent</a> according to CUREC guidelines and good practice in your discipline before participation?</p>	<p>Yes</p>	
<p>If you have marked 'No', please give a brief explanation and justification for this decision here:</p>		
<p>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.</p>		<p>No</p>
<p>If you have marked 'Yes', please make sure that you have included some <b>supporting information</b> (as directed in question 14 of this section) showing the range of questions covering these issues.</p>		

<p><b>18. Management and handling of personal and other research data</b></p> <p>Your management and handling of <a href="#">personal data</a> and <a href="#">special category data</a> of human participants, either directly or via a third party, will need to comply with the requirements of the General Data Protection Regulation (GDPR) and the new Data Protection Act, as set out in the <a href="#">University's Guidance on Data Protection and Research</a>. In answering the questions below, please also consider the points raised in the <a href="#">Data Protection Checklist</a>. For advice on research data management and security, please consult with the University's Research Data Team (<a href="mailto:researchdata@ox.ac.uk">researchdata@ox.ac.uk</a>) and/or your local IT department and the University's <a href="#">web pages on research data management</a>.</p>		
<p>a) Will your research involve the collection of <b>records of consent</b> (e.g. written forms, audio-recorded, or other recorded consent)?</p> <p><b>If 'Yes', these will be classed as fully identifiable personal data (directly linked to an individual).</b></p>	<p>Yes</p>	
<p>b) Will your research involve the collection of <b>other personal data</b>?</p> <p><b>If 'Yes', specify in what form(s) this will be stored:</b></p> <ul style="list-style-type: none"> <li>• Fully identifiable (directly linked to an individual)</li> <li>• Pseudonymised (potentially identifiable as data may be attributed to an individual if linkage information can be accessed elsewhere by researchers)</li> <li>• Fully anonymised (i.e. cannot be linked to an individual)</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p>	<p>No</p>
<p>c) Will any of the personal data you collect classify as <a href="#">special category</a> data?</p> <p><b>If 'Yes', in what form(s) will this be stored:</b></p> <ul style="list-style-type: none"> <li>• Fully identifiable (directly linked to an individual)</li> <li>• Pseudonymised (potentially identifiable as data may be attributed to an individual if linkage information can be accessed elsewhere by researchers)</li> <li>• Fully anonymised (i.e. cannot be linked to an individual)</li> </ul>		<p>No</p>
<p>d) How will any personally identifiable data be collected, <a href="#">transferred and backed up</a>? Please describe the arrangements for any physical transfer of personal data (including paper records and data captured electronically via portable media) from where it is collected to local storage.</p>		
<p>Personally identifiable data will be collected during the interview using an audio recording device. The recordings will be transferred to a laptop via a USB stick. Both the USB stick and the laptop will be encrypted. The recordings will be kept locally (offline) and not uploaded to any cloud storage service (or anywhere online).</p>		
<p>e) Where, and for how long, will participants' personally identifiable data be stored during and after the study? (Please outline the procedures for ensuring confidentiality, eg security arrangements, anonymisation or pseudonymisation of such data. Please distinguish between records of consent and other forms of personally identifiable data stored)</p>		

The following is collected from interviews:

Consent form and contact information (Personally identifiable information):

- Collection: Consent forms will be sent out and collected, at the beginning of the interview, in person or in email.
- Storage: If the consent form is digital (sent by email), it will be encrypted by the signatory, before being emailed (Participants will be asked to password protect the form). If the consent form is printed (handed out physically), it will be stored safely in safe or secure location based on the advice of my supervisor and the Department of Computer Science.
- Backup: The consent forms will be electronically backed up on an encrypted dark disk.

Audio Recordings (Personally identifiable information):

- Collection: During the interview, audio data will be recorded using a digital recorder on the computer.
- Storage: All recordings will be immediately be transferred to a secure and encrypted university disk after the interview and be deleted from the portable recorder. Once the audio recordings are transcribed, they will be deleted from the university disk. The transcriptions will be anonymised and stored on encrypted university disks.
- Backup: The anonymised transcriptions will be backup on a secure on an encrypted hard disk.

Generated Token: A token will generated to identify all data collected for each participant (including their consent forms and anonymised interview transcripts). This way, if a participant expresses a desire to withdraw from the study, the data can be deleted from the hard drives upon request. The token will be kept in a separate encrypted hard drive only accessible to me.

Personal data will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 4 months where the personal data will be held. Therefore, the personal data will be held for 4 months.

f) If storing pseudonymised data, please confirm that identifiers will be held separately from the research data and linked through a unique study number. Specify how and at what point the pseudonymisation will occur, how the linkage information will be stored and state whether or not (and when) the linkage will be destroyed.

The audio recordings will be transcribed (manually) into text and the personally identifiable data will be erased from the text (such as names, extra or unnecessary information, etc ). According to [UK Data Service](#), there are direct and indirect identifiers which can disclose a person's identity. All of that data will be removed from the text.

A pseudonymisation token will be generated for each participant, which is used to identify all data collected for each participant (including their consent forms, survey responses and anonymised interview transcripts). These tokens will be kept on a separate encrypted hard disk only accessible to me. The token will be used to destroy participant data if they express a desire to withdraw from the study. The token will be destroyed one year after the study has been completed.

Identifiers will be held separately from the research data and linked through a unique study number.

g) Who will have access to the personally identifiable data? If personally identifiable data is to be shared with another organisation, how will it be transferred/disclosed securely?

My supervisor and I (George Chalhou) will have access to the research data.

Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

No other entity or organisation will receive any personally identifiable data.

h) When and how will personally identifiable data be destroyed? (NB. Personally identifiable data should be destroyed when no longer required.)
The audio recording device will be wiped. The USB stick and laptop used will be wiped/formatted using available tools.
i) How, where and for how long will other research data be stored after the study has finished? For more information about University and research funder retention policies, please see the University's web pages on <a href="#">research data management</a> .
According to EPSRC's Research Data requirements, our research data will be stored securely on a university hard drive for a minimum of ten years after project publications and then destroyed.

Interview

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	X
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)	X
16. Photography of participant (you will generally need specific consent from participants for this)	
17. Others (please specify):	



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. <b>Note:</b> this is not an exhaustive list.		<b>Please mark 'X'</b>
Research specialism/ methodology	Association and guidance document	
Anthropology	<a href="#">Association of Social Anthropologists of the UK and Commonwealth</a>	
Criminology	<a href="http://www.britsoccrim.org/ethics/">http://www.britsoccrim.org/ethics/</a>	
Education	<a href="#">British Educational Research Association Ethical Guidelines for Educational Research</a>	
Geography	<a href="#">Association of American Geographers Statement on Professional Ethics</a>	
History	<a href="#">Oral History Society of the UK Ethical Guidelines</a>	X
Internet-based Research	<a href="#">British Psychological Society: Conducting Research on the Internet</a> <a href="#">Association of Internet Researchers Ethics Guide</a> Also see our <a href="#">Best Practice Guidance on internet-based research</a>	X
Law (Socio-Legal)	<a href="#">Socio-Legal Studies Association: Statement of Principles of Ethical Research</a>	
Management	<a href="#">Academy of Management's Professional Code of Ethics</a>	
Political Science	<a href="#">American Political Science Association (APSA) Guide to Professional Ethics in Political Science</a>	
Politics	<a href="#">Political Studies Association. Guidelines for Good Professional Conduct</a>	
Psychology	<a href="#">British Psychological Society Code of Ethics and Conduct</a>	
Social Research	<a href="#">Social Research Association: Ethical Guidelines</a>	X
Sociology	<a href="#">The British Sociological Association: Statement of Ethical Practice</a>	
Visual Research	<a href="#">ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research</a>	
Other professional guidelines. Please specify the other guidelines used here:		
Please indicate what training in research ethics the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at <a href="http://researchsupport.admin.ox.ac.uk/support/training/ethics">http://researchsupport.admin.ox.ac.uk/support/training/ethics</a> ).		
If no formal training has been undertaken, please indicate any discussions of research methodology between researchers and supervisors here.		
Research Integrity: Arts and Humanities		

**SECTION E: Signatures** (The SSH IDREC Secretariat accepts either option below. If you have a [DREC](#), check which signature option it prefers.)

- **Option 1:** 'Electronic signatures', i.e. 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 in the sections below.**
- **Option 2:** Handwritten (wet-ink) signatures. Please scan them and the rest of the checklist pages to create a single PDF document and email through.

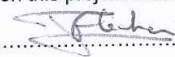
Please ensure this checklist is signed by:

For staff research:	For student research:
1. <a href="#">Principal investigator</a>	1. <a href="#">Principal investigator (project supervisor)</a>
2. <a href="#">Head of Department (or nominee)</a>	2. <a href="#">Head of Department (or nominee)</a>
	3. <a href="#">Student researcher</a>

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:  .....

Print name (block capitals): IVAN FLECHAIS ..... Date: 2/5/2019 .....

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: .....

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.

Signed by student: /george chalhoub/ (by email)  ..... Date: 26/04/2019

Print name (block capitals): GEORGE CHALHOUB

SECTION F: SUBMITTING THE COMPLETED CHECKLIST	Please mark 'X'
1. Check you have completed all sections (A-E)	X
2. Ensure your application is signed by you, your supervisor (if student) and department	X
3. <b>Please attach all supporting documents (see section B, question 14b for details).</b> If the appropriate supporting documentation is not included with your application, you will then be asked to provide this separately. <b>This may well delay the ethical review process, and thus the start of your research.</b>	X X
4. Ensure you have declared conflicts of interest (if any) in Section B, question 14a.	X
5. If your department has a <a href="#">Departmental Research Ethics Committee (DREC)</a> , submit this checklist and supporting information to the appropriate departmental officer.	X
6. If your department does not have a DREC, submit the checklist and supporting information to the SSH IDREC (email <a href="mailto:ethics@socsci.ox.ac.uk">ethics@socsci.ox.ac.uk</a> ).	X
7. Applications must be sent by email from your official ox.ac.uk email account. Please do not send applications by post.	X

Interview

X

## E.1.2 Information Sheet

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University email address: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### User Experience and Security of Home Smart Speakers

#### PARTICIPANT INFORMATION SHEET

Central University Research Ethics Committee (CUREC) Approval Reference: **CS\_C1A\_19\_024**

**1. Why is this research being conducted?**

The goal of this research project is to investigate or study how much do User Experience (UX) factors influence the security and privacy behaviour of users of home smart speakers (such as Amazon's Alexa, Google Home or Apple's HomePod).

**2. Why have I been invited to take part?**

You have been invited because you are an adult (aged 18 and above) and have owned and/or used smart home speakers in the past.

**3. Do I have to take part?**

No. You can ask questions about the research before deciding whether or not to take part. If you do agree to take part, you may withdraw yourself from the study at any time, without giving a reason, and without negative consequences, by advising me of this decision. The deadline by which you can withdraw any information you have contributed to the research is 13/09/2019. In the event where you withdraw your information, all of the recordings and information collected will be deleted and excluded from the study results.

**4. What will happen to me if I take part in the research?**

If you are happy to take part in the research, you will be asked to attend an interview in a single visit at *Robert Hooke Building, Parks Road, Oxford, OX1 3PR*. Information about the building (including accessibility information) can be found here:

<https://www.admin.ox.ac.uk/access/dandt/mpls/computersciences/roberthookebuilding/>. If you can't make it to the building, I might be able to schedule the interview on Skype.

When you arrive, I will talk you through the study procedures and give you the chance to ask any questions.

The interview/session should take approximately 30 minutes. You can also ask to pause or stop the interview at any time.

If you are still happy to take part, I will ask you to sign a consent form.

With your consent, I would like to audio record you because for audio recording, I can have an accurate record of your thoughts.

**5. Are there any potential risks in taking part?**

The main potential risk in taking part is a breach of confidentiality. To reduce any potential risks, your interview data will not be directly linked to your name. As you are going along, you can ask the interviewer to ignore or delete anything that you would not like to be kept on record.

**6. Are there any benefits in taking part?**

There will be no direct or personal benefit to you from taking part in this research.

**7. Expenses and payments**

You will receive a £10 Amazon voucher for your participation in the study.

**8. What happens to the data provided?**

The information you provide during the study is the **research data**. Any research data from which you can be identified (name, signature, audio recording etc.) is known as **personal data**.

**Personal / sensitive data** will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 2 months where the personal data will be held. Therefore, the personal data will be held for 2 months.

**Other research data** (including consent forms) will be stored for at least 3 years after publication or public release of the work of the research.

The researcher and/or supervisor will have access to the research data. Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

I would like your permission to use direct quotes against a pseudonym in any research outputs.

**9. Will the research be published?**

The research may be published in academic publications, websites and in the university.

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.

The research will be written up as a student's 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. If so, the thesis will be openly accessible.

**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\_19\_024).

**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 George Chalhoub ([george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)), and I will do our best to answer your query. I will acknowledge your concern within 10 working days and give you an indication of how it will be dealt with. If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter as soon as possible:

Chair, **Andrew Martin**; Email: [ethics@cs.ox.ac.uk](mailto:ethics@cs.ox.ac.uk).

**12. Data Protection**

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study.

The University will process your personal data for the purpose of the research outlined above. Research is a task that is performed in the public interest.

Further information about your rights with respect to your personal data is available from <http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/>.

**13. Further Information and Contact Details**

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

George Chalhoub  
Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD  
University email: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

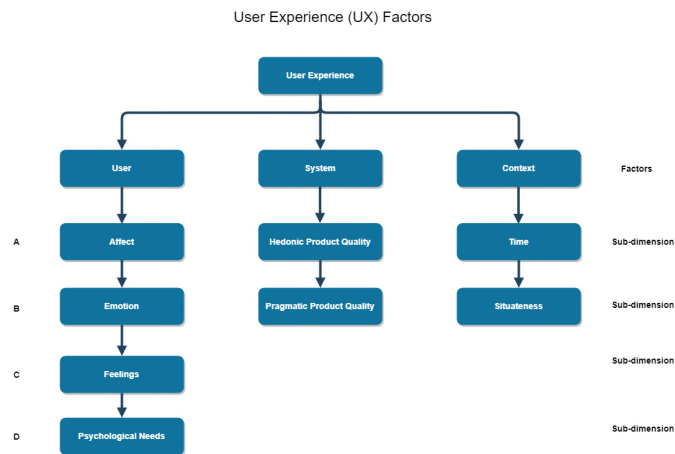
### E.1.3 Guide to Interview Questions

George Chalhoub  
 DPhil Cyber Security  
 Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

#### GUIDE TO INTERVIEW QUESTIONS

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_19\_024

The questions will be driven from the literature review which will be undertaken. There is no way that interview questions will be determined, however they will be scoped to the use of smart home speakers, experiences of people around smart home speakers and the security and privacy of smart home speakers. First, we will look at UX factors and sub-dimensions where we expect them to look like this:



Second, we will look at behaviour:

*E: Privacy*

*F: Security*

Then interview questions will be structured in this manner:

Q1: E + F (A)

Q2: E (B)

Q3: F (C)

Q4: E + F (D)

.

.

.

QN

Sample Questions (Estimation):

Demographics:

1. Country
2. Age
3. Gender
4. Education Level

Smart Device Use Questions:

5. What kind of Smart Home Device have you used in the past?
6. Tell us about your experiences with Smart Home Devices
7. Is this your own smart home device?
8. Is there someone else who uses your smart home device?
9. How many smart home devices do you own?
10. Are there any people using your smart home device for any reason?
11. Have you ever cancelled the installation of an app on your smart home device? If so why?
12. Have you ever uninstalled an app? If so, why?
13. What kind of apps do you use?
14. Do you use pre-installed security mechanisms on your Smart Home Device?

**In the event where interviewees overshare information (highly unlikely), it will be erased from the record as soon as possible.**



## E.1.4 Participant Consent Form

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### PARTICIPANT CONSENT FORM

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_19\_024

#### User Experience and Security of Home Smart Speakers

Purpose of Study: We are investigating how much User Experience (UX) factors influence the security and privacy behaviour of users of home smart speakers (such as Amazon's Alexa, Google Home or Apple's HomePod).

Please read the following. If you agree with the points below, tick each box and sign the form.

- |   |  | <i>Please initial each box</i> |
|---|--|--------------------------------|
| 1 | I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. | <input type="checkbox"/>       |
| 2 | I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason, and without any adverse consequences or penalty.                                | <input type="checkbox"/>       |
| 3 | I understand that research data collected during the study may be looked at by authorised people outside the research team. I give permission for these individuals to access my data.                 | <input type="checkbox"/>       |
| 4 | I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.                                     | <input type="checkbox"/>       |
| 5 | I understand who will have access to personal data provided, how the data will be stored and what will happen to the data at the end of the project.   | <input type="checkbox"/>       |
| 6 | I understand how this research will be written up and published.   | <input type="checkbox"/>       |
| 7 | I understand how to raise a concern or make a complaint.   | <input type="checkbox"/>       |
| 8 | I consent to being audio recorded.   | <input type="checkbox"/>       |
| 9 | I understand how audio recordings will be used in research outputs.  | <input type="checkbox"/>       |

10 I give permission to be quoted directly in research outputs against a pseudonym.

11 I agree to take part in the study.

Please sign below:

\_\_\_\_\_  
Name of Participant      dd / mm / yyyy  
Date      \_\_\_\_\_  
Signature

\_\_\_\_\_  
Name of person taking consent      dd / mm / yyyy  
Date      \_\_\_\_\_  
Signature

## E.1.5 Poster Advertisement

Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
[george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

User Experience and Security of Home Smart Speakers  
Ethics Approval Reference: CS\_C1A\_19\_024

### **VOLUNTEERS NEEDED FOR A STUDY**

We are investigating how much User Experience (UX) factors influence the security and privacy behaviour of users of home smart speakers (such as Amazon's Alexa, Google Home or Apple's HomePod).

We are looking for volunteers, aged 18 and above to answer questions in a small interview. You must own or have owned smart home speakers to participate. You would be invited to attend the interview in Robert Hooke Building, OX1 3QD to for 1 interview session. The session would take about 30 minutes of your time. You would be asked to answer questions related to your previous use of home smart speakers?

If you are interested and would like more information please contact George Chalhoub at the Department of Computer Science, 15 Parks Rd, Oxford OX1 3QD, on [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk). There is no obligation to take part.

You will be compensated for your time.

Thank you!

## E.2 Ethics Application CUREC/CS\_C1A\_1949

### E.2.1 Application Material

**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](mailto:ethics@socsci.ox.ac.uk) using your official [ox.ac.uk](mailto:ox.ac.uk) email address. **Only type-written, emailed applications will be accepted.**

<b>SECTION A: Filter for CUREC 2 application</b>		
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. <b>(Please mark 'X' in the Yes/No column.)</b>		
1. Are research participants classed as <a href="#">people whose ability to give free and informed consent is in question</a> ? (This may include under 18s (although see " <a href="#">competent youths</a> "), prisoners, or adults "at risk".) Your attention is drawn to the University's <a href="#">Safeguarding Code of Practice</a> 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 <b>and</b> also answer question 5 below.)	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
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 <input type="checkbox"/>	No <input checked="" type="checkbox"/>
3. Does the research involve the <a href="#">deception</a> of participants?	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
4. Does your research raise issues relevant to the <b>Counter-Terrorism and Security Act (the Prevent duty)</b> , which seeks to prevent people from being drawn into terrorism? Please see advice on this on our <a href="#">Best Practice Guidance web page</a> .	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
If you answered 'No' to <u>all</u> the questions above, go to <b>Section B</b> . If you answered 'Yes' to <u>any</u> question above, continue to question 5 below.		
5. Is your project covered by a CUREC <a href="#">Approved Procedure</a> (formerly known as "CUREC Protocols")?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes, give the specific Approved Procedure number(s):		
If you answered 'Yes' to <b>ANY</b> of questions 1-4, <b>and</b> answered 'No' to question 5, <b>stop completing this checklist and do not submit it for ethical review</b> . Instead, complete the <a href="#">CUREC 2 application form</a> from the CUREC website, then submit that for ethical review. If you answered 'Yes' to ANY of questions 1-3, <b>and</b> answered 'Yes' to question 5, go on to <b>Section B</b> .		

SECTION B: Contact details and project description	
<b>Contact details:</b>	
1. <b>Principal investigator</b> OR supervisor (if student research) (give title and full name)	Prof. Ivan Flechais
2. Name of student (if student research)	George Chalhoub
3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil	DPhil Cyber Security
4. Department or Institute name	Department of Computer Science
5. Address for correspondence (if different from above)	Pembroke College, St. Aldates Oxford, OX1 1DW
6. University ( <b>not</b> private) e-mail address and telephone number	<a href="mailto:george.chalhoub@pmb.ox.ac.uk">george.chalhoub@pmb.ox.ac.uk</a> 07716365711
7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant)	N/A

<b>Project description:</b>	
8. Title of research project	Exploring the relationship between UX, security, and privacy in smart home IoT devices
9. List of location(s) where project will be conducted	For users: Departmental premises, during working hours For designers: Departmental premises, during working hours. I am willing to go to business premises if required.
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 <u>University travel insurance</u> .) 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 <input type="checkbox"/> No <input type="checkbox"/> Not required in this instance <input checked="" type="checkbox"/>
11. Anticipated duration of overall research project	12 months
12.a) Anticipated start and end dates of the part of the research project involving human participants and/or personal data	From: (21/11/19) To: (01/11/20) <b>Note:</b> You will need ethics approval <b>before</b> you start your research. CUREC 1As may take up to 30 days to process. <b>Retrospective ethics approval cannot be granted.</b>

12. b) 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)?	N/A
13. <b>External</b> organisation funding the research (if applicable)	N/A
<p>14. a) Title and brief description of <a href="#">research</a> (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. <b>Please also declare any <a href="#">conflicts of interest</a> here.</b></p>	
<p><b>Exploring the relationship between UX, security, and privacy in smart home IoT devices</b></p> <p>To tackle our exploratory study, we aim to conduct interviews, followed by surveys, with users and designers of smart home IoT devices.</p> <p><i>Interviews with Users:</i> Based on results from previous research, we know that UX influences security and privacy in three areas: (1) the perception of risk, (2) the experience of harm and (3) the mitigation practice. We need to understand further how UX principles affect those three areas. We want to carry out 13 to 25 semi-structured interviews with IoT users in order to understand how (1) perceptions in UX influence people's understanding of risk and (2) how UX influences balancing behaviour.</p> <p><i>Interviews with Designers:</i> We're also conducting a qualitative investigation with IoT designers aimed to explore (1) how designers take into consideration and evaluate UX in the development of IoT features, (2) if and how a user-friendly approach is used to develop security and privacy features, and (3) the challenges faced when designing user-friendly security or privacy solutions. We aim to conduct around 13 to 25 semi-structured interviews and analyse them on the basis of grounded theory.</p> <p>The length of the interviews will be around 30 to 45 minutes. Names and contact details will not be kept as part of the research data; consent forms will be stored separately and linked to the research data by a token which is also stored separately. No sensitive, disturbing, suggestive or offensive questions will be asked. I will follow the <a href="#">Best Practice guide to Elite and expert interviewing</a> and the <a href="#">Oral History guidelines for interviewing</a>: the basic guidance applies to all interviews.</p> <p>To further validate our findings, we will conduct quantitative surveys (e.g. vignette) with users and designers in order to measure how much they align with the findings of our interviews. Data collected from the surveys will include demographic information about participants, work experience and motivations. No personally identifiable information will be collected from the surveys.</p>	
<p>14.b) Description of participants and how you will <a href="#">obtain informed consent</a> to take part in the research (about 200 words)</p> <p>1. Description of participants <b>and</b> your criteria for inclusion/exclusion</p>	

	<p>In the process of recruiting interviewees and conducting surveys, we will follow these criteria for inclusion:</p> <ul style="list-style-type: none"> <li>• <i>For Users:</i> Have used and owned IoT Devices. <i>For Designers:</i> have developed or designed IoT devices.</li> <li>• Individuals aged 18 and above will be selected.</li> <li>• Ability to give informed consent without special requirements.</li> <li>• Fluency in the English language</li> </ul> <p>The individuals will be asked if they are 18 and above before proceeding to the interview. No IDs will be checked unless the interviewees appear to look less than 18 years old.</p>
2.	<p>Your method(s) of recruitment</p> <p>Participants will be recruited via emails and connections/acquaintances. Posters will be made. We also might go to conferences and find designers that we can recruit. For surveys, we might use Prolific Academic (<a href="https://www.missmanypennies.com/prolific-academic/">https://www.missmanypennies.com/prolific-academic/</a>).</p>
3.	<p>Your processes for obtaining consent from participants</p> <p>Informed Consent forms will be printed and presented to the interviewees before the interview. Interviewees will be required to read and sign them before proceeding to the interview. While the informed consent form will clearly mention that the interviewees can opt-out and withdraw their consent (stop the interview) at any time during the interview, I will verbally and clearly tell the interviewees that they can opt-out and withdraw their consent (stop the interview) at any time.</p> <p>The interviews are aimed to be conducted in person in Oxford premises (e.g. Wolfson Building, Robert Hooke Building); however, if the interviewees cannot make it to the interview, the interview will be rescheduled on Skype (audio).</p> <p>In the event where the interviewee decides to withdraw her or his consent, the recording will stop and be deleted immediately. The interviewee will be thanked for his or her time and will be informed that all data collected is removed.</p> <p>The interviewees will be given a cut-off date to withdraw their consent after they have undertaken the study. The cut-off date will be the end of the project date: 01/11/20.</p>
<p>Please <b>attach separate supporting documents (in Word)</b> 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.</p>	
<p><input checked="" type="checkbox"/> <a href="#">Recruitment and advertisement material</a> (e.g. a poster, social media recruitment text, or brief invitation letter/ email)</p> <p><input checked="" type="checkbox"/> Information for participants to read (or hear) before they agree to take part (e.g. <a href="#">written information</a> or, if applicable, an outline <a href="#">oral information script</a>).</p>	

<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> A document to record informed consent. Templates for <a href="#">written consent forms</a> and/or <a href="#">oral information scripts</a> (in case of an oral consent process) are available from the CUREC website</li> <li><input checked="" type="checkbox"/> Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire)</li> <li><input type="checkbox"/> (If relevant) debriefing document after participants have taken part</li> <li><input type="checkbox"/> If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants</li> <li><input type="checkbox"/> Please complete section 15 if you cannot obtain informed consent</li> </ul>
<p><i>Please add any further details here.</i></p>
<p>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.</p>
<p>N/A</p>
<p>16. What are the ethical issues connected with your research and what steps have you taken to address them? <b>Please do not answer 'none'</b>. 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:</p> <ul style="list-style-type: none"> <li>• Participant burdens and/or risks             <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>For surveys:                      Risk: Potential to identify participants based on answers                      Mitigation: Using a 1-5 scale instead of a free-text response/anonymising data</p> <p>For interviews:                      Risk: Interviewees oversharing information                      Mitigation: If the interviewees overshare information, it will be removed from the study and the transcription of the audio. Oversharing includes personal circumstances such as messy divorce, bankruptcy or death of a beloved pet. I will also follow the guidance for <a href="#">Elite and Expert Interviewing</a>.</p> <p>Risk: Possibility of upsetting or embarrassing the interviewees                      Mitigation: Avoiding the discussion of any sensitive topics. Informing the participants verbally and in writing that they can opt out at any time.</p> </div> </li> <li>• Your own physical and psychological safety as a researcher or of fieldworkers you may employ (see the <a href="#">University's</a> and <a href="#">Social Science Division's Safety in Fieldwork guidance</a>)             <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Risk: Researcher safety risk                      Mitigation: Following <a href="#">CUREC's BPG 01 Researcher Safety</a> guidelines. Staying on university premises</p> </div> </li> <li>• Data protection/ confidentiality (also see Section 18).</li> </ul>



<div style="border: 1px solid black; padding: 5px;"> <p>Risk: Leaking of the audio recordings of the interviewees Mitigation: Encryption of the audio recordings at rest and storing them offline only.</p> </div>		
<p>For more guidance on ethical issues, please see <a href="http://researchsupport.admin.ox.ac.uk/governance/ethics/resources">http://researchsupport.admin.ox.ac.uk/governance/ethics/resources</a></p>		
<p><i>Discuss other ethical issues here</i></p>		
<p>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.</p>	<p>Yes <input type="checkbox"/></p>	<p>No <input checked="" type="checkbox"/></p>
<p><i>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.</i></p>		

<b>18. Management and handling of personal and other research data</b>	
<p>For the purpose of completing this section, all information provided by participants is considered <b>research data</b>. Any research data from which participants can be identified is known as <i>personal data</i>; any personal data which is sensitive is considered <i>special category data</i>.</p> <p>Management of <a href="#">personal data</a> and <a href="#">special category data</a> 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 <a href="#">University's Guidance on Data Protection and Research</a>. In answering the questions below, please also consider the points raised in the <a href="#">Data Protection Checklist</a>. For advice on research data management and security, please consult with the University's Research Data Team (<a href="mailto:researchdata@ox.ac.uk">researchdata@ox.ac.uk</a>) and/or your local IT department, and the University's <a href="#">web pages on research data management</a>.</p>	
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)	<input checked="" type="checkbox"/>
Online consent (may be anonymous)	<input type="checkbox"/>
Opt-out forms	<input type="checkbox"/>
Contact details for research purposes only (destroyed when no longer needed for this research)	<input type="checkbox"/>
Contact details kept for future studies	<input type="checkbox"/>

Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive)	<input checked="" type="checkbox"/>
Video recordings	<input type="checkbox"/>
Transcript of audio/video recordings	<input checked="" type="checkbox"/>
Photographs	<input type="checkbox"/>
Task results (e.g. paper/online tasks, diary completion)	<input type="checkbox"/>
Questionnaire answers	<input checked="" type="checkbox"/>
Field notes	<input type="checkbox"/>
Other (please specify below)	<input type="checkbox"/>
b.) For <b>each</b> 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.	
See answer below	
c.) How and where will <b>each type of data</b> 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. <a href="#">Nexus 365</a> <a href="#">OneDrive for Business</a> , <a href="#">SharePoint</a> ), security arrangements and de-identification of such data. Do not store unencrypted data in freely available cloud services or unprotected USB drives.	
Consent form and contact information (Personally identifiable information):	
<ul style="list-style-type: none"> <li>• Collection: Consent forms will be sent out and collected, at the beginning of the interview, in person or in email.</li> <li>• Storage: <b>If the consent form is digital</b> (sent by email), it will be encrypted by the signatory, before being emailed. Participants will be asked to password-protect the file, but not all users will know how to do that. I will be able to give technical advice if required. If the encryption by the signatory process is difficult, an oral consent process will take place: I will send all documents in advance, then go through the consent documents together at the start of the interview (I would note on my own copy of the form the parts that the participant agrees to, and put [verbal consent] in place of their signature at the bottom). <b>If the consent form is printed</b> (handed out physically), it will be stored safely in safe or secure location based on the advice of my supervisor and the Department of Computer Science.</li> <li>• Backup: The consent forms will be electronically backed up on an encrypted dark disk.</li> </ul>	
Audio Recordings (Personally identifiable information):	
<ul style="list-style-type: none"> <li>• Collection: During the interview, audio data will be recorded using a digital recorder. The recordings will be transferred to a laptop via a USB stick. Both the USB stick and the laptop will be encrypted. The recordings will be kept locally (offline) and not uploaded to any cloud storage service (or anywhere online).</li> <li>• Storage: All recordings will be immediately be transferred to a secure and encrypted disk after the interview and be deleted from the portable recorder. Once the audio recordings are transcribed, they will be deleted from the disk. The transcriptions will be anonymised and stored on the disks.</li> <li>• Backup: The anonymised transcriptions will be backed up on a secure on an encrypted hard disk.</li> </ul>	

Generated Token: A token will be generated to identify all data collected for each participant (including their consent forms and anonymised interview transcripts). This way, if a participant expresses a desire to withdraw from the study, the data can be deleted from the hard drives upon request. The token will be kept in a separate encrypted hard drive only accessible to me.

Online Surveys:

The surveys will be hosted on the Online Surveys platform (formerly BOS). Online surveys is hosted by JISC and is accessible through the University's subscription. The platform provides rigorous access to the response data, allowing access to permitted users only. Furthermore, the Data Protection section of their Terms and Conditions (<https://www.onlinesurveys.ac.uk/terms-and-conditions/>) states that no personal data is disclosed to third parties unless legally required, which guarantees the security of our survey and privacy of our survey participants.

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?

A pseudonymisation token will be generated for each participant, which is used to identify all data collected for each participant (including their consent forms, survey responses and anonymised interview transcripts). These tokens will be kept on a separate encrypted hard disk only accessible to me. The token will be used to destroy participant data if they express a desire to withdraw from the study. The token will be destroyed one year after the study has been completed.

Identifiers will be held separately from the research data and linked through a unique study number.

e.) Who will have access to the research data?

My supervisor (Prof. Ivan Flechais) and I will have access to the research data.

Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

No other entity or organisation will be permitted to access our research data.

f.) If research data is to be shared with another organisation, how will it be transferred / disclosed securely?

N/A

g.) When and how will identifiable data (including audio/video recordings & photos) be destroyed or deleted?

**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.

Personal data will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 12 months where the personal data will be held. Therefore, the personal data will be held for 12 months.

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

<p>If <b>'Yes'</b>, please give details of who will store the data and on storage format, location and security. Note that <a href="#">open science</a> is encouraged.</p> <p>If <b>'No'</b>, please provide further details below.</p>		
<p>Other research data will be stored safely in safe or secure location based on the advice of my supervisor and the Department of Computer Science.</p>		
<p>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 <b>"No"</b>, please go to section <b>19</b>.)</p>	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
<p>j.) Do you have data access agreements for the use of this secondary data? (If so, please attach these.)</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<p>k.) Is your use of this secondary data compatible with what data subjects/participants agreed that their data should be used for?</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<p>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?</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
<p><b>19. Publication and dissemination of research data</b></p>		
<p>How will you disseminate and feedback project outcomes at the end of the research?</p>	<p>The research may be published in academic publications, websites and in the university.</p> <p>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.</p> <p>The research will be written up as a student's thesis.</p> <p>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. If so, the thesis will be openly accessible.</p>	

<b>SECTION C: Methods and procedures to be used</b>	
<b>Method used:</b> Please ensure you have addressed any potential ethical issues related to these methods in Section 14 and in your Participant Information Sheet	<b>Please mark 'X'</b>
1. Analysis of existing records	<input type="checkbox"/>
2. Snowball sampling (recruiting through contacts of existing participants)	<input type="checkbox"/>
3. Use of casual or local workers e.g. interpreters	<input type="checkbox"/>
4. Participant observation	<input type="checkbox"/>
5. Covert observation	<input type="checkbox"/>
6. Observation of specific organisational practices	<input type="checkbox"/>
7. Participant completes questionnaire in hard copy	<input type="checkbox"/>
8. Participant completes online questionnaire or other online task	<input checked="" type="checkbox"/>
9. Using social media	<input type="checkbox"/>
10. Participant performs paper and pencil task	<input type="checkbox"/>
11. Participant performs verbal or aural task (e.g. for linguistic study)	<input type="checkbox"/>
12. Focus group	<input type="checkbox"/>
13. Interview	<input checked="" type="checkbox"/>
14. Audio recording of participant (you will generally need specific consent from participants for this)	<input checked="" type="checkbox"/>
15. Video recording of participant (you will generally need specific consent from participants for this)	<input type="checkbox"/>
16. Photography of participant (you will generally need specific consent from participants for this)	<input type="checkbox"/>
17. Others (please specify below)	<input type="checkbox"/>

<b>SECTION D: Professional guidelines and training</b>		
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. <b>Note:</b> this is not an exhaustive list.		<b>Please mark 'X'</b>
<b>Research specialism/ methodology</b>	<b>Association and guidance document</b>	
Anthropology	<a href="#">Association of Social Anthropologists of the UK and Commonwealth</a>	<input type="checkbox"/>
Criminology	<a href="http://www.britsoccrim.org/ethics/">http://www.britsoccrim.org/ethics/</a>	<input type="checkbox"/>
Education	<a href="#">British Educational Research Association Ethical Guidelines for Educational Research</a>	<input type="checkbox"/>
Geography	<a href="#">Association of American Geographers Statement on Professional Ethics</a>	<input type="checkbox"/>
History	<a href="#">Oral History Society of the UK Ethical Guidelines</a>	<input checked="" type="checkbox"/>
Internet-based Research	<a href="#">British Psychological Society: Conducting Research on the Internet</a> <a href="#">Association of Internet Researchers Ethics Guide</a> Also see our <a href="#">Best Practice Guidance on internet-based research</a>	<input checked="" type="checkbox"/>
Law (Socio-Legal)	<a href="#">Socio-Legal Studies Association: Statement of Principles of Ethical Research</a>	<input type="checkbox"/>
Management	<a href="#">Academy of Management's Professional Code of Ethics</a>	<input type="checkbox"/>
Political Science	<a href="#">American Political Science Association (APSA) Guide to Professional Ethics in Political Science</a>	<input type="checkbox"/>
Politics	<a href="#">Political Studies Association. Guidelines for Good Professional Conduct</a>	<input type="checkbox"/>
Psychology	<a href="#">British Psychological Society Code of Ethics and Conduct</a>	<input type="checkbox"/>
Social Research	<a href="#">Social Research Association: Ethical Guidelines</a>	<input checked="" type="checkbox"/>
Sociology	<a href="#">The British Sociological Association: Statement of Ethical Practice</a>	<input type="checkbox"/>
Visual Research	<a href="#">ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research</a>	<input type="checkbox"/>
Other professional guidelines. Please specify the other guidelines used here:		<input type="checkbox"/>
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 <a href="http://researchsupport.admin.ox.ac.uk/support/training/ethics">http://researchsupport.admin.ox.ac.uk/support/training/ethics</a> ), or discussions between researchers and supervisors, if applicable.		
Research Integrity: Arts and Humanities		

**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. <a href="#">Principal investigator</a>	1. <a href="#">Principal investigator</a> (project supervisor)
2. <b>Head of Department (or nominee)</b>	2. <b>Head of Department (or nominee)</b>
	3. <b>Student researcher</b>

**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](mailto:ethics@cs.ox.ac.uk) confirming they've seen and approved the application** .....

**Print name** (block capitals): PROF. IVAN FLECHAIS

**Date:** 06/11/2019

**2. Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

- consider the principal investigator to be aware of her/his ethical responsibilities in regard to this research;
- 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);
- 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](mailto:ethics@cs.ox.ac.uk) from your Oxford address.**

**Print name** (block capitals): GEORGE CHALHOUB

**Date:** 25/10/2019

## E.2.2 Information Sheet

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University email address: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### Exploring the relationship between UX, security, and privacy in smart home IoT devices

#### PARTICIPANT INFORMATION SHEET

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_19\_049

**1. Why is this research being conducted?**

The goal of this research project is to investigate or study the relationship between User Experience (UX), security and privacy in smart home IoT devices.

**2. Why have I been invited to take part?**

You have been invited because you are an adult (aged 18 and above) and have used or designed an IoT device in the past.

**3. Do I have to take part?**

No. You can ask questions about the research before deciding whether or not to take part. If you do agree to take part, you may withdraw yourself from the study at any time, without giving a reason, and without negative consequences, by advising me of this decision. The deadline by which you can withdraw any information you have contributed to the research is 1 November 2020. In the event where you withdraw your information, all of the recordings and information collected will be deleted and excluded from the study results.

**4. What will happen to me if I take part in the research?**

If you are happy to take part in the research, you will be asked to attend an interview in a single visit at *Robert Hooke Building, Parks Road, Oxford, OX1 3PR*. Information about the building (including accessibility information) can be found here:

<https://www.admin.ox.ac.uk/access/dandt/mpls/computersciences/roberthookebuilding/>. If you can't make it to the building, I might be able to schedule the interview on Skype.

When you arrive, I will talk you through the study procedures and give you the chance to ask any questions.

The interview/session should be between 30 and 45 minutes. You can also ask to pause or stop the interview at any time.

If you are still happy to take part, I will ask you to sign a consent form.



With your consent, I would like to audio record you because for audio recording, I can have an accurate record of your thoughts.

**5. Are there any potential risks in taking part?**

The main potential risk in taking part is a breach of confidentiality. To reduce any potential risks, your interview data will not be directly linked to your name. As you are going along, you can ask the interviewer to ignore or delete anything that you would not like to be kept on record.

**6. Are there any benefits in taking part?**

There will be no direct or personal benefit to you from taking part in this research.

**7. Expenses and payments**

You will receive Amazon voucher (£10 or £15) for your participation in the study.

**8. What happens to the data provided?**

The information you provide during the study is the **research data**. Any research data from which you can be identified (name, signature, audio recording etc.) is known as **personal data**.

**Personal / sensitive data** will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 2 months where the personal data will be held. Therefore, the personal data will be held for 2 months.

**Other research data** (including consent forms) will be stored for at least 3 years after publication or public release of the work of the research.

The researcher and/or supervisor will have access to the research data. Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

I would like your permission to use direct quotes against a pseudonym in any research outputs.

**9. Will the research be published?**

The research may be published in academic publications, websites and in the university.

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.

The research will be written up as a student's 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. If so, the thesis will be openly accessible.

**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\_19\_049).

**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 George Chalhoub ([george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)), and I will do our best to answer your query. I will acknowledge your concern within 10 working days and give you an indication of how it will be dealt with. If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter as soon as possible:

Chair, **Andrew Martin**; Email: [ethics@cs.ox.ac.uk](mailto:ethics@cs.ox.ac.uk).

**12. Data Protection**

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study.

The University will process your personal data for the purpose of the research outlined above. Research is a task that is performed in the public interest.

Further information about your rights with respect to your personal data is available from <http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/>.

**13. Further Information and Contact Details**

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

George Chalhoub  
Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD  
University email: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

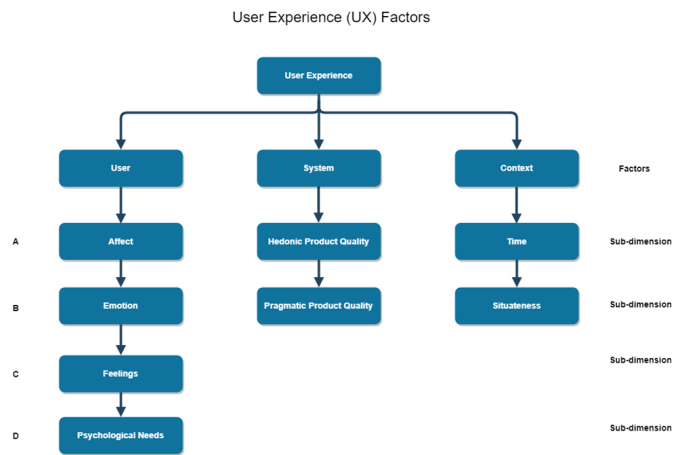
## E.2.3 Guide to Interview Questions

George Chalhoub  
 DPhil Cyber Security  
 Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### GUIDE TO INTERVIEW QUESTIONS

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_19\_049

The questions will be driven from the literature review which will be undertaken. There is no way that interview questions will be determined, however they will be scoped to the use of smart home devices, experiences of people around smart home devices and the security and privacy of smart home devices. First, we will look at UX factors and sub-dimensions where we expect them to look like this:



Second, we will look at behaviour:

*E: Privacy*

*F: Security*

Then interview questions will be structured in this manner:

Q1: E + F (A)

Q2: E (B)

Q3: F (C)

Q4: E + F (D)

.

.

.

QN

Sample Questions (Estimation):

Demographics:

1. Country
2. Age
3. Gender
4. Education Level

Smart Device Use Questions:

Users:

5. What kind of Smart Home Device have you used in the past?
6. Tell us about your experiences with Smart Home Devices
7. How do you feel about your smart home devices?
8. Do you take any measures to protect yourself from those devices? Do you feel the need to?
9. Is there someone else who uses your smart home device?
10. How many smart home devices do you own?
11. Are there any people using your smart home device for any reason?

Designers:

12. Describe how you are working with UX in the development process for IoT?
13. Describe how you are considering with security and privacy during the development process for IoT?
14. How are decisions made for security and privacy? On what basis are the decisions made?
15. Does the design team work with the security and privacy team?
16. How are UX and security/privacy choices factored during the development process?

**In the event where interviewees overshare information (highly unlikely), it will be erased from the record as soon as possible.**

## E.2.4 Participant Consent Form

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### PARTICIPANT CONSENT FORM

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_19\_049.

#### Exploring the relationship between UX, security, and privacy in smart home IoT devices

Purpose of Study: We are investigating the relationship between User Experience (UX), security and privacy in smart home IoT devices.

Please read the following. If you agree with the points below, tick each box and sign the form.

- |    |  | <i>Please initial each box</i> |
|----|--|--------------------------------|
| 1  | I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. | <input type="checkbox"/>       |
| 2  | I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason, and without any adverse consequences or penalty.                                | <input type="checkbox"/>       |
| 3  | I understand that research data collected during the study may be looked at by authorised people outside the research team. I give permission for these individuals to access my data.                 | <input type="checkbox"/>       |
| 4  | I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.                                     | <input type="checkbox"/>       |
| 5  | I understand who will have access to personal data provided, how the data will be stored and what will happen to the data at the end of the project.   | <input type="checkbox"/>       |
| 6  | I understand how this research will be written up and published.   | <input type="checkbox"/>       |
| 7  | I understand how to raise a concern or make a complaint.   | <input type="checkbox"/>       |
| 8  | I consent to being audio recorded.   | <input type="checkbox"/>       |
| 9  | I understand how audio recordings will be used in research outputs.  | <input type="checkbox"/>       |
| 10 | I give permission to be quoted directly in research outputs against a pseudonym.   | <input type="checkbox"/>       |
| 11 | I agree to take part in the study.   | <input type="checkbox"/>       |

Please sign below:

\_\_\_\_\_  
Name of Participant      dd / mm / yyyy  
Date      \_\_\_\_\_  
Signature

\_\_\_\_\_  
Name of person taking consent      dd / mm / yyyy  
Date      \_\_\_\_\_  
Signature

## E.2.5 Poster Advertisement

Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
[george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

Exploring the relationship between UX, security, and privacy in smart home IoT devices  
Ethics Approval Reference: CS\_C1A\_19\_049

### **VOLUNTEERS NEEDED FOR A STUDY**

We are investigating the relationship between User Experience (UX) and Security/Privacy in the smart home.

We are looking for volunteers, aged 18 and above to answer questions in a small interview. You must have used or designed smart home IoT devices to participate. You would be invited to attend the interview in Robert Hooke Building, OX1 3QD to for 1 interview session. The session would take about 30-45 minutes of your time. You would be asked to answer questions related to your previous experiences with home smart speakers.

If you are interested and would like more information please contact George Chalhoub at the Department of Computer Science, 15 Parks Rd, Oxford OX1 3QD, on [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk). There is no obligation to take part.

You will be compensated for your time.

Thank you!

## E.3 Ethics Application CS\_C1A\_021\_037

### E.3.1 Application Material

#### 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](mailto:ethics@socsci.ox.ac.uk) using your official [ox.ac.uk](mailto: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. <b>(Please mark 'X' in the Yes/No column.)</b>		
1. Are research participants classed as <a href="#">people whose ability to give free and informed consent is in question</a> ? (This may include under 18s (although see " <a href="#">competent youths</a> "), prisoners, or adults "at risk".) Your attention is drawn to the University's <a href="#">Safeguarding Code of Practice</a> 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 <b>and</b> also answer question 5 below.)	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
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 <input type="checkbox"/>	No <input checked="" type="checkbox"/>
3. Does the research involve the <a href="#">deception</a> of participants?	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
4. Does your research raise issues relevant to the <b>Counter-Terrorism and Security Act (the Prevent duty)</b> , which seeks to prevent people from being drawn into terrorism? Please see advice on this on our <a href="#">Best Practice Guidance web page</a> .	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
If you answered 'No' to <u>all</u> the questions above, go to <b>Section B</b> . If you answered 'Yes' to <u>any</u> question above, continue to question 5 below.		
5. Is your project covered by a CUREC <a href="#">Approved Procedure</a> (formerly known as "CUREC Protocols")?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
If yes, give the specific Approved Procedure number(s):		
If you answered 'Yes' to <b>ANY</b> of questions 1-4, <b>and</b> answered 'No' to question 5, <b>stop completing this checklist and do not submit it for ethical review</b> . Instead, complete the <a href="#">CUREC 2 application form</a> from the CUREC website, then submit that for ethical review. If you answered 'Yes' to ANY of questions 1-3, <b>and</b> answered 'Yes' to question 5, go on to <b>Section B</b> .		



SECTION B: Contact details and project description	
<b>Contact details:</b>	
1. <b>Principal investigator</b> OR supervisor (if student research) (give title and full name)	Prof. Ivan Flechais
2. Name of student (if student research)	George Chalhoub
3. Degree programme (if student research), e.g. BA, BSc, MSc, MPhil, DPhil	DPhil Cyber Security
4. Department or Institute name	Department of Computer Science
5. Address for correspondence (if different from above)	Pembroke College, St. Aldates Oxford, OX1 1DW
6. University ( <b>not</b> private) e-mail address and telephone number	<a href="mailto:george.chalhoub@pmb.ox.ac.uk">george.chalhoub@pmb.ox.ac.uk</a> 07716365711
7. Name and status of others taking part in the project (e.g. third year undergraduate; postdoctoral research assistant)	N/A

Project description:	
8. Title of research project	<b>Co-design workshops with users and designers of smart home products</b>
9. List of location(s) where project will be conducted	The project will be conducted remotely.
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 <a href="#">University travel insurance</a> .) 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 <input type="checkbox"/> No <input type="checkbox"/> Not required in this instance <input checked="" type="checkbox"/>
11. Anticipated duration of overall research project	12 months
12.a) Anticipated start and end dates of the part of the research project involving human participants and/or personal data	From: (1/11/22) To: (1/11/23) <b>Note:</b> You will need ethics approval <b>before</b> you start your research. CUREC 1As may take up to 30 days to process. <b>Retrospective ethics approval cannot be granted.</b>
12. b) 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)?	N/A

13. <b>External</b> organisation funding the research (if applicable)	N/A		
<p>14. a) Title and brief description of <a href="#">research</a> (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. <b>Please also declare any <a href="#">conflicts of interest</a> here.</b></p>			
<p><b>Co-design workshops with users and designers of smart home products</b></p> <p>We want to carry out 3 workshops having 3 to 4 participants each where we participants will use design heuristics to address challenges of data protection. For each workshop, participants will be asked to design a security and privacy solution for smart home products, using heuristics. The participants will be asked questions afterwards where will be able to capture their experiences.</p> <p>The length of the interviews will be around 30 to 45 minutes. Names and contact details will not be kept as part of the research data; consent forms will be stored separately and linked to the research data by a token which is also stored separately. No sensitive, disturbing, suggestive or offensive questions will be asked. I will follow the <a href="#">Best Practice guide to Elite and expert interviewing</a> and the <a href="#">Oral History guidelines for interviewing</a>: the basic guidance applies to all interviews.</p>			
<p>14.b) Description of participants and how you will <a href="#">obtain informed consent</a> to take part in the research (about 200 words)</p> <ol style="list-style-type: none"> <li>1. Description of participants <b>and</b> your criteria for inclusion/exclusion <table border="1" data-bbox="312 1043 1315 1346"> <tr> <td data-bbox="312 1043 1315 1346"> <p>In the process of recruiting interviewees and conducting surveys, we will follow these criteria for inclusion:</p> <ul style="list-style-type: none"> <li>• Individuals aged 18 and above will be selected.</li> <li>• Ability to give informed consent without special requirements.</li> <li>• Fluency in the English language</li> </ul> <p>The individuals will be asked if they are 18 and above before proceeding to the interview. No IDs will be checked unless the interviewees appear to look less than 18 years old.</p> </td> </tr> </table> </li> <li>2. Your method(s) of recruitment <table border="1" data-bbox="312 1402 1315 1469"> <tr> <td data-bbox="312 1402 1315 1469"> <p>Participants will be recruited via emails and connections/acquaintances. Posters will be made. We also might go to conferences and find designers that we can recruit.</p> </td> </tr> </table> </li> <li>3. Your processes for obtaining consent from participants</li> </ol>		<p>In the process of recruiting interviewees and conducting surveys, we will follow these criteria for inclusion:</p> <ul style="list-style-type: none"> <li>• Individuals aged 18 and above will be selected.</li> <li>• Ability to give informed consent without special requirements.</li> <li>• Fluency in the English language</li> </ul> <p>The individuals will be asked if they are 18 and above before proceeding to the interview. No IDs will be checked unless the interviewees appear to look less than 18 years old.</p>	<p>Participants will be recruited via emails and connections/acquaintances. Posters will be made. We also might go to conferences and find designers that we can recruit.</p>
<p>In the process of recruiting interviewees and conducting surveys, we will follow these criteria for inclusion:</p> <ul style="list-style-type: none"> <li>• Individuals aged 18 and above will be selected.</li> <li>• Ability to give informed consent without special requirements.</li> <li>• Fluency in the English language</li> </ul> <p>The individuals will be asked if they are 18 and above before proceeding to the interview. No IDs will be checked unless the interviewees appear to look less than 18 years old.</p>			
<p>Participants will be recruited via emails and connections/acquaintances. Posters will be made. We also might go to conferences and find designers that we can recruit.</p>			

<p>Informed Consent forms will be printed and presented to the interviewees before the interview. Interviewees will be required to read and sign them before proceeding to the interview. While the informed consent form will clearly mention that the interviewees can opt-out and withdraw their consent (stop the interview) at any time during the interview, I will verbally and clearly tell the interviewees that they can opt-out and withdraw their consent (stop the interview) at any time.</p> <p>The interviews are aimed to be conducted online via Oxford University's Microsoft Teams service.</p> <p>In the event where the interviewee decides to withdraw her or his consent, the recording will stop and be deleted immediately. The interviewee will be thanked for his or her time and will be informed that all data collected is removed.</p> <p>The interviewees will be given a cut-off date to withdraw their consent after they have undertaken the study. The cut-off date will be the end of the project date.</p>	
<p>Please <b>attach separate supporting documents (in Word)</b> 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.</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <a href="#">Recruitment and advertisement material</a> (e.g. a poster, social media recruitment text, or brief invitation letter/ email)</li> <li><input checked="" type="checkbox"/> Information for participants to read (or hear) before they agree to take part (e.g. <a href="#">written information</a> or, if applicable, an outline <a href="#">oral information script</a>).</li> <li><input checked="" type="checkbox"/> A document to record informed consent. Templates for <a href="#">written consent forms</a> and/or <a href="#">oral information scripts</a> (in case of an oral consent process) are available from the CUREC website</li> <li><input checked="" type="checkbox"/> Questions to be asked of participants (e.g. interview questions, or a preliminary scope of questions, or a sample questionnaire)</li> <li><input type="checkbox"/> (If relevant) debriefing document after participants have taken part</li> <li><input type="checkbox"/> If you feel the above approaches are not appropriate for your study, provide details on how you will obtain consent from participants</li> <li><input type="checkbox"/> Please complete section 15 if you cannot obtain informed consent</li> </ul>	
<p><i>Please add any further details here.</i></p>	
<p>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.</p>	
<p>N/A</p>	

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

For interviews:  
 Risk: Interviewees oversharing information  
 Mitigation: If the interviewees overshare information, it will be removed from the study and the transcription of the audio. Oversharing includes personal circumstances such as messy divorce, bankruptcy or death of a beloved pet. I will also follow the guidance for [Elite and Expert Interviewing](#).  
  
 Risk: Possibility of upsetting or embarrassing the interviewees  
 Mitigation: Avoiding the discussion of any sensitive topics. Informing the participants verbally and in writing that they can opt out at any time.

- 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](#))

Risk: Researcher safety risk  
 Mitigation: Following [CUREC's BPG 01 Researcher Safety](#) guidelines. Staying on university premises

- Data protection/ confidentiality (also see Section 18).

Risk: Leaking of the audio recordings of the interviewees  
 Mitigation: Encryption of the audio recordings at rest and storing them offline only.

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?

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*.

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](mailto:researchdata@ox.ac.uk)) and/or your local IT department, and the University's [web pages on research data management](#).

#### 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)	<input checked="" type="checkbox"/>
Online consent (may be anonymous)	<input type="checkbox"/>
Opt-out forms	<input type="checkbox"/>
Contact details for research purposes only (destroyed when no longer needed for this research)	<input type="checkbox"/>
Contact details kept for future studies	<input type="checkbox"/>
Audio recordings (preferably using PIN-protected audio recorder and stored on device's hard drive)	<input type="checkbox"/>
Video recordings	<input type="checkbox"/>
Transcript of audio/video recordings	<input type="checkbox"/>
Photographs	<input type="checkbox"/>
Task results (e.g. paper/online tasks, diary completion)	<input type="checkbox"/>
Questionnaire answers	<input type="checkbox"/>
Field notes	<input type="checkbox"/>
Other (please specify below)	<input type="checkbox"/>

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.

See answer below

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.

Consent form and contact information (Personally identifiable information):

- Collection: Consent forms will be sent out and collected, at the beginning of the interview, in person or in email.
- Storage: **If the consent form is digital** (sent by email), it will be encrypted by the signatory, before being emailed. Participants will be asked to password-protect the file, but not all users will know how to do that. I will be able to give technical advice if required. If the encryption by the signatory process is difficult, an oral consent process will take place: I will send all documents in advance, then go through the consent documents together at the start of the interview (I would note on my own copy of the form the parts that the participant agrees to, and put [verbal consent] in place of their signature at the bottom). **If the consent form is printed** (handed out physically), it will be stored safely in safe or secure location based on the advice of my supervisor and the Department of Computer Science.
- Backup: The consent forms will be electronically backed up on an encrypted dark disk.

Audio Recordings (Personally identifiable information):

- Collection: During the interview, audio data will be recorded using a digital recorder. The recordings will be transferred to a laptop via a USB stick. Both the USB stick and the laptop will be encrypted. The recordings will be kept locally (offline) and not uploaded to any cloud storage service (or anywhere online).
- Storage: All recordings will be immediately be transferred to a secure and encrypted disk after the interview and be deleted from the portable recorder. Once the audio recordings are transcribed, they will be deleted from the disk. The transcriptions will be anonymised and stored on the disks.
- Backup: The anonymised transcriptions will be backed up on a secure on an encrypted hard disk.

Generated Token: A token will generated to identify all data collected for each participant (including their consent forms and anonymised interview transcripts). This way, if a participant expresses a desire to withdraw from the study, the data can be deleted from the hard drives upon request. The token will be kept in a separate encrypted hard drive only accessible to me.

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?

A pseudonymisation token will be generated for each participant, which is used to identify all data collected for each participant (including their consent forms, survey responses and anonymised interview transcripts). These tokens will be kept on a separate encrypted hard disk only accessible to me. The token will be used to destroy participant data if they express a desire to withdraw from the study. The token will be destroyed one year after the study has been completed.

Identifiers will be held separately from the research data and linked through a unique study number.

e.) Who will have access to the research data?		
My supervisor (Prof. Ivan Flechais) and I will have access to the research data.		
Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.		
No other entity or organisation will be permitted to access our research data.		
f.) If research data is to be shared with another organisation, how will it be transferred / disclosed securely?		
N/A		
g.) When and how will identifiable data (including audio/video recordings & photos) be destroyed or deleted?		
<b>Note:</b> Records of consent should be retained for a <b>minimum of three years after publication or public release</b> . Some funders may require longer periods (see <a href="http://www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies">http://www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies</a> ). 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.		
Personal data will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 12 months where the personal data will be held. Therefore, the personal data will be held for 12 months.		
h.) Please confirm that you will store <b>other research data</b> safely for at least 3 years after final publication or public release and adhere to <a href="#">any additional research funder policies</a> . For more information about the University policies, please see the University's web pages on <a href="#">research data management</a> .	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
If ' <b>Yes</b> ', please give details of who will store the data and on storage format, location and security. Note that <a href="#">open science</a> is encouraged.		
If ' <b>No</b> ', please provide further details below.		
Other research data will be stored safely in safe or secure location based on the advice of my supervisor and the Department of Computer Science.		
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 " <b>No</b> ", please go to section 19.)	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
j.) Do you have data access agreements for the use of this secondary data? (If so, please attach these.)	Yes <input type="checkbox"/>	No <input type="checkbox"/>
k.) Is your use of this secondary data compatible with what data subjects/participants agreed that their data should be used for?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
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 <input type="checkbox"/>	No <input type="checkbox"/>
<b>19. Publication and dissemination of research data</b>		

<p>How will you disseminate and feedback project outcomes at the end of the research?</p>	<p>The research may be published in academic publications, websites and in the university.</p> <p>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.</p> <p>The research will be written up as a student's thesis.</p> <p>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. If so, the thesis will be openly accessible.</p>
---	---



<b>SECTION C: Methods and procedures to be used</b>	
<b>Method used:</b> Please ensure you have addressed any potential ethical issues related to these methods in Section 14 and in your Participant Information Sheet	<b>Please mark 'X'</b>
1. Analysis of existing records	<input type="checkbox"/>
2. Snowball sampling (recruiting through contacts of existing participants)	<input type="checkbox"/>
3. Use of casual or local workers e.g. interpreters	<input type="checkbox"/>
4. Participant observation	<input type="checkbox"/>
5. Covert observation	<input type="checkbox"/>
6. Observation of specific organisational practices	<input type="checkbox"/>
7. Participant completes questionnaire in hard copy	<input type="checkbox"/>
8. Participant completes online questionnaire or other online task	<input type="checkbox"/>
9. Using social media	<input type="checkbox"/>
10. Participant performs paper and pencil task	<input type="checkbox"/>
11. Participant performs verbal or aural task (e.g. for linguistic study)	<input type="checkbox"/>
12. Focus group	<input type="checkbox"/>
13. Interview	<input checked="" type="checkbox"/>
14. Audio recording of participant (you will generally need specific consent from participants for this)	<input checked="" type="checkbox"/>
15. Video recording of participant (you will generally need specific consent from participants for this)	<input type="checkbox"/>
16. Photography of participant (you will generally need specific consent from participants for this)	<input type="checkbox"/>
17. Others (please specify below)	<input type="checkbox"/>

<b>SECTION D: Professional guidelines and training</b>		
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. <b>Note:</b> this is not an exhaustive list.		<b>Please mark 'X'</b>
<b>Research specialism/ methodology</b>	<b>Association and guidance document</b>	
Anthropology	<a href="#">Association of Social Anthropologists of the UK and Commonwealth</a>	<input type="checkbox"/>
Criminology	<a href="http://www.britsoccrim.org/ethics/">http://www.britsoccrim.org/ethics/</a>	<input type="checkbox"/>
Education	<a href="#">British Educational Research Association Ethical Guidelines for Educational Research</a>	<input type="checkbox"/>
Geography	<a href="#">Association of American Geographers Statement on Professional Ethics</a>	<input type="checkbox"/>
History	<a href="#">Oral History Society of the UK Ethical Guidelines</a>	<input checked="" type="checkbox"/>
Internet-based Research	<a href="#">British Psychological Society: Conducting Research on the Internet</a> <a href="#">Association of Internet Researchers Ethics Guide</a> Also see our <a href="#">Best Practice Guidance on internet-based research</a>	<input checked="" type="checkbox"/>
Law (Socio-Legal)	<a href="#">Socio-Legal Studies Association: Statement of Principles of Ethical Research</a>	<input type="checkbox"/>
Management	<a href="#">Academy of Management's Professional Code of Ethics</a>	<input type="checkbox"/>
Political Science	<a href="#">American Political Science Association (APSA) Guide to Professional Ethics in Political Science</a>	<input type="checkbox"/>
Politics	<a href="#">Political Studies Association. Guidelines for Good Professional Conduct</a>	<input type="checkbox"/>
Psychology	<a href="#">British Psychological Society Code of Ethics and Conduct</a>	<input type="checkbox"/>
Social Research	<a href="#">Social Research Association: Ethical Guidelines</a>	<input checked="" type="checkbox"/>
Sociology	<a href="#">The British Sociological Association: Statement of Ethical Practice</a>	<input type="checkbox"/>
Visual Research	<a href="#">ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research</a>	<input type="checkbox"/>
Other professional guidelines. Please specify the other guidelines used here:		<input type="checkbox"/>
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 <a href="http://researchsupport.admin.ox.ac.uk/support/training/ethics">http://researchsupport.admin.ox.ac.uk/support/training/ethics</a> ), or discussions between researchers and supervisors, if applicable.		
Research Integrity: Arts and Humanities		

**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. <a href="#">Principal investigator</a>	1. <a href="#">Principal investigator</a> (project supervisor)
2. <b>Head of Department (or nominee)</b>	2. <b>Head of Department (or nominee)</b>
	3. <b>Student researcher</b>

**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](mailto:ethics@cs.ox.ac.uk) confirming they've seen and approved the application** .....

**Print name** (block capitals): ..... **Date:** .....

**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](mailto:ethics@cs.ox.ac.uk) from your Oxford address.**

**Print name** (block capitals): GEORGE CHALHOUB **Date:** 28/09/2021

## E.3.2 Information Sheet

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University email address: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### Co-design workshops with users and designers of smart home products

#### PARTICIPANT INFORMATION SHEET

Central University Research Ethics Committee (CUREC) Approval Reference: **CS\_C1A\_21\_037**

**1. Why is this research being conducted?**

The goal of this research project is to investigate how heuristics can improve and address the challenges of data protection in smart home devices.

**2. Why have I been invited to take part?**

You have been invited because you are an adult (aged 18 and above) and have used or designed an IoT device in the past.

**3. Do I have to take part?**

No. You can ask questions about the research before deciding whether or not to take part. If you do agree to take part, you may withdraw yourself from the study at any time, without giving a reason, and without negative consequences, by advising me of this decision. The deadline by which you can withdraw any information you have contributed to the research is 01/11/23. In the event where you withdraw your information, all of the recordings and information collected will be deleted and excluded from the study results.

**4. What will happen to me if I take part in the research?**

If you are happy to take part in the research, you will be asked to attend an interview remotely on Microsoft Teams.

When you arrive, I will talk you through the study procedures and give you the chance to ask any questions.

The interview/session should be between 30 and 45 minutes. You can also ask to pause or stop the interview at any time.

If you are still happy to take part, I will ask you to sign a consent form.

With your consent, I would like to audio record you because for audio recording, I can have an accurate record of your thoughts.

**5. Are there any potential risks in taking part?**

The main potential risk in taking part is a breach of confidentiality. To reduce any potential risks, your interview data will not be directly linked to your name. As you are going along, you can ask the interviewer to ignore or delete anything that you would not like to be kept on record.

**6. Are there any benefits in taking part?**

There will be no direct or personal benefit to you from taking part in this research.

**7. Expenses and payments**

You will receive Amazon voucher (£10 or £15) for your participation in the study.

**8. What happens to the data provided?**

The information you provide during the study is the **research data**. Any research data from which you can be identified (name, signature, audio recording etc.) is known as **personal data**.

**Personal / sensitive data** will be stored for as long as it is needed to conduct the research (with the exception of consent forms, which will be stored for at least 3 years). The time needed to conduct the research is 2 months where the personal data will be held. Therefore, the personal data will be held for 2 months.

**Other research data** (including consent forms) will be stored for at least 3 years after publication or public release of the work of the research.

The researcher and/or supervisor will have access to the research data. Responsible members of the University of Oxford may be given access to data for monitoring and/or audit of the research.

I would like your permission to use direct quotes against a pseudonym in any research outputs.

**9. Will the research be published?**

The research may be published in academic publications, websites and in the university.

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.

The research will be written up as a student's 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. If so, the thesis will be openly accessible.

**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\_037).

**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 George Chalhoub ([george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)), and I will do our best to answer your query. I will acknowledge your concern within 10 working days and give you an indication of how it will be dealt with. If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter as soon as possible:

Chair, **Andrew Martin**; Email: [ethics@cs.ox.ac.uk](mailto:ethics@cs.ox.ac.uk).

**12. Data Protection**

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study.

The University will process your personal data for the purpose of the research outlined above. Research is a task that is performed in the public interest.

Further information about your rights with respect to your personal data is available from <http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/>.

**13. Further Information and Contact Details**

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

George Chalhoub  
Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD  
University email: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

### **E.3.3 Guide to Interview Questions**

George Chalhoub  
DPhil Cyber Security  
Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

#### **GUIDE TO INTERVIEW QUESTIONS**

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_21\_037

Workshop design interactions example:

1. Can you please use the heuristics we provided to design smart home interactions?
2. Can you please tell us what the reasoning behind designing this interaction?
3. Are there other interactions you can use to build these heuristics?
4. Tell us about your experiences using these heuristics?
5. How difficult or easy were these heuristics provided?
6. Can you point to specific obstacles faced when using these heuristics?
7. Is there any way we can improve these heuristics for you?
8. Can you think of other heuristics we can use to design better smart home interactions?

**In the event where interviewees overshare information (highly unlikely), it will be erased from the record as soon as possible.**

### E.3.4 Participant Consent Form

15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
DPhil Cyber Security  
Oxford University e-mail: [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

#### PARTICIPANT CONSENT FORM

Central University Research Ethics Committee (CUREC) Approval Reference: CS\_C1A\_21\_037

#### Co-design workshops with users and designers of smart home products

Purpose of Study: We are investigating how heuristics can improve and address the challenges of data protection in smart home devices.

Please read the following. If you agree with the points below, tick each box and sign the form.

- |    |  | <i>Please initial each box</i> |
|----|--|--------------------------------|
| 1  | I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. | <input type="checkbox"/>       |
| 2  | I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason, and without any adverse consequences or penalty.                                | <input type="checkbox"/>       |
| 3  | I understand that research data collected during the study may be looked at by authorised people outside the research team. I give permission for these individuals to access my data.                 | <input type="checkbox"/>       |
| 4  | I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.                                     | <input type="checkbox"/>       |
| 5  | I understand who will have access to personal data provided, how the data will be stored and what will happen to the data at the end of the project.   | <input type="checkbox"/>       |
| 6  | I understand how this research will be written up and published.   | <input type="checkbox"/>       |
| 7  | I understand how to raise a concern or make a complaint.   | <input type="checkbox"/>       |
| 8  | I consent to being audio recorded.   | <input type="checkbox"/>       |
| 9  | I understand how audio recordings will be used in research outputs.  | <input type="checkbox"/>       |
| 10 | I give permission to be quoted directly in research outputs against a pseudonym.   | <input type="checkbox"/>       |
| 11 | I agree to take part in the study.   | <input type="checkbox"/>       |



Please sign below:

_____	<u>dd / mm / yyyy</u>	_____
Name of Participant	Date	Signature

_____	<u>dd / mm / yyyy</u>	_____
Name of person taking consent	Date	Signature

## E.3.5 Poster Advertisement

Department of Computer Science  
15 Parks Rd, Oxford OX1 3QD



George Chalhoub  
[george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk)

**Co-design workshops with users and designers of smart home products**

Ethics Approval Reference: CS\_C1A\_21\_037

### **VOLUNTEERS NEEDED FOR A STUDY**

We are investigating how heuristics can improve and address the challenges of data protection in smart home devices.

We are looking for volunteers, aged 18 and above to participate in a design workshop. You would be invited to attend the interview remotely on Microsoft Teams. The session would take about 30-45 minutes of your time. You would be asked to design smart home interactions using heuristics.

If you are interested and would like more information please contact George Chalhoub at the Department of Computer Science, 15 Parks Rd, Oxford OX1 3QD, on [george.chalhoub@pmb.ox.ac.uk](mailto:george.chalhoub@pmb.ox.ac.uk). There is no obligation to take part.

You will be compensated for your time.

Thank you!

## References

- [1] Jitesh Ubrani, Ramon Llamas, and Michael Shirer. *Double-Digit Growth Expected in the Smart Home Market, Says IDC*. Mar. 2019. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS44971219> (visited on 12/21/2019).
- [2] Statista Market Forecast. *Smart Home - United States: Statista Market Forecast*. 2020. URL: <https://www.statista.com/outlook/279/smart-home>.
- [3] Kavi Bains et al. *IoT: the \$1 trillion revenue opportunity*. May 2018. (Visited on 10/08/2019).
- [4] Nick Parker. *Outrage as Amazon device listens to Brits having sex and swearing*. en-GB. July 2019. (Visited on 10/16/2019).
- [5] Michele De Donno et al. “DDoS-capable IoT malwares: Comparative analysis and Mirai investigation”. In: *Security and Communication Networks 2018* (2018).
- [6] Thorin Klosowski. *How to Protect Your Digital Privacy*. en-us. 2019. (Visited on 10/08/2019).
- [7] Parks Associates. *Parks Associates: Privacy concerns increasing among smart home device owners*. Oct. 2019. (Visited on 12/21/2019).
- [8] Isis Chong, Aiping Xiong, and Robert W. Proctor. “Human factors in the privacy and security of the internet of things”. In: *Ergonomics in Design* 27.3 (2019), pp. 5–10.
- [9] Noura Aleisa and Karen Renaud. “Privacy of the Internet of Things: a systematic literature review”. In: *Proceedings of the 50th Hawaii International Conference on System Sciences*. 2017.
- [10] Razvan Nicolescu et al. “State of The Art in IoT-Beyond Economic Value”. In: *London*. (2018).
- [11] Claire Rowland and Martin Charlier. *User Experience Design for the Internet of Things*. O’Reilly Media, 2015.
- [12] Kai Zhao and Lina Ge. “A survey on the internet of things security”. In: *2013 Ninth international conference on computational intelligence and security*. IEEE, 2013, pp. 663–667.
- [13] Paul Dunphy et al. “Understanding the experience-centeredness of privacy and security technologies”. In: *Proceedings of the 2014 New Security Paradigms Workshop*. ACM, 2014, pp. 83–94.
- [14] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. “Needs, affect, and interactive products—Facets of user experience”. In: *Interacting with computers* 22.5 (2010), pp. 353–362.

- [15] Jesse James Garrett. *Elements of user experience, the: user-centered design for the web and beyond*. Pearson Education, 2010.
- [16] Marc Hassenzahl and Noam Tractinsky. “User experience-a research agenda”. In: *Behaviour & information technology* 25.2 (2006), pp. 91–97.
- [17] John McCarthy and Peter Wright. *Technology as experience*. MIT press, 2007.
- [18] Johanna Bergman and Isabelle Johansson. “The user experience perspective of Internet of Things development”. In: (2017).
- [19] Claire Rowland et al. *Designing connected products: UX for the consumer Internet of Things*. " O'Reilly Media, Inc.", 2015.
- [20] 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. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 305–325.
- [21] George Chalhoub et al. “‘It did not give me an option to decline’: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. New York, NY, USA: Association for Computing Machinery, May 2021, pp. 1–16. URL: <https://doi.org/10.1145/3411764.3445691> (visited on 09/02/2021).
- [22] George Chalhoub et al. “Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 2020, pp. 185–204.
- [23] George Chalhoub et al. “Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study”. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA '20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 1–9. URL: <https://doi.org/10.1145/3334480.3382850> (visited on 09/02/2021).
- [24] George Chalhoub and Ivan Flechais. “Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives”. In: *The 25th ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW 2022)* (Nov. 2022), The 25th ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW 2022).
- [25] George Chalhoub. “The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home”. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA '20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 1–6. URL: <https://doi.org/10.1145/3334480.3381436> (visited on 09/02/2021).
- [26] Marc Hassenzahl. “User experience (UX): towards an experiential perspective on product quality.” In: *IHM*. Vol. 8. 2008, pp. 11–15.
- [27] Christopher Alexander. *The timeless way of building*. Vol. 1. New York: Oxford University Press, 1979.

- [28] Ivan Flechais, Cecilia Mascolo, and Martina Angela Sasse. “Integrating security and usability into the requirements and design process”. In: *International Journal of Electronic Security and Digital Forensics* 1.1 (2007). Publisher: Inderscience Publishers, pp. 12–26.
- [29] Abdulaziz Alkussayer. *Towards a secure software development framework based on an integrated engineering process*. Florida Institute of Technology, 2011.
- [30] D. Balfanz et al. “In search of usable security: five lessons from the field”. In: *IEEE Security & Privacy Magazine* (2004).
- [31] Ross Anderson. “Why cryptosystems fail”. In: *Proceedings of the 1st ACM Conference on Computer and Communications Security*. 1993, pp. 215–227.
- [32] Alma Whitten and J. Doug Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” In: *USENIX Security Symposium*. Vol. 348. 1999, pp. 169–184.
- [33] Anne Adams and Martina Angela Sasse. “Users are not the enemy”. In: *Communications of the ACM* 42.12 (1999). Publisher: ACM New York, NY, USA, pp. 40–46.
- [34] Alexander Brostoff. “Improving password system effectiveness.” PhD Thesis. University of London, 2005.
- [35] Sacha Brostoff and M. Angela Sasse. “Are Passfaces more usable than passwords? A field trial investigation”. In: *People and computers XIV—usability or else!* Springer, 2000, pp. 405–424.
- [36] Cynthia Kuo, Sasha Romanosky, and Lorrie Faith Cranor. “Human selection of mnemonic phrase-based passwords”. In: *Proceedings of the second symposium on Usable privacy and security*. 2006, pp. 67–78.
- [37] Susan Wiedenbeck et al. “Authentication using graphical passwords: Effects of tolerance and image choice”. In: *Proceedings of the 2005 symposium on Usable privacy and security*. 2005, pp. 1–12.
- [38] Simson L. Garfinkel and Robert C. Miller. “Johnny 2: a user test of key continuity management with S/MIME and Outlook Express”. In: *Proceedings of the 2005 symposium on Usable privacy and security*. 2005, pp. 13–24.
- [39] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use*. " O’Reilly Media, Inc.", 2005.
- [40] Uwe Jendricke and D. Gerd tom Markotten. “Usability meets security—the identity-manager as your personal security assistant for the internet”. In: *Proceedings 16th Annual Computer Security Applications Conference (ACSAC’00)*. IEEE, 2000, pp. 344–353.
- [41] Ronald Kainda, Ivan Flechais, and A. W. Roscoe. “Usability and security of out-of-band channels in secure device pairing protocols”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 2009, pp. 1–12.
- [42] Ersin Uzun, Kristiina Karvonen, and Nadarajah Asokan. “Usability analysis of secure pairing methods”. In: *International Conference on Financial Cryptography and Data Security*. Springer, 2007, pp. 307–324.

- [43] Alfred Kobsa et al. “Serial hook-ups: a comparative usability study of secure device pairing methods”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 2009, pp. 1–12.
- [44] Majed Alshamari. “A Review of Gaps between Usability and Security/Privacy”. en. In: *International Journal of Communications, Network and System Sciences* 9.10 (Sept. 2016). Number: 10 Publisher: Scientific Research Publishing, pp. 413–429. URL: <http://www.scirp.org/Journal/Paperabs.aspx?paperid=71466> (visited on 03/22/2020).
- [45] Premkumar T. Devanbu and Stuart Stubblebine. “Software engineering for security: a roadmap”. In: *Proceedings of the Conference on The Future of Software Engineering*. ICSE '00. Limerick, Ireland: Association for Computing Machinery, May 2000, pp. 227–239. URL: <https://doi.org/10.1145/336512.336559> (visited on 03/22/2020).
- [46] Andreas Holzinger. “Usability engineering methods for software developers”. In: *Communications of the ACM* 48.1 (Jan. 2005), pp. 71–74. URL: <https://doi.org/10.1145/1039539.1039541> (visited on 03/22/2020).
- [47] Nikhat Parveen, Rizwan Beg, and M. H. Khan. “Integrating security and usability at requirement specification process”. In: *International Journal of Computer Trends and Technology* 10.5 (2014), pp. 236–240.
- [48] Lorrie Faith Cranor and Simson Garfinkel. “Guest Editors’ Introduction: Secure or Usable?” In: *IEEE security & privacy* 2.5 (2004). Publisher: IEEE, pp. 16–18.
- [49] Mary Ellen Zurko and Richard T. Simon. “User-centered security”. In: *Proceedings of the 1996 workshop on New security paradigms*. 1996, pp. 27–33.
- [50] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. “User-centered design”. In: *Bainbridge, W. Encyclopedia of Human-Computer Interaction*. Thousand Oaks: Sage Publications 37.4 (2004), pp. 445–456.
- [51] Dennis Wixon, Karen Holtzblatt, and Stephen Knox. “Contextual design: an emergent view of system design”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1990, pp. 329–336.
- [52] Jakob Nielsen. “Guerrilla HCI: Using discount usability engineering to penetrate the intimidation barrier”. In: *Cost-justifying usability* (1994). Publisher: Academic Press New York, pp. 245–272.
- [53] Richard Rubinstein and Harry Hersh. *The human factor: Designing computer systems for people*. Morgan Kaufmann Publishers Inc., 1987.
- [54] HongHai Shen and Prasun Dewan. “Access control for collaborative environments”. In: *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*. 1992, pp. 51–58.
- [55] Giovanni Iachello and Jason Hong. “End-user privacy in human–computer interaction”. In: *Foundations and Trends® in Human–Computer Interaction* 1.1 (2007). Publisher: Now Publishers, Inc., pp. 1–137.
- [56] William Gaver et al. “Realizing a video environment: EuroPARC’s RAVE system”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 1992, pp. 27–35.

- [57] Michael J. Muller et al. “Privacy, anonymity and interpersonal competition issues identified during participatory design of project management groupware!” In: *ACM SIGCHI Bulletin* 23.1 (1991). Publisher: ACM New York, NY, USA, pp. 82–87.
- [58] Marc Langheinrich. “Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems”. en. In: *Ubicomp 2001: Ubiquitous Computing*. Ed. by Gregory D. Abowd, Barry Brumitt, and Steven Shafer. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001, pp. 273–291.
- [59] Alan D. Smith and Felix Offodile. “Information management of automatic data capture: an overview of technical developments”. In: *Information Management & Computer Security* (2002). Publisher: MCB UP Ltd.
- [60] Don Norman. *The design of everyday things: Revised and expanded edition*. Basic books, 2013.
- [61] Mark S. Ackerman and Scott D. Mainwaring. “Privacy issues and human-computer interaction”. In: *Computer* 27.5 (2005), pp. 19–26.
- [62] Ian Sommerville. “Software documentation”. In: *Software engineering 2* (2001), pp. 143–154.
- [63] Clare-Marie Karat, Carolyn Brodie, and John Karat. “Usability design and evaluation for privacy and security solutions”. In: *Security and usability* (2005). Publisher: O’Reilly, pp. 47–74.
- [64] Lorrie Faith Cranor. “Privacy policies and privacy preferences”. In: *Security and usability* (2005). Publisher: O’Reilly, pp. 447–472.
- [65] Colin Birge. “Enhancing research into usable privacy and security”. In: *Proceedings of the 27th ACM international conference on Design of communication*. ACM, 2009, pp. 221–226.
- [66] Joseph’Jofish’ Kaye. “Self-reported password sharing strategies”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2011, pp. 2619–2622.
- [67] Paul Dunphy, Andreas P. Heiner, and N. Asokan. “A closer look at recognition-based graphical passwords on mobile devices”. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. 2010, pp. 1–12.
- [68] John Vines et al. “The joy of cheques: trust, paper and eighty somethings”. In: *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. 2012, pp. 147–156.
- [69] Paul Dourish and Ken Anderson. “Collective information practice: Exploring privacy and security as social and cultural phenomena”. In: *Human-computer interaction* 21.3 (2006). Publisher: Taylor & Francis, pp. 319–342.
- [70] F. B. Shava and D. Van Greunen. “Factors affecting user experience with security features: A case study of an academic institution in Namibia”. In: *2013 Information Security for South Africa*. 2013, pp. 1–8.
- [71] Niels Raabjerg Mathiasen and Susanne Bødker. “Threats or threads: from usable security to secure experience?” In: *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. ACM, 2008, pp. 283–289.

- [72] Panagiotis Zagouras, Christos Kalloniatis, and Stefanos Gritzalis. “Managing User Experience: Usability and Security in a New Era of Software Supremacy”. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2017, pp. 174–188.
- [73] Lydia Kraus et al. “User experience in authentication research: A Survey”. In: *Proceedings of the PQS (2016)*, pp. 54–58.
- [74] Earl L. Wiener and David C. Nagel. *Human factors in aviation*. Gulf Professional Publishing, 1988.
- [75] Jakob Nielsen. *Usability engineering*. Morgan Kaufmann, 1994.
- [76] Donald A. Norman and Stephen W. Draper. *User Centered System Design; New Perspectives on Human-Computer Interaction*. USA: L. Erlbaum Associates Inc., 1986.
- [77] Christian Kraft. *User experience innovation: User centered design that works*. Apress, 2012.
- [78] Javier A. Bargas-Avila and Kasper Hornbæk. “Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2011, pp. 2689–2698.
- [79] Effie Lai-Chong Law et al. “Understanding, scoping and defining user experience: a survey approach”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2009, pp. 719–728.
- [80] Virpi Roto et al. “User experience white paper: Bringing clarity to the concept of user experience”. In: *Dagstuhl Seminar on Demarcating User Experience*. 2011, p. 12.
- [81] Jenny Preece et al. *Human-computer interaction*. Addison-Wesley Longman Ltd., 1994.
- [82] International Organization for Standardization. *Systems and Software Engineering: Systems and Software Quality Requirements and Evaluation (SQuaRE): Guide to SQuaRE*. ISO/IEC, 2014.
- [83] ISO DIS. “9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems”. In: *International Standardization Organization (ISO).Switzerland (2009)*.
- [84] Don Norman and Jakob Nielsen. “The definition of user experience (UX)”. In: *Nielsen Norman Group Publication 1 (2016)*.
- [85] Peter Brooks and Bjørn Hestnes. “User measures of quality of experience: why being objective and quantitative is important”. In: *IEEE network 24.2 (2010)*. Publisher: IEEE, pp. 8–13.
- [86] Nick Kellingley. “What is the difference between Interaction Design and UX Design?” In: *Interaction Design Foundation (2015)*.
- [87] Rod Stephens. *Beginning software engineering*. John Wiley & Sons, 2015.
- [88] *Manifesto for Agile Software Development*. URL: <http://agilemanifesto.org/> (visited on 03/10/2020).



- [89] Gabriela Jurca, Theodore D. Hellmann, and Frank Maurer. “Integrating Agile and user-centered design: a systematic mapping and review of evaluation and validation studies of Agile-UX”. In: *2014 Agile Conference*. IEEE, 2014, pp. 24–32.
- [90] Marc Hassenzahl. “Experience design: Technology for all the right reasons”. In: *Synthesis lectures on human-centered informatics* 3.1 (2010), pp. 1–95.
- [91] Peter Wright, John McCarthy, and Lisa Meekison. “Making sense of experience”. In: *Funology 2*. Springer, 2018, pp. 315–330.
- [92] Charles S. Carver and Michael F. Scheier. *On the self-regulation of behavior*. Cambridge University Press, 2001.
- [93] Susanne Bødker. “Activity theory as a challenge to systems design”. In: *DAIMI Report Series* 334 (1990).
- [94] Thomas T. Hewett et al. *ACM SIGCHI curricula for human-computer interaction*. ACM, 1992.
- [95] Gilbert Cockton. “Value-centred HCI”. In: *Proceedings of the third Nordic conference on Human-computer interaction*. 2004, pp. 149–160.
- [96] Effie Lai-Chong Law, Paul van Schaik, and Virpi Roto. “Attitudes towards user experience (UX) measurement”. en. In: *International Journal of Human-Computer Studies*. Interplay between User Experience Evaluation and System Development 72.6 (June 2014), pp. 526–541. URL: <http://www.sciencedirect.com/science/article/pii/S1071581913001304> (visited on 03/21/2020).
- [97] *What is Human-Computer Interaction (HCI)?* en. Library Catalog: [www.interaction-design.org](http://www.interaction-design.org). 2018. URL: <https://www.interaction-design.org/literature/topics/human-computer-interaction> (visited on 03/21/2020).
- [98] Colin M. Gray, Erik Stolterman, and Martin A. Siegel. “Reprioritizing the relationship between HCI research and practice: bubble-up and trickle-down effects”. In: *Proceedings of the 2014 conference on Designing interactive systems*. DIS ’14. Vancouver, BC, Canada: Association for Computing Machinery, June 2014, pp. 725–734. URL: <https://doi.org/10.1145/2598510.2598595> (visited on 03/21/2020).
- [99] *Report of the EPSRC Human Computer Interaction Theme Day and Survey*. en. Tech. rep. Engineering and Physical Sciences Research Council, Mar. 2012, p. 31. URL: <https://epsrc.ukri.org/newsevents/pubs/report-of-the-epsrc-human-computer-interaction-theme-day-and-survey/>.
- [100] Erin Friess. “Personas and decision making in the design process: an ethnographic case study”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, May 2012, pp. 1209–1218. URL: <https://doi.org/10.1145/2207676.2208572> (visited on 03/21/2020).
- [101] Elizabeth Goodman. “Delivering design: Performance and materiality in professional interaction design”. PhD Thesis. UC Berkeley, 2013.
- [102] *A dictionary of business and management*. English. OCLC: 277068142. Oxford [England]; New York: Oxford University Press, 2009.

- [103] Richard Morris. *The fundamentals of product design*. Bloomsbury Publishing, 2016.
- [104] Kenneth B. Kahn, George Castellion, and Abbie Griffin. *The PDMA handbook of new product development*. Wiley Hoboken, NJ, 2005.
- [105] Don Koberg and Jim Bagnall. “The Universal Traveler, A Soft-Systems Guide to: Creativity, Problem Solving, and the Process of Reaching Goals.[Revised Edition].” In: (1974). Publisher: ERIC.
- [106] *Presidency of the Council: "Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex,"* Dec. 2015. URL: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.
- [107] Peter Carey. *Data protection: a practical guide to UK and EU law*. Oxford University Press, Inc., 2018.
- [108] Lee A. Bygrave. “Data protection by design and by default: Deciphering the EU’s legislative requirements”. In: *Oslo Law Review* 4.02 (2017), pp. 105–120.
- [109] Information Commissioner Office. *Data protection by design and default*. en. Aug. 2019. 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 02/01/2020).
- [110] Ronald Hes and John Borking. “Privacy Enhancing Technologies: the path to anonymity”. In: *Registratiekamer, The Hague* (2000).
- [111] P. Hustinx. *Privacy by design: delivering the promises. Identity Inf Soc 3 (2): 253–255*. 2010.
- [112] Privacy Commissioners. “Privacy by design resolution”. In: *32nd international conference of data protection and privacy commissioners*. 2010, p. 33.
- [113] Ann Cavoukian. “Privacy by design: The 7 foundational principles”. In: *Information and privacy commissioner of Ontario, Canada* 5 (2009).
- [114] Ann Cavoukian. “Privacy by design in law, policy and practice”. In: *A white paper for regulators, decision-makers and policy-makers* (2011).
- [115] Joanna CS Santos, Katy Tarrit, and Mehdi Mirakhorli. “A catalog of security architecture weaknesses”. In: *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*. IEEE, 2017, pp. 220–223.
- [116] L. Bruce Archer. *Design awareness and planned creativity in industry*. Department of Industry, Trade, Commerce, and the Design Council of Great . . . , 1974.
- [117] Rex Hartson and Pardha S. Pyla. *The UX Book: Process and guidelines for ensuring a quality user experience*. Elsevier, 2012.
- [118] Mattias Arvola. *Interaktionsdesign och UX: om att skapa en god användarupplevelse*. Studentlitteratur AB, 2014.
- [119] C. Forrest. *Ten examples of IoT and big data working well together*. ZDNet, 2015.

- [120] Vance Wilson and Soussan Djasasbi. “Human-computer interaction in health and wellness: Research and publication opportunities”. In: *AIS Transactions on Human-Computer Interaction* 7.3 (2015), pp. 97–108.
- [121] Christian Terwiesch and Karl T. Ulrich. *Innovation tournaments: Creating and selecting exceptional opportunities*. Harvard Business Press, 2009.
- [122] Judy Estrin. “Closing the innovation gap”. In: *Reigniting the spark of creativity in a global economy*. McGrawHill: San Francisco (2009).
- [123] Nora Fronemann and Matthias Peissner. “User experience concept exploration: user needs as a source for innovation”. In: *Proceedings of the 8th nordic conference on human-computer interaction: Fun, fast, foundational*. 2014, pp. 727–736.
- [124] Andreas Sonnleitner et al. “Experimentally Manipulating Positive User Experience Based on the Fulfilment of User Needs”. en. In: *Human-Computer Interaction – INTERACT 2013*. Ed. by Paula Kotzé et al. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013, pp. 555–562.
- [125] Matthew S. O’Hern and Aric Rindfleisch. “Customer co-creation: a typology and research agenda”. In: *Review of marketing research*. Routledge, 2017, pp. 108–130.
- [126] Marc Hassenzahl. “The Thing and I: Understanding the Relationship Between User and Product”. en. In: *Funology 2: From Usability to Enjoyment*. Ed. by Mark Blythe and Andrew Monk. Human-Computer Interaction Series. Cham: Springer International Publishing, 2018, pp. 301–313. URL: [https://doi.org/10.1007/978-3-319-68213-6\\_19](https://doi.org/10.1007/978-3-319-68213-6_19) (visited on 03/18/2020).
- [127] Soussan Djasasbi and Diane Strong. “User Experience-driven Innovation in Smart and Connected Worlds”. In: *AIS Transactions on Human-Computer Interaction* 11.4 (Dec. 2019), pp. 215–231. URL: <https://aisel.aisnet.org/thci/vol11/iss4/2>.
- [128] Donald A. Norman and Roberto Verganti. “Incremental and radical innovation: Design research vs. technology and meaning change”. In: *Design issues* 30.1 (2014). Publisher: MIT Press, pp. 78–96.
- [129] Anu Kankainen. “UCPCD: user-centered product concept design”. In: *Proceedings of the 2003 conference on Designing for user experiences*. 2003, pp. 1–13.
- [130] Christopher R. Wilkinson and Antonella De Angeli. “Applying user centred and participatory design approaches to commercial product development”. In: *Design Studies* 35.6 (2014). Publisher: Elsevier, pp. 614–631.
- [131] Coimbatore K. Prahalad and Venkatram Ramaswamy. “The new frontier of experience innovation”. In: *MIT Sloan management review* 44.4 (2003). Publisher: Massachusetts Institute of Technology, Cambridge, MA, p. 12.
- [132] Virpi Roto et al. “Abstracts Collection–Demarcating User eXperience”. In: *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2011.
- [133] Youngsoo Shin et al. “Design for experience innovation: understanding user experience in new product development”. In: *Behaviour & Information Technology* 36.12 (2017). Publisher: Taylor & Francis, pp. 1218–1234.
- [134] Florian Schaub et al. “A design space for effective privacy notices”. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015*. 2015, pp. 1–17.

- [135] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. “Is your inseam a biometric? a case study on the role of usability studies in developing public policy”. In: *Proc. USEC 14* (2014).
- [136] Lorrie Faith Cranor. “Necessary but not sufficient: Standardized mechanisms for privacy notice and choice”. In: *J. on Telecomm. & High Tech. L.* 10 (2012), p. 273.
- [137] Carlos Jensen and Colin Potts. “Privacy policies as decision-making tools: an evaluation of online privacy notices”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '04. New York, NY, USA: Association for Computing Machinery, Apr. 2004, pp. 471–478. URL: <https://doi.org/10.1145/985692.985752> (visited on 05/06/2021).
- [138] Huiqing Fu et al. “A field study of run-time location access disclosures on android smartphones”. In: *Proc. USEC 14* (2014).
- [139] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. “User interfaces for privacy agents”. In: *ACM Transactions on Computer-Human Interaction* 13.2 (June 2006), pp. 135–178. URL: <https://doi.org/10.1145/1165734.1165735> (visited on 05/06/2021).
- [140] Patrick Gage Kelley et al. “Standardizing privacy notices: an online study of the nutrition label approach”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '10. New York, NY, USA: Association for Computing Machinery, Apr. 2010, pp. 1573–1582. URL: <https://doi.org/10.1145/1753326.1753561> (visited on 05/06/2021).
- [141] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. “Privacy as part of the app decision-making process”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13. New York, NY, USA: Association for Computing Machinery, Apr. 2013, pp. 3393–3402. URL: <https://doi.org/10.1145/2470654.2466466> (visited on 05/06/2021).
- [142] Marc Langheinrich. “A Privacy Awareness System for Ubiquitous Computing Environments”. en. In: *UbiComp 2002: Ubiquitous Computing*. Ed. by Gaetano Borriello and Lars Erik Holmquist. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2002, pp. 237–245.
- [143] *W3C Tracking Protection Working Group*. 2011. URL: <https://www.w3.org/2011/tracking-protection/> (visited on 05/06/2021).
- [144] Federal Trade Commission. “Internet of things: Privacy & security in a connected world”. In: *Washington, DC: Federal Trade Commission* (2015).
- [145] Tony Vila, Rachel Greenstadt, and David Molnar. “Why we can’t be bothered to read privacy policies models of privacy economics as a lemons market”. In: *Proceedings of the 5th international conference on Electronic commerce*. ICEC '03. New York, NY, USA: Association for Computing Machinery, Sept. 2003, pp. 403–407. URL: <https://doi.org/10.1145/948005.948057> (visited on 05/06/2021).
- [146] Jens Grossklags and Nathan Good. “Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers”. en. In: *Financial Cryptography and Data Security*. Ed. by Sven Dietrich and Rachna Dhamija. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007, pp. 341–355.

- [147] Oksana Kulyk et al. “this website uses cookies”: Users’ perceptions and reactions to the cookie disclaimer”. In: *European Workshop on Usable Security (EuroUSEC)*. 2018.
- [148] Rainer Böhme and Stefan Köpsell. “Trained to accept? a field experiment on consent dialogs”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’10. New York, NY, USA: Association for Computing Machinery, Apr. 2010, pp. 2403–2406. URL: <https://doi.org/10.1145/1753326.1753689> (visited on 05/06/2021).
- [149] Adrienne Porter Felt et al. “How to Ask for Permission.” In: *HotSec 12* (2012), pp. 7–7.
- [150] Dominique Machuletz and Rainer Böhme. “Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR”. In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 481–498. URL: <https://doi.org/10.2478/popets-2020-0037>.
- [151] Victor Dahl and Marco Österlin. *Impact of GDPR on Data Sharing Behavior of Smart Home Users*. eng. Malmö universitet/Teknik och samhälle, 2020. URL: <http://urn.kb.se/resolve?urn=urn:nbn:se:mau:diva-20336> (visited on 08/30/2021).
- [152] Avirup Dasgupta, Asif Qumer Gill, and Farookh Hussain. “Privacy of IoT-enabled smart home systems”. In: *Internet of Things (IoT) for automated and smart applications*. IntechOpen, 2019.
- [153] Daniel Bastos et al. “GDPR privacy implications for the Internet of Things”. In: *4th Annual IoT Security Foundation Conference*. Vol. 4. 2018, pp. 1–8.
- [154] Dean Ivancevic. *Privacy and security of IoT : A smart home perspective*. eng. 2020. URL: <http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-99071> (visited on 08/30/2021).
- [155] Lachlan Urquhart and Jiahong Chen. *On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity*. en. SSRN Scholarly Paper ID 3629119. Rochester, NY: Social Science Research Network, June 2020. URL: <https://papers.ssrn.com/abstract=3629119> (visited on 08/30/2021).
- [156] Olga Gkotsopoulou et al. “Data Protection by Design for cybersecurity systems in a Smart Home environment”. In: *2019 IEEE Conference on Network Softwarization (NetSoft)*. June 2019, pp. 101–109.
- [157] 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.
- [158] Lachlan Urquhart and Jiahong Chen. “Stuck in The Middle With U (Sers): Domestic Data Controllers & Demonstrations of Accountability in Smart Homes”. In: *ETHICOMP 2020* (2020), p. 211.
- [159] Joseph Galen Lindley et al. “Anticipating GDPR in Smart Homes Through Fictional Conversational Objects”. In: (2017).
- [160] Sahar Allegue, Mouna Rhahla, and Takoua Abdellatif. “Toward gdpr compliance in iot systems”. In: *International Conference on Service-Oriented Computing*. Springer, 2019, pp. 130–141.

- [161] Beth Hutchens, Gavin Keene, and David Stieber. “Regulating the Internet of Things: Protecting the “Smart” Home”. In: (2017). Publisher: University of Washington Technology Law and Public Policy Clinic.
- [162] Eoghan Furey and Juanita Blue. “Can i trust her? Intelligent personal assistants and GDPR”. In: *2019 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2019, pp. 1–6.
- [163] Max-R. Ulbricht and Frank Pallas. “YaPPL - A Lightweight Privacy Preference Language for Legally Sufficient and Automated Consent Provision in IoT Scenarios”. en. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Ed. by Joaquin Garcia-Alfaro et al. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 329–344.
- [164] Christine Utz et al. “(Un)informed Consent: Studying GDPR Consent Notices in the Field”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 973–990. URL: <https://doi.org/10.1145/3319535.3354212> (visited on 04/28/2021).
- [165] Vincenzo Mangini, Irina Tal, and Arghir-Nicolae Moldovan. “An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective”. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. ARES ’20. New York, NY, USA: Association for Computing Machinery, Aug. 2020, pp. 1–9. URL: <https://doi.org/10.1145/3407023.3407080> (visited on 03/25/2021).
- [166] Daniel Anderson and Richard von Seck. “The GDPR and its impact on the web”. In: *Network 1* (2020).
- [167] Martin Degeling et al. “We value your privacy... now take some cookies: Measuring the GDPR’s impact on web privacy”. In: *arXiv preprint arXiv:1808.05096* (2018).
- [168] Christoph Bösch et al. “Tales from the dark side: Privacy dark strategies and privacy dark patterns”. In: *Proceedings on Privacy Enhancing Technologies 2016.4* (2016), pp. 237–254.
- [169] Gregory Conti and Edward Sobiesk. “Malicious interface design: exploiting the user”. In: *Proceedings of the 19th international conference on World wide web*. WWW ’10. New York, NY, USA: Association for Computing Machinery, Apr. 2010, pp. 271–280. URL: <https://doi.org/10.1145/1772690.1772719> (visited on 05/06/2021).
- [170] Colin M. Gray et al. “The Dark (Patterns) Side of UX Design”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI ’18. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–14. URL: <https://doi.org/10.1145/3173574.3174108> (visited on 05/06/2021).
- [171] Arunesh Mathur et al. “Dark patterns at scale: Findings from a crawl of 11K shopping websites”. In: *Proceedings of the ACM on Human-Computer Interaction 3*. CSCW (2019), pp. 1–32.
- [172] Norwegian Consumer Council. “Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy”. In: *Norwegian Consumer Council Report* (2018).

- [173] *EDPS Opinion on the legislative package 'A New Deal for Consumers'*. Tech. rep. Oct. 2018. URL: [https://edps.europa.eu/sites/edp/files/publication/18-10-05\\_opinion\\_consumer\\_law\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf).
- [174] 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 05/06/2021).
- [175] Midas Nouwens et al. “Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI ’20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 1–13. URL: <https://doi.org/10.1145/3313831.3376321> (visited on 05/06/2021).
- [176] James Vincent. *California bans ‘dark patterns’ that trick users into giving away their personal data*. en. Mar. 2021. URL: <https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data> (visited on 05/06/2021).
- [177] David Parkins. “The world’s most valuable resource is no longer oil, but data”. In: *The economist* 6 (2017).
- [178] Marc van Lieshout. “The value of personal data”. In: *IFIP International Summer School on Privacy and Identity Management*. Springer, 2014, pp. 26–38.
- [179] Lujo Bauer et al. *An Introduction to Privacy for Technology Professionals*. en. Google-Books-ID: aubIygEACAAJ. International Association of Privacy Professionals, 2020.
- [180] Stacy-Ann Elvy. “Paying for privacy and the personal data economy”. In: *Colum. L. Rev.* 117 (2017), p. 1369.
- [181] C. Kalapesi. “Unlocking the value of personal data: From collection to usage”. In: *World Economic Forum technical report*. 2013.
- [182] Klaus Schwab et al. “Personal data: The emergence of a new asset class”. In: *An Initiative of the World Economic Forum*. 2011.
- [183] John Deighton and Peter A. Johnson. “The Value of Data: Consequences for insight, innovation and efficiency in the US economy”. In: *Data-Driven Marketing Institute* 14 (2013), pp. 1–105.
- [184] Kenneth C. Laudon. “Markets and privacy”. In: *Communications of the ACM* 39.9 (1996). Publisher: ACM New York, NY, USA, pp. 92–104.
- [185] Nicole Lindsey. *Personal Data Marketplaces Might Not Be the Best Solution for Data Privacy*. en-US. Section: Data Privacy. Apr. 2019. URL: <https://www.cpomagazine.com/data-privacy/personal-data-marketplaces-might-not-be-the-best-solution-for-data-privacy/> (visited on 05/05/2021).
- [186] Sarah Spiekermann et al. “The challenges of personal data markets and privacy”. In: *Electronic markets* 25.2 (2015), pp. 161–167.

- [187] 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), pp. 65–86. URL: <https://doi.org/10.1080/13600869.2019.1631621> (visited on 05/05/2021).
- [188] Jeffrey Ritter and Anna Mayer. “Regulating data as property: a new construct for moving forward”. In: *Duke L. & Tech. Rev.* 16 (2017), p. 220.
- [189] Mark MacCarthy. *Privacy Is Not A Property Right In Personal Information*. en. Nov. 2018. URL: <https://www.forbes.com/sites/washingtonbytes/2018/11/02/privacy-is-not-a-property-right-in-personal-information/> (visited on 05/05/2021).
- [190] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. “The economics of privacy”. In: *Journal of Economic Literature* 54.2 (2016), pp. 442–92.
- [191] Cameron F. Kerry and John B. Morris. “Why Data Ownership Is the Wrong Approach to Protecting Privacy”. In: *Brookings Institution, June 26* (2019).
- [192] Avi Goldfarb and Catherine E. Tucker. “Online advertising, behavioral targeting, and privacy”. In: *Communications of the ACM* 54.5 (2011), pp. 25–27.
- [193] OECD. “Exploring the economics of personal data”. In: *OECD Digital Economy Papers 220* (2013). Publisher: Paris, France: OECD.
- [194] Stefan Berthold and Rainer Böhme. “Valuating privacy with option pricing theory”. In: *Economics of information security and privacy*. Springer, 2010, pp. 187–209.
- [195] Alessandro Acquisti, Leslie K. John, and George Loewenstein. “What is privacy worth?” In: *The Journal of Legal Studies* 42.2 (2013). Publisher: University of Chicago Press Chicago, IL, pp. 249–274.
- [196] Jens Grossklags and Alessandro Acquisti. “When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.” In: *WEIS*. 2007.
- [197] Michael Lesk. “The Price of Privacy”. In: *IEEE Security Privacy* 10.5 (Sept. 2012). Conference Name: IEEE Security Privacy, pp. 79–81.
- [198] Nicola Jentzsch, Sören Preibusch, and Andreas Harasser. “Study on monetising privacy: An economic model for pricing personal information”. In: *ENISA, Feb 1.1* (2012).
- [199] Alessandro Acquisti. “Privacy in electronic commerce and the economics of immediate gratification”. In: *Proceedings of the 5th ACM conference on Electronic commerce*. 2004, pp. 21–29.
- [200] Jatinder Singh et al. “Twenty security considerations for cloud-supported Internet of Things”. In: *IEEE Internet of things Journal* 3.3 (2015), pp. 269–284.
- [201] D. Bastos, M. Shackleton, and F. El-Moussa. “Internet of things: A survey of technologies and security risks in smart home and city environments”. In: (2018).
- [202] Manos Antonakakis et al. “Understanding the mirai botnet”. In: *26th USENIX Security Symposium (USENIX Security 17)*. 2017, pp. 1093–1110.



- [203] Antonio José Vielma Berkeley Lovelace Jr. *Friday's third cyberattack on Dyn 'has been resolved,' company says*. en. Vol. 2019. May 19, 2016. URL: <https://www.cnn.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html>.
- [204] Irina Brass et al. "Regulating IoT: enabling or disabling the capacity of the Internet of Things?" In: *Risk & Regulation* 33 (2017), pp. 12–15.
- [205] *SB-327 Information privacy: connected devices*. Vol. 1798.91.04. 2018. URL: [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180SB327](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327).
- [206] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges". In: *Security and Communication Networks* 7.12 (2014), pp. 2728–2742.
- [207] Abbas Acar et al. "Peek-a-Boo: I see your smart home activities, even encrypted!" In: *arXiv preprint arXiv:1808.02741* (2018).
- [208] Steven I. Friedland. "Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy". In: *W. Va.L.Rev.* 119 (2016), p. 891.
- [209] Michael Onuoha Thomas, Beverly Amunga Onyimbo, and Rajasvaran Logeswaran. "Usability evaluation criteria for internet of things". In: *Int J Inf Technol Comput Sci* 8 (2016), pp. 10–18.
- [210] Jonathan Follett. *Designing for emerging technologies: UX for genomics, robotics, and the internet of things*. " O'Reilly Media, Inc.", 2014.
- [211] Ali Asghar Nazari Shirehjini and Azin Semsar. "Human interaction with IoT-based smart environments". In: *Multimedia Tools and Applications* 76.11 (2017), pp. 13343–13365.
- [212] Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey". In: *Computer networks* 54.15 (2010), pp. 2787–2805.
- [213] Timo Jokela. "Assessments of usability engineering processes: experiences from experiments". In: *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 2003, 9–pp.
- [214] Rosa Yáñez Gómez, Daniel Cascado Caballero, and José-Luis Sevillano. "Heuristic evaluation on mobile interfaces: A new checklist". In: *The Scientific World Journal* 2014 (2014).
- [215] Eun Kyoung Choe et al. "Investigating receptiveness to sensing and inference in the home using sensor proxies". In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. UbiComp '12. Pittsburgh, Pennsylvania: Association for Computing Machinery, Sept. 2012, pp. 61–70. URL: <https://doi.org/10.1145/2370216.2370226> (visited on 03/29/2020).
- [216] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. "Benefits and risks of smart home technologies". In: *Energy Policy* 103 (2017), pp. 72–83.
- [217] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. "Smart homes and their users: a systematic analysis and key challenges". In: *Personal and Ubiquitous Computing* 19.2 (2015), pp. 463–476.

- [218] Meredydd Williams, Jason RC 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)*. IEEE, 2017, pp. 181–18109.
- [219] Eric Zeng, Shrirang Mare, and Franziska Roesner. “End user security and privacy concerns with smart homes”. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 2017, pp. 65–80.
- [220] Alessandro Montanari et al. “Understanding the Privacy Design Space for Personal Connected Objects”. In: (July 2016). Publisher: BCS Learning & Development. URL: <https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/HCI2016.18> (visited on 03/10/2020).
- [221] Noah Apthorpe et al. “Discovering smart home internet of things privacy norms using contextual integrity”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2.2* (2018), p. 59.
- [222] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. “More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019.
- [223] Nathan Malkin et al. “Privacy Attitudes of Smart Speaker Users”. In: *Proceedings on Privacy Enhancing Technologies 2019.4* (2019), pp. 250–271.
- [224] Nathan Malkin et al. ““What Can’t Data Be Used For?” Privacy Expectations about Smart TVs in the US”. In: *European Workshop on Usable Security (Euro USEC)*. 2018.
- [225] Pardis Emami Naeini et al. “Privacy expectations and preferences in an IoT world”. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 2017, pp. 399–412.
- [226] Kopo Marvin Ramokapane et al. “Privacy Design Strategies for Home Energy Management Systems (HEMS)”. 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. 1–15. URL: <https://doi.org/10.1145/3491102.3517515> (visited on 07/20/2022).
- [227] Hosub Lee and Alfred Kobsa. “Understanding user privacy in Internet of Things environments”. In: *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 2016, pp. 407–412.
- [228] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. “Exploring consumers’ attitudes of smart TV related privacy risks”. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2017, pp. 656–674.
- [229] Noah Apthorpe, Dillon Reisman, and Nick Feamster. “A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic”. In: *arXiv preprint arXiv:1705.06805* (2017).
- [230] Christine Geeng and Franziska Roesner. “Who’s In Control?: Interactions In Multi-User Smart Homes”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, p. 268.

- [231] Anupam Das et al. “Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications”. In: *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, 2017, pp. 1387–1396.
- [232] Jessica Groopman and Susan Etlinger. “Consumer perceptions of privacy in the Internet of Things: What brands can learn from a concerned citizenry”. In: *Altimeter Group: San Francisco, CA, USA* (2015), pp. 1–25.
- [233] 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.
- [234] Helen Nissenbaum. “A contextual approach to privacy online”. In: *Daedalus* 140.4 (2011), pp. 32–48.
- [235] *Citizen Perspectives on the Customization/Privacy Paradox Related to Smart Meter Implementation: Security & Forensics Journal Article | IGI Global*. URL: <https://www.igi-global.com/article/citizen-perspectives-on-the-customizationprivacy-paradox-related-to-smart-meter-implementation/124867> (visited on 03/10/2020).
- [236] Lesa Lorenzen-Huber et al. “Privacy, technology, and aging: a proposed framework”. In: *Ageing International* 36.2 (2011), pp. 232–252.
- [237] Alison Burrows, David Coyle, and Rachael Goberman-Hill. “Privacy, boundaries and smart homes for health: An ethnographic study”. In: *Health & place* 50 (2018), pp. 112–118.
- [238] Marshini Chetty et al. “Who’s hogging the bandwidth: the consequences of revealing the invisible in the home”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’10. Atlanta, Georgia, USA: Association for Computing Machinery, Apr. 2010, pp. 659–668. URL: <https://doi.org/10.1145/1753326.1753423> (visited on 03/29/2020).
- [239] Weijia He et al. “Rethinking Access Control and Authentication for the Home Internet of Things (IoT)”. en. In: 2018, pp. 255–272. URL: <https://www.usenix.org/conference/usenixsecurity18/presentation/he> (visited on 09/02/2021).
- [240] Franziska Roesner et al. “Augmented reality: Hard problems of law and policy”. In: *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: adjunct publication*. 2014, pp. 1283–1288.
- [241] Yaxing Yao et al. “Privacy Perceptions and Designs of Bystanders in Smart Homes”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019), 59:1–59:24. URL: <https://doi.org/10.1145/3359161> (visited on 09/02/2021).
- [242] Julia Bernd et al. “Smart Home Bystanders: Further Complexifying a Complex Context”. In: ().
- [243] Irum Rauf et al. “Influences of developers’ perspectives on their engagement with security in code”. In: *Proceedings of the 15th International Conference on Cooperative and Human Aspects of Software Engineering*. CHASE ’22. New York, NY, USA: Association for Computing Machinery, May 2022, pp. 86–95. URL: <https://doi.org/10.1145/3528579.3529180> (visited on 08/30/2022).

- [244] Partha Das Chowdhury et al. “Developers Are Neither Enemies Nor Users: They Are Collaborators”. In: *2021 IEEE Secure Development Conference (SecDev)*. Oct. 2021, pp. 47–55.
- [245] Dirk van der Linden et al. “Schrödinger’s Security: Opening the Box on App Developers’ Security Rationale”. In: *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)*. ISSN: 1558-1225. Oct. 2020, pp. 149–160.
- [246] Charles Weir, Awais Rashid, and James Noble. “How to Improve the Security Skills of Mobile App Developers? Comparing and Contrasting Expert Views”. en. In: 2016. URL: <https://www.usenix.org/conference/soups2016/workshop-program/wsiw16/presentation/weir> (visited on 08/30/2022).
- [247] Charles Weir, Awais Rashid, and James Noble. *Developer Essentials: Top Five Interventions to Support Secure Software Development*. en. Lancaster: Lancaster University, Mar. 2017. URL: <https://eprints.lancs.ac.uk/id/eprint/85933/> (visited on 08/30/2022).
- [248] Awais Rashid. “Developer-Centred Security”. en. In: *Encyclopedia of Cryptography, Security and Privacy*. Ed. by Sushil Jajodia, Pierangela Samarati, and Moti Yung. Berlin, Heidelberg: Springer, 2019, pp. 1–3. URL: [https://doi.org/10.1007/978-3-642-27739-9\\_1578-1](https://doi.org/10.1007/978-3-642-27739-9_1578-1) (visited on 08/30/2022).
- [249] Kenneth A. Bamberger and Deirdre K. Mulligan. “Privacy on the Books and on the Ground”. In: *Stan. L. Rev.* 63 (2010), p. 247.
- [250] Ari Ezra Waldman. “Designing Without Privacy”. In: *Hous. L. Rev.* 55 (2017), p. 659.
- [251] Daniel Greene and Katie Shilton. “Platform privacies: Governance, collaboration, and the different meanings of “privacy” in iOS and Android development:” en. In: *New Media & Society* (Apr. 2017). Publisher: SAGE PublicationsSage UK: London, England. URL: <https://journals.sagepub.com/doi/10.1177/1461444817702397> (visited on 03/24/2020).
- [252] Katie Shilton and Daniel Greene. “Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development”. en. In: *Journal of Business Ethics* 155.1 (Mar. 2019), pp. 131–146. URL: <https://doi.org/10.1007/s10551-017-3504-8> (visited on 03/24/2020).
- [253] 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: <https://doi.org/10.1007/s11948-016-9754-5> (visited on 01/19/2020).
- [254] Nikhil Patnaik, Joseph Hallett, and Awais Rashid. “Usability Smells: An Analysis of {Developers’} Struggle With Crypto Libraries”. en. In: 2019, pp. 245–257. URL: <https://www.usenix.org/conference/soups2019/presentation/patnaik> (visited on 07/20/2022).
- [255] Charles Weir et al. “Promoting Developer Security: ACM/IEEE International Conference on Software Engineering”. In: May 2019.

- [256] Irum Rauf et al. “Security but not for security’s sake: The impact of social considerations on app developers’ choices”. In: *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. New York, NY, USA: Association for Computing Machinery, June 2020, pp. 141–144. URL: <https://doi.org/10.1145/3387940.3392230> (visited on 07/20/2022).
- [257] Hala Assal and Sonia Chiasson. “Security in the software development lifecycle”. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS) 2018*. 2018, pp. 281–296.
- [258] Tayyaba Nafees et al. “Idea-caution before exploitation: the use of cybersecurity domain knowledge to educate software engineers against software vulnerabilities”. In: *International Symposium on Engineering Secure Software and Systems*. Springer, 2017, pp. 133–142.
- [259] Tayyaba Nafees et al. “Vulnerability anti-patterns: a timeless way to capture poor software practices (vulnerabilities)”. In: *Proceedings of the 24th Conference on Pattern Languages of Programs*. The Hillside Group, 2017, p. 23.
- [260] Tyler W Thomas et al. “Security during application development: An application security expert perspective”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 2018, pp. 1–12.
- [261] Norbert Nthala and Ivan Flechais. “Informal support networks: an investigation into home data security practices”. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 2018, pp. 63–82.
- [262] Eric Zeng and Franziska Roesner. “Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study”. In: *28th USENIX Security Symposium (USENIX Security 19)*. 2019, pp. 159–176.
- [263] Serena Zheng et al. “User perceptions of smart home IoT privacy”. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), p. 200.
- [264] Jeungmin Oh and Uichin Lee. “Exploring UX issues in Quantified Self technologies”. In: *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*. Jan. 2015, pp. 53–59.
- [265] Johanna Bergman et al. “An exploratory study on how Internet of Things developing companies handle User Experience Requirements”. In: *International Working Conference on Requirements Engineering: Foundation for Software Quality*. Springer, 2018, pp. 20–36.
- [266] Claire Rowland. *UX AND SERVICE DESIGN FOR CONNECTED PRODUCTS*. en. June 2018. URL: <https://iotuk.org.uk/wp-content/uploads/2018/06/UX-and-Service-Design-IoTUK.pdf>.
- [267] William T. Riley et al. “Health behavior models in the age of mobile interventions: are our theories up to the task?” In: *Translational behavioral medicine* 1.1 (2011). Publisher: Oxford University Press, pp. 53–71.
- [268] Paschal Sheeran, William MP Klein, and Alexander J. Rothman. “Health behavior change: Moving from observation to intervention”. In: *Annual review of psychology* 68 (2017). Publisher: Annual Reviews, pp. 573–600.

- [269] Marc Pallot, Kulwant Pawar, and Roberto Santoro. “A user experience framework and model within experiential living labs for Internet of Things”. In: *2013 International Conference on Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference*. IEEE, 2013, pp. 1–15.
- [270] Marc Pallot. “The living lab approach: A user centred open innovation ecosystem”. In: *Webergence Blog* 2010 (2009).
- [271] Idris Jahn. *IoT: Risk or Reward?* English. Feb. 2016. URL: [https://www.webroot.com/blog/wp-content/uploads/2016/02/IoT\\_Risk-or-Reward.pdf](https://www.webroot.com/blog/wp-content/uploads/2016/02/IoT_Risk-or-Reward.pdf).
- [272] Jay F. Nunamaker, Minder Chen, and Titus D.M. Purdin. “Systems Development in Information Systems Research”. In: *Journal of Management Information Systems* 7.3 (Dec. 1990), pp. 89–106. URL: <https://doi.org/10.1080/07421222.1990.11517898> (visited on 03/22/2022).
- [273] Norbert Nthala. “Home data security decisions”. en. <http://purl.org/dc/dcmitype/Text>. University of Oxford, 2019. URL: <https://ora.ox.ac.uk/objects/uuid:72401f07-d923-4448-af20-f99ecb677e3a> (visited on 10/25/2021).
- [274] Farm Credit Administration. “FCA Essential Practices for Information Technology Based on Industry Standards and FFIEC Examination Guidance”. In: (Oct. 2017). URL: <https://www.fca.gov/template-fca/download/ITManual/itsystemsdevelopment.pdf> (visited on 03/23/2022).
- [275] Bill Curtis. “Introduction to empirical research on the design process in MCC’s software technology program”. In: *Empirical Studies of the Design Process: Papers for the Second Workshop on Empirical Studies of Programmers*. 1987, pp. 1–4.
- [276] Alan McIntosh and Jennifer Pontius. “Chapter 1 - Tools and Skills”. en. In: *Science and the Global Environment*. Ed. by Alan McIntosh and Jennifer Pontius. Boston: Elsevier, Jan. 2017, pp. 1–112. URL: <https://www.sciencedirect.com/science/article/pii/B9780128017128000019> (visited on 03/23/2022).
- [277] Ben Shneiderman et al. “Designing the User Interface: Strategies for Effective Human-Computer Interaction, 6th Edition”. In: *CCE Faculty Books and Book Chapters* (Apr. 2016). URL: [https://nsuworks.nova.edu/gscis\\_facbooks/18](https://nsuworks.nova.edu/gscis_facbooks/18).
- [278] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. en. Google-Books-ID: hbkdDQAAQBAJ. Morgan Kaufmann, Apr. 2017.
- [279] Joseph Check and Russell K. Schutt. *Research Methods in Education*. en. Google-Books-ID: nSWYAAAAQBAJ. SAGE Publications, Oct. 2011.
- [280] Julie Ponto. “Understanding and Evaluating Survey Research”. In: *Journal of the Advanced Practitioner in Oncology* 6.2 (2015), pp. 168–171. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4601897/> (visited on 03/23/2022).
- [281] KATE KELLEY et al. “Good practice in the conduct and reporting of survey research”. In: *International Journal for Quality in Health Care* 15.3 (May 2003), pp. 261–266. URL: <https://doi.org/10.1093/intqhc/mzg031> (visited on 03/23/2022).

- [282] 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 (2009). \_eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1745-6606.2009.01148.x>, pp. 449–473. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2009.01148.x> (visited on 03/23/2022).
- [283] Wm Arthur Conklin. “Computer security behaviors of home PC users: A diffusion of innovation approach”. English. ISBN: 9780542809019. Ph.D. United States – Texas: The University of Texas at San Antonio. URL: <https://www.proquest.com/docview/304915755/abstract/58E88C6108EE442APQ/1> (visited on 03/23/2022).
- [284] Floyd J. Fowler Jr. *Survey Research Methods*. en. Google-Books-ID: WM11AwAAQBAJ. SAGE Publications, Sept. 2013.
- [285] Marilyn L. Taylor and Mikael Søndergaard. *Unraveling the Mysteries of Case Study Research: A Guide for Business and Management Students*. en. Google-Books-ID: a2EsDwAAQBAJ. Edward Elgar Publishing, July 2017.
- [286] Geoff Rolls, ed. *Classic Case Studies in Psychology: Fourth Edition*. 4th ed. London: Routledge, Dec. 2019.
- [287] Robert K. Yin. *Case study research and applications*. Sage, 2018.
- [288] Izak Benbasat, David K. Goldstein, and Melissa Mead. “The Case Research Strategy in Studies of Information Systems”. In: *MIS Quarterly* 11.3 (1987). Publisher: Management Information Systems Research Center, University of Minnesota, pp. 369–386. URL: <https://www.jstor.org/stable/248684> (visited on 03/23/2022).
- [289] Dennis Basil Bromley and Bromley Dennis Basil. *The case-study method in psychology and related disciplines*. John Wiley & Sons, 1986.
- [290] A. Milton Jenkins. “Research methodologies and MIS research”. In: *Research methods in information systems* 2.1 (1985). Publisher: Elsevier Science Publishers BV, Amsterdam, Holland, pp. 103–117.
- [291] Gideon Sjoberg, Anthony M. Orum, and Joe R. Feagin. *A Case for the Case Study*. Chapel Hill: The University of North Carolina Press, 2020. URL: <https://muse.jhu.edu/book/77227> (visited on 03/23/2022).
- [292] Albert J. Mills, Gabrielle Durepos, and Elden Wiebe. *Encyclopedia of Case Study Research*. en. Google-Books-ID: XMJ1AwAAQBAJ. SAGE Publications, Oct. 2009.
- [293] Dictionary.com. *Definition of ethnography | Dictionary.com*. en. 2022. URL: <https://www.dictionary.com/browse/ethnography> (visited on 03/23/2022).
- [294] Hugh Gusterson. “Ethnographic research”. In: *Qualitative methods in international relations*. Springer, 2008, pp. 93–113.

- [295] Mayukh Dewan. “Understanding Ethnography: An ‘Exotic’ Ethnographer’s Perspective”. en. In: *Asian Qualitative Research in Tourism: Ontologies, Epistemologies, Methodologies, and Methods*. Ed. by Paolo Mura and Catheryn Khoo-Lattimore. Perspectives on Asian Tourism. Singapore: Springer, 2018, pp. 185–203. URL: [https://doi.org/10.1007/978-981-10-7491-2\\_10](https://doi.org/10.1007/978-981-10-7491-2_10) (visited on 03/23/2022).
- [296] 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, a1020. URL: <https://www.bmj.com/content/337/bmj.a1020> (visited on 03/23/2022).
- [297] Mike Allen. *The SAGE Encyclopedia of Communication Research Methods*. en. Google-Books-ID: 81B5DQAAQBAJ. SAGE Publications, Jan. 2017.
- [298] Kim Salazar. *Diary Studies: Understanding Long-Term User Behavior and Experiences*. en. June 2016. URL: <https://www.nngroup.com/articles/diary-studies/> (visited on 03/23/2022).
- [299] Eiji Hayashi and Jason Hong. “A diary study of password usage in daily life”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’11. New York, NY, USA: Association for Computing Machinery, May 2011, pp. 2627–2630. URL: <https://doi.org/10.1145/1978942.1979326> (visited on 03/23/2022).
- [300] Anselm Strauss and Juliet Corbin. *Basics of qualitative research techniques*. Sage publications Thousand Oaks, CA, 1998.
- [301] Ivan Fléchaïs. “Designing secure and usable systems”. In: *PhD diss., University College London* (2005).
- [302] Barney G. Glaser and Anselm L. Strauss. *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.
- [303] Columbia Public Health. *Content Analysis Method and Examples | Columbia Public Health*. 2022. URL: <https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis> (visited on 03/28/2022).
- [304] Sara Kraemer, Pascale Carayon, and John Clem. “Human and organizational factors in computer and information security: Pathways to vulnerabilities”. en. In: *Computers & Security* 28.7 (Oct. 2009), pp. 509–520. URL: <https://www.sciencedirect.com/science/article/pii/S0167404809000467> (visited on 03/28/2022).
- [305] David L. Morgan. “Qualitative Research Methods: Focus groups as qualitative research”. In: *Thousand Oaks, CA: SAGE Publications, Inc.* doi 10 (1997), p. 9781412984287.
- [306] 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 03/28/2022).



- [307] Satu Elo and Helvi Kyngäs. “The qualitative content analysis process”. en. In: *Journal of Advanced Nursing* 62.1 (2008). \_eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1365-2648.2007.04569.x>, pp. 107–115. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2648.2007.04569.x> (visited on 03/28/2022).
- [308] Hsiu-Fang Hsieh and Sarah E. Shannon. “Three Approaches to Qualitative Content Analysis”. en. In: *Qualitative Health Research* 15.9 (Nov. 2005). Publisher: SAGE Publications Inc, pp. 1277–1288. URL: <https://doi.org/10.1177/1049732305276687> (visited on 03/28/2022).
- [309] David F. Marks and Lucy Yardley. *Research Methods for Clinical and Health Psychology*. en. Google-Books-ID: wd3ELez9D4C. SAGE, 2004.
- [310] 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.
- [311] 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 03/23/2022).
- [312] Detmar W. Straub and Richard J. Welke. “Coping with Systems Risk: Security Planning Models for Management Decision Making”. In: *MIS Quarterly* 22.4 (1998). Publisher: Management Information Systems Research Center, University of Minnesota, pp. 441–469. URL: <https://www.jstor.org/stable/249551> (visited on 03/28/2022).
- [313] Adam Beautement et al. “Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours”. en. In: 2016, pp. 253–270. URL: <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement> (visited on 03/28/2022).
- [314] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. “I Think They’re Trying to Tell Me Something: Advice Sources and Selection for Digital Security”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2016, pp. 272–288.
- [315] Richard L. Baskerville. “Investigating information systems with action research”. In: *Communications of the association for information systems* 2.1 (1999), p. 19.
- [316] Sauvik Das et al. “Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’14. New York, NY, USA: Association for Computing Machinery, Nov. 2014, pp. 739–749. URL: <https://doi.org/10.1145/2660267.2660271> (visited on 03/28/2022).

- [317] William R. Shadish and Thomas D. Cook. “The Renaissance of Field Experimentation in Evaluating Interventions”. In: *Annual Review of Psychology* 60.1 (2009). \_eprint: <https://doi.org/10.1146/annurev.psych.60.110707.163544>, pp. 607–629. URL: <https://doi.org/10.1146/annurev.psych.60.110707.163544> (visited on 03/28/2022).
- [318] Alan S. Gerber and Donald P. Green. *Field Experiments and Natural Experiments*. en. ISBN: 9780199604456. July 2011. URL: <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199604456.001.0001/oxfordhb-9780199604456-e-050> (visited on 03/28/2022).
- [319] Mikko T. Siponen and Harri Oinas-Kukkonen. “A review of information security issues and respective research contributions”. In: *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 38.1 (Feb. 2007), pp. 60–80. URL: <https://doi.org/10.1145/1216218.1216224> (visited on 10/25/2021).
- [320] Robert D. Galliers and Frank F. Land. “Choosing appropriate information systems research methodologies”. In: *Communications of the ACM* 30.11 (1987), pp. 901–902.
- [321] Gurpreet Dhillon and James Backhouse. “Current directions in IS security research: towards socio-organizational perspectives”. en. In: *Information Systems Journal* 11.2 (2001), pp. 127–153. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2575.2001.00099.x> (visited on 10/25/2021).
- [322] David M. Fetterman. *Ethnography: Step-by-step*. Sage publications, 2019.
- [323] John Mingers. “Combining IS Research Methods: Towards a Pluralist Methodology”. In: *Information Systems Research* 12.3 (Sept. 2001). Publisher: INFORMS, pp. 240–259. URL: <https://pubsonline.informs.org/doi/abs/10.1287/isre.12.3.240.9709> (visited on 03/23/2022).
- [324] Izak Benbasat. “Laboratory experiments in information systems studies with a focus on individuals: a critical appraisal”. In: *The information systems research challenge: Experimental research methods 2* (1989), pp. 33–47.
- [325] Steve Harrison. “Courtesy Art, Deborah Tatar, and Phoebe Sengers. The three paradigms of HCI”. In: *In SIGCHI Conference on Human Factors in Computing Systems*. 2007.
- [326] J.H. Saltzer and M.D. Schroeder. “The protection of information in computer systems”. In: *Proceedings of the IEEE* 63.9 (Sept. 1975), pp. 1278–1308.
- [327] Simson Garfinkel and Heather Richter Lipford. “Usable Security: History, Themes, and Challenges”. In: *Synthesis Lectures on Information Security, Privacy, and Trust* 5.2 (Sept. 2014), pp. 1–124. URL: <https://www.morganclaypool.com/doi/abs/10.2200/S00594ED1V01Y201408SPT011> (visited on 10/27/2021).

- [328] Weijia He et al. “Clap On, Clap Off: Usability of Authentication Methods in the Smart Home”. en. In: *Proceedings of the Interactive Workshop on the Human Aspect of Smarthome Security and Privacy* (Jan. 2018). URL: <https://par.nsf.gov/biblio/10095908-clap-clap-off-usability-authentication-methods-smart-home> (visited on 09/02/2021).
- [329] Alexander Ponticello, Matthias Fassl, and Katharina Krombholz. “Exploring Authentication for Security-Sensitive Tasks on Smart Home Voice Assistants”. en. In: 2021, pp. 475–492. URL: <https://www.usenix.org/conference/soups2021/presentation/ponticello> (visited on 09/01/2021).
- [330] Yuqi Liu et al. “What Influences the Perceived Trust of a Voice-Enabled Smart Home System: An Empirical Study”. en. In: *Sensors* 21.6 (Jan. 2021). Number: 6 Publisher: Multidisciplinary Digital Publishing Institute, p. 2037. URL: <https://www.mdpi.com/1424-8220/21/6/2037> (visited on 05/26/2021).
- [331] Alena Naiakshina et al. “If you want, I can store the encrypted password”: A Password-Storage Field Study with Freelance Developers”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–12. URL: <https://doi.org/10.1145/3290605.3300370> (visited on 10/26/2021).
- [332] Frank Li et al. “Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines”. en. In: 2019, pp. 273–288. URL: <https://www.usenix.org/conference/soups2019/presentation/li> (visited on 10/27/2021).
- [333] M. A. Sasse and I. Flechais. “Usable Security: Why Do We Need It? How Do We Get It?” eng. In: *In: Cranor, LF and Garfinkel, S, (eds.) Security and Usability: Designing secure systems that people can use. (13 - 30). O’Reilly: Sebastopol, US. (2005)*. Ed. by L. F. Cranor and S. Garfinkel. Sebastopol, US: O’Reilly, 2005, pp. 13–30. URL: <http://shop.oreilly.com/product/9780596008277.do> (visited on 10/27/2021).
- [334] Yaxing Yao. “Designing for Better Privacy Awareness in Smart Homes”. In: *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. CSCW ’19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 98–101. URL: <https://doi.org/10.1145/3311957.3361863> (visited on 09/02/2021).
- [335] Yaxing Yao et al. “Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–12. URL: <https://doi.org/10.1145/3290605.3300428> (visited on 09/02/2021).
- [336] Roberto Hoyle et al. “Privacy behaviors of lifeloggers using wearable cameras”. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. UbiComp ’14. Seattle, Washington: Association for Computing Machinery, Sept. 2014, pp. 571–582. URL: <https://doi.org/10.1145/2632048.2632079> (visited on 07/29/2020).
- [337] Ingolf Becker. “Measuring and Understanding Security Behaviours”. PhD Thesis. UCL (University College London), 2019.

- [338] Ingolf Becker, Simon Parkin, and M. Angela Sasse. “Measuring the Success of Context-Aware Security Behaviour Surveys”. en. In: 2017, pp. 77–86. URL: <https://www.usenix.org/conference/laser2017/presentation/becker> (visited on 08/26/2021).
- [339] Jakob Nielsen and Rolf Molich. “Heuristic evaluation of user interfaces”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 1990, pp. 249–256.
- [340] Timo Jakobi et al. “The Catch(es) with Smart Home: Experiences of a Living Lab Field Study”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI '17. Denver, Colorado, USA: Association for Computing Machinery, May 2017, pp. 1620–1633. URL: <https://doi.org/10.1145/3025453.3025799> (visited on 07/29/2020).
- [341] Florian Alt and Emanuel von Zeszchitz. “Emerging Trends in Usable Security and Privacy”. In: *i-com* (2019).
- [342] Bryan D. Payne and W. Keith Edwards. “A Brief Introduction to Usable Security”. In: *IEEE Internet Computing* 12.3 (May 2008). Conference Name: IEEE Internet Computing, pp. 13–21.
- [343] Anselm Strauss and Juliet M. Corbin. *Grounded theory in practice*. Sage, 1997.
- [344] Denis Walsh and Soo Downe. “Meta-synthesis method for qualitative research: a literature review”. In: *Journal of advanced nursing* 50.2 (2005), pp. 204–211.
- [345] Pamela S. Hinds, Ralph J. Vogel, and Laura Clarke-Steffen. “The Possibilities and Pitfalls of Doing a Secondary Analysis of a Qualitative Data Set:” en. In: *Qualitative Health Research* (July 2016). Publisher: Sage PublicationsSage CA: Thousand Oaks, CA. URL: <https://journals.sagepub.com/doi/10.1177/104973239700700306> (visited on 09/15/2020).
- [346] John W. Creswell and J. David Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.
- [347] Barbara B. Kawulich. “Participant observation as a data collection method”. In: *Forum qualitative sozialforschung/forum: Qualitative social research*. Vol. 6. 2005.
- [348] 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 (2013). \_eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/nhs.12048>, pp. 398–405. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/nhs.12048> (visited on 07/25/2020).
- [349] Sharan B. Merriam. *Case study research in education: A qualitative approach*. Case study research in education: A qualitative approach. San Francisco, CA, US: Jossey-Bass, 1988.
- [350] Sharan B. Merriam. *Qualitative Research and Case Study Applications in Education. Revised and Expanded from " Case Study Research in Education."*. ERIC, 1998.
- [351] Charles F. Cannell, Peter V. Miller, and Lois Oksenberg. “Research on interviewing techniques”. In: *Sociological methodology* 12 (1981), pp. 389–437.

- [352] Lorraine Olszewski Walker and Kay Coalson Avant. *Strategies for theory construction in nursing*. Vol. 4. Pearson/Prentice Hall Upper Saddle River, NJ, 2005.
- [353] Kathleen Carley. “Coding Choices for Textual Analysis: A Comparison of Content Analysis and Map Analysis”. In: *Sociological Methodology* 23 (1993), pp. 75–126. URL: <https://www.jstor.org/stable/271007> (visited on 02/18/2022).
- [354] Yosef Jabareen. “Building a Conceptual Framework: Philosophy, Definitions, and Procedure”. en. In: *International Journal of Qualitative Methods* 8.4 (Dec. 2009), pp. 49–62. URL: <https://doi.org/10.1177/160940690900800406> (visited on 02/18/2022).
- [355] George Chalhoub. *r/oxford - Do you own a smart speaker (Alexa, Google Home)? Get paid £10 for a 30 minutes interview*. en. URL: <https://www.reddit.com/r/oxford/comments/cgrxgm>.
- [356] Google. *Allow personal results on your shared devices* URL: <https://support.google.com/assistant/answer/7684543>.
- [357] Sidney Fussell. *Consumer Surveillance Enters Its Bargaining Phase*. en-US. Vol. 2019. Sep 11, 2019. URL: <https://www.theatlantic.com/technology/archive/2019/06/alex-google-incognito-mode-not-real-privacy/590734/>.
- [358] *Security Vulnerabilities of Voice Recognition Technologies*. en-US. Vol. 2019. Sep 11, 2015. URL: <https://resources.infosecinstitute.com/security-vulnerabilities-of-voice-recognition-technologies/>.
- [359] *Sensory is Enabling Offline Smart Speakers with No Cloud Connectivity to Maximize Security*. en-US. Vol. 2019. Sep 11, 2019. URL: <https://voicebot.ai/2019/01/18/sensory-is-enabling-offline-smart-speakers-with-no-cloud-connectivity-to-maximize-security/>.
- [360] John Adams. “Risk and morality: three framing devices”. In: *Risk and morality* (2003), pp. 87–106.
- [361] Michael Thompson. “Taking account of societal concerns about risk”. In: ().
- [362] Melissa P. Johnston. “Secondary data analysis: A method of which the time has come”. In: *Qualitative and quantitative methods in libraries* 3.3 (2017), pp. 619–626.
- [363] Asa Blomquist and Mattias Arvola. “Personas in action: ethnography in an interaction design team”. In: *Proceedings of the second Nordic conference on Human-computer interaction*. 2002, pp. 197–200.
- [364] Paul Piccone. “The Reality of Ethnomethodology”. en. In: *Telos* 1975.26 (Dec. 1975). Publisher: Telos Press, pp. 195–205. URL: <http://journal.telospress.com/content/1975/26/195> (visited on 01/09/2023).
- [365] Harold Garfinkel. *Studies in Ethnomethodology*. Malden MA: Polity Press/Blackwell Publishing, 1984.
- [366] Kenneth Leiter. *A Primer on Ethnomethodology*. en. Google-Books-ID: Ivi1AAAIAAJ. Oxford University Press, 1980.

- [367] David W. Stewart, David W. Stewart, and Michael A. Kamins. *Secondary research: Information sources and methods*. Vol. 4. Sage, 1993.
- [368] Angela Dale, Sara Arber, and Michael Procter. *Doing secondary analysis*. Unwin Hyman, 1988.
- [369] Daniel M. Doolan and Erika S. Froelicher. “Using an existing data set to answer new research questions: a methodological review”. eng. In: *Research and Theory for Nursing Practice* 23.3 (2009), pp. 203–215.
- [370] Mary L. McHugh. “Interrater reliability: the kappa statistic”. In: *Biochemia medica: Biochemia medica* 22.3 (2012). Publisher: Medicinska naklada, pp. 276–282.
- [371] Scott Davidoff et al. “Principles of Smart Home Control”. en. In: *UbiComp 2006: Ubiquitous Computing*. Ed. by Paul Dourish and Adrian Friday. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2006, pp. 19–34.
- [372] Stuart E. Dreyfus and Hubert L. Dreyfus. *A five-stage model of the mental activities involved in directed skill acquisition*. Tech. rep. California Univ Berkeley Operations Research Center, 1980.
- [373] Elizabeth A. Suter. “Focus groups in ethnography of communication: Expanding topics of inquiry beyond participant observation”. In: *The Qualitative Report* 5.1 (2000), pp. 1–14.
- [374] Robert V. Labaree. “Research Guides: Organizing Your Social Sciences Research Paper: 5. The Literature Review”. In: (2009).
- [375] Robert K. Yin. *Qualitative research from start to finish*. Guilford publications, 2015.
- [376] Chris Duckett. *Google needs to break up its all-or-nothing approach to permissions*. en. Nov. 2018. URL: <https://www.zdnet.com/article/google-needs-to-break-up-its-all-or-nothing-approach-to-permissions/> (visited on 09/13/2020).
- [377] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. “An empirical investigation of concerns of everyday tracking and recording technologies”. In: *Proceedings of the 10th international conference on Ubiquitous computing*. New York, NY, USA: Association for Computing Machinery, Sept. 2008, pp. 182–191. URL: <https://doi.org/10.1145/1409635.1409661> (visited on 09/08/2020).
- [378] Norbert Nthala and Emilee Rader. “Towards a Conceptual Model for Provoking Privacy Speculation”. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA '20. New York, NY, USA: Association for Computing Machinery, Apr. 2020, pp. 1–8. URL: <https://doi.org/10.1145/3334480.3382815> (visited on 09/08/2020).
- [379] Anupam Das et al. “The tangled web of password reuse.” In: *NDSS*. Vol. 14. 2014, pp. 23–26.
- [380] Charlton, Alistair. *Sharing your smart home with others is a minefield of inconvenience*. en. Sept. 2018. URL: <https://www.gearbrain.com/sharing-smart-home-devices-2608366363.html> (visited on 09/09/2020).

- [381] Ry Crist. *Multiple users, multiple systems, multiple devices: Is this the smart home from hell?* en. Dec. 2015. URL: <https://www.cnet.com/news/multiple-users-multiple-systems-multiple-devices-is-this-the-smart-home-from-hell/> (visited on 09/09/2020).
- [382] Bradley Chambers. *HomeKit Weekly: Apple should allow selective access to HomeKit devices for Family Sharing.* en-US. Jan. 2020. URL: <https://9to5mac.com/2020/01/24/homekit-family-sharing/> (visited on 09/09/2020).
- [383] Jack Narcotta. *Smart Home Surveillance Camera Market Analysis and Forecast.* en. Strategy Analytics. Apr. 2018. (Visited on 02/12/2020).
- [384] Matt Burgess. “The IoT’s security nightmare will never end. You can now search insecure cameras by address”. In: *Wired UK* (Nov. 2018). URL: <https://www.wired.co.uk/article/internet-of-things-security-camera-search-location> (visited on 02/12/2020).
- [385] Kambiz Ghazinour and Emil Shirima. “Privacy for Security Monitoring Systems”. In: *3rd Workshop on Inclusive Privacy and Security (WIPS)* (Aug. 2018).
- [386] 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.* IEEE, 2011, pp. 1–6.
- [387] Jasper van Kuijk et al. “Barriers to and Enablers of Usability in Electronic Consumer Product Development: A Multiple Case Study”. In: *Human-Computer Interaction* 32.1 (Jan. 2017), pp. 1–71. URL: <https://doi.org/10.1080/07370024.2015.1117373> (visited on 02/23/2020).
- [388] Clive Seale. “Quality in qualitative research”. In: *Qualitative inquiry* 5.4 (1999), pp. 465–478.
- [389] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Sage publications, 2014.
- [390] Greg Guest, Arwen Bunce, and Laura Johnson. “How many interviews are enough? An experiment with data saturation and variability”. In: *Field methods* 18.1 (2006), pp. 59–82.
- [391] “Self-Report Study”. In: *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: <http://methods.sagepub.com/reference/the-sage-dictionary-of-social-research-methods/n186.xml> (visited on 05/26/2020).
- [392] Kathy Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis.* sage, 2006.
- [393] Nayan B. Ruparelia. “Software development lifecycle models”. In: *ACM SIGSOFT Software Engineering Notes* 35.3 (2010). Publisher: ACM New York, NY, USA, pp. 8–13.
- [394] Lassi A. Liikkanen et al. “Lean UX: the next generation of user-centered agile development?” In: *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational.* ACM, 2014, pp. 1095–1100.

- [395] Paul Voigt and Axel Von dem Bussche. “The eu general data protection regulation (gdpr)”. In: *A Practical Guide, 1st Ed.*, Cham: Springer International Publishing (2017).
- [396] Mary Ellen Zurko. “User-centered security: Stepping up to the grand challenge”. In: *21st Annual Computer Security Applications Conference (ACSAC’05)*. IEEE, 2005, 14–pp.
- [397] Marcia Ford and William Palmer. “Alexa, are you listening to me? An analysis of Alexa voice service network traffic”. en. In: *Personal and Ubiquitous Computing* 23.1 (Feb. 2019), pp. 67–79. URL: <https://doi.org/10.1007/s00779-018-1174-x> (visited on 06/09/2020).
- [398] Zhi-Kai Zhang et al. “IoT security: ongoing challenges and research opportunities”. In: *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 2014, pp. 230–234.
- [399] Teng Xu, James B. Wendt, and Miodrag Potkonjak. “Security of IoT systems: Design challenges and opportunities”. In: *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*. IEEE Press, 2014, pp. 417–423.
- [400] Xiaocheng Ge et al. “Extreme Programming Security Practices”. en. In: *Agile Processes in Software Engineering and Extreme Programming*. Ed. by Giulio Concas et al. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007, pp. 226–230.
- [401] James Stewart. *Why ‘security says no’ won’t cut it anymore - Technology in government*. en. July 2016. URL: <https://technology.blog.gov.uk/2016/07/13/why-security-says-no-wont-cut-it-anymore/> (visited on 02/17/2020).
- [402] Steffen Bartsch. “Practitioners’ Perspectives on Security in Agile Development”. In: *2011 Sixth International Conference on Availability, Reliability and Security*. ISSN: null. Aug. 2011, pp. 479–484.
- [403] Eddie Keane. “The GDPR and Employee’s Privacy: Much Ado but Nothing New”. In: *King’s Law Journal* 29.3 (2018). Publisher: Taylor & Francis, pp. 354–363.
- [404] IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*. en. Google-Books-ID: LicDEAAAQBAJ. IT Governance Ltd, Oct. 2020.
- [405] Ross Bentley. *Data protection: strictly confidential*. en-GB. Jan. 2008. URL: <https://www.personneltoday.com/hr/data-protection-strictly-confidential/> (visited on 08/30/2021).
- [406] Winfried Veil. *The GDPR: The Emperor’s New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law*. en. SSRN Scholarly Paper ID 3305056. Rochester, NY: Social Science Research Network, Dec. 2018. URL: <https://papers.ssrn.com/abstract=3305056> (visited on 08/30/2021).
- [407] Leo A. Goodman. “Snowball sampling”. In: *The annals of mathematical statistics* (1961), pp. 148–170.



- [408] 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 08/30/2021).
- [409] 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 08/30/2021).
- [410] Rowland Atkinson and John Flint. “Accessing hidden and hard-to-reach populations: Snowball research strategies”. In: *Social research update* 33.1 (2001). Publisher: Guildford, pp. 1–4.
- [411] Sri Kurniawan. “Interaction design: Beyond human–computer interaction by Preece, Sharp and Rogers (2001), ISBN 0471492787”. en. In: *Universal Access in the Information Society* 3.3 (Oct. 2004), pp. 289–289. URL: <https://doi.org/10.1007/s10209-004-0102-1> (visited on 08/05/2021).
- [412] Nicola Dell et al. “"Yours is better!": participant response bias in HCI”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, May 2012, pp. 1321–1330. URL: <https://doi.org/10.1145/2207676.2208589> (visited on 08/17/2021).
- [413] Kathy Baxter, Catherine Courage, and Kelly Caine. *Understanding your users: a practical guide to user research methods*. Morgan Kaufmann, 2015.
- [414] H. Russell Bernard and Harvey Russell Bernard. *Social Research Methods: Qualitative and Quantitative Approaches*. en. Google-Books-ID: 7sZHuhyzBNQC. SAGE, 2013.
- [415] Benjamin Koskei and Catherine Simiyu. “Role of interviews, observation, pitfalls and ethical issues in qualitative research methods”. In: *Journal of Educational Policy and Entrepreneurial Research* 2.3 (2015), pp. 108–117.
- [416] Annabel Bhamani Kajornboon. “Using interviews as research instruments”. In: *E-journal for Research Teachers* 2.1 (2005), pp. 1–9.
- [417] Peter Birmingham and David Wilkinson. *Using research instruments: A guide for researchers*. Routledge, 2003.
- [418] C N Trueman. *Structured Interviews*. English. History Learning Site. May 2015. URL: <https://www.historylearningsite.co.uk/sociology/research-methods-in-sociology/structured-interviews/> (visited on 08/04/2021).
- [419] DataGuidance Future of Privacy Forum. “Comparing privacy laws: GDPR v. CCPA”. In: *Comparing Privacy Laws: GDPR vs CCPA* (2019), p. 9. URL: [https://ec.europa.eu/futurium/en/system/files/ged/gdpr\\_ccpa\\_comparison-guide.pdf](https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf).

- [420] Carine Lallemand, Guillaume Gronier, and Vincent Koenig. “User experience: A concept without consensus? Exploring practitioners’ perspectives through an international survey”. en. In: *Computers in Human Behavior* 43 (Feb. 2015), pp. 35–48. URL: <https://www.sciencedirect.com/science/article/pii/S0747563214005718> (visited on 08/26/2021).
- [421] Eric Schaffer and Apala Lahiri. *Institutionalization of UX: A Step-by-Step Guide to a User Experience Practice*. en. Google-Books-ID: XIpTAGAAQBAJ. Addison-Wesley, Dec. 2013.
- [422] Alfonso Gómez-Arzola. *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 05/20/2021).
- [423] 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 05/20/2021).
- [424] 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 05/20/2021).
- [425] 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 05/20/2021).
- [426] Sebastian Rieger and Caroline Sindere. “Dark Patterns: Regulating Digital Design”. en. In: (2020), p. 28. URL: <https://www.stiftung-nv.de/sites/default/files/dark.patterns.english.pdf>.
- [427] Hatchd. *The dangers of dishonest design*. en-AU. July 2017. URL: <https://www.hatchd.com.au/blog/the-dangers-of-dishonest-design> (visited on 05/20/2021).
- [428] 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](https://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=0affa34d-2165-4424-a65a-6d6d2111d1e0) (visited on 05/20/2021).
- [429] Mark Warner and Debra Fischer. *Senators Introduce Bipartisan Legislation to Ban Manipulative “Dark Patterns”*. 2020.
- [430] Dennis D. Hirsch. “The glass house effect: Big Data, the new oil, and the power of analogy”. In: *Me. L. Rev.* 66 (2013), p. 373.
- [431] Carrie Gates and Peter Matthews. “Data Is the New Currency”. In: *Proceedings of the 2014 New Security Paradigms Workshop*. NSPW ’14. New York, NY, USA: Association for Computing Machinery, Sept. 2014, pp. 105–116. URL: <https://doi.org/10.1145/2683467.2683477> (visited on 05/26/2021).

- [432] Gary Clayton. “Safeguarding the world’s new currency”. English. In: *Information Management Journal* 36.3 (June 2002). Num Pages: 6 Place: Lenexa, United States Publisher: ARMA International, pp. 18–24. URL: <https://www.proquest.com/docview/227759723/abstract/E13F13BB279143E7PQ/1> (visited on 05/26/2021).
- [433] Edmund G. Howe III and Falcia Elenberg. “Ethical Challenges Posed by Big Data”. In: *Innovations in Clinical Neuroscience* 17.10-12 (Oct. 2020), pp. 24–30. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7819582/> (visited on 01/07/2023).
- [434] Natasha Lomas. *Cookie consent tools are being used to undermine EU privacy rules, study suggests*. en-US. Jan. 2020. URL: <https://social.techcrunch.com/2020/01/10/cookie-consent-tools-are-being-used-to-undermine-eu-privacy-rules-study-suggests/> (visited on 05/16/2021).
- [435] *GDPR Best Practices*. en-US. 2020. URL: <https://www.compliancejunction.com/gdpr-best-practices/> (visited on 05/16/2021).
- [436] *GDPR best practices in 7 steps*. en-US. June 2018. URL: <https://blog.back4app.com/gdpr-best-practices/> (visited on 05/16/2021).
- [437] DUN & BRADSTREET. *7 Best Practices for Effective GDPR Compliance*. en. July 2017. URL: <https://www.dnb.co.uk/perspectives/finance-credit-risk/7-best-practices-gdpr-compliance.html> (visited on 05/16/2021).
- [438] Bridgeline Digital. *GDPR Compliance Best Practices Guide*. 2018. URL: <https://www.bridgeline.com/resources/gdpr-best-practices-guide> (visited on 05/16/2021).
- [439] claudiu. *6 Key Steps to Ensure GDPR Compliance - The Steps You Need to Take*. en-US. May 2018. URL: <https://www.codeinwp.com/blog/gdpr-compliance/> (visited on 05/16/2021).
- [440] Simon Wilson. “A framework for security technology cohesion in the era of the GDPR”. en. In: *Computer Fraud & Security* 2018.12 (Dec. 2018), pp. 8–11. URL: <https://www.sciencedirect.com/science/article/pii/S1361372318301192> (visited on 05/16/2021).
- [441] Freek Vermeulen. “When ‘Best Practices’ Backfire”. In: *Harvard Business Review* (Nov. 2017). Section: Business processes. URL: <https://hbr.org/podcast/2017/11/when-best-practices-backfire> (visited on 05/16/2021).
- [442] William Vogeler. *Can ‘Best Practices’ Be Bad for Your Law Practice?* en-US. Nov. 2017. URL: <https://blogs.findlaw.com/strategist/2017/11/can-best-practices-be-bad-for-your-law-practice.html> (visited on 05/16/2021).
- [443] Mike Myatt. *Best Practices - Aren’t*. en. Section: Leadership. Aug. 2012. URL: <https://www.forbes.com/sites/mikemyatt/2012/08/15/best-practices-arent/> (visited on 05/16/2021).

- [444] Kevin F McCloskey. “Current trends in outsourcing and addressing third party risk”. en. In: (2019), p. 5. URL: <https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Current%20trends%20in%20outsourcing%20and%20addressing%20third%20party%20risk.pdf>.
- [445] A29 WP. *WP243 ANNEX - FREQUENTLY ASKED QUESTIONS*. 2021. URL: [https://ec.europa.eu/information\\_society/newsroom/image/document/2016-51/wp243\\_annex\\_en\\_40856.pdf](https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf).
- [446] Joe Curtis. *Don't outsource your GDPR compliance*. en. July 2017. URL: <https://www.cloudpro.co.uk/leadership/6834/dont-outsource-your-gdpr-compliance> (visited on 05/16/2021).
- [447] Luke Irwin. *The GDPR: Why you need to review your third-party service providers' security*. en-GB. May 2020. URL: <https://www.itgovernance.eu/blog/en/the-gdpr-why-you-need-to-review-your-third-party-service-providers-security> (visited on 05/16/2021).
- [448] Grant McGregor. *GDPR, Outsourcing and Third-Party Data - what you need to know*. en-gb. May 2018. URL: <https://blog.grantmcgregor.co.uk/2018/gdpr-outsourcing-and-third-party-data-what-you-need-to-know-before-the-sky-falls-in-this-friday> (visited on 05/16/2021).
- [449] Jacob Nielsen. *Agile Development Projects and Usability*. en. Nov. 2018. URL: <https://www.nngroup.com/articles/agile-development-and-usability/> (visited on 06/01/2021).
- [450] Jakob Nielsen. “Usability engineering at a discount”. In: *Proceedings of the third international conference on human-computer interaction on Designing and using human-computer interfaces and knowledge based systems (2nd ed.)* USA: Elsevier Science Inc., Sept. 1989, pp. 394–401. (Visited on 06/01/2021).
- [451] Jakob Nielsen. “Discount usability: 20 years”. In: *Jakob Nielsen's Alertbox Available at http://www.useit.com/alertbox/discount-usability.html [Accessed 23 January 2012]* (2009).
- [452] Reinhard Sefelin, Manfred Tscheligi, and Verena Giller. “Paper prototyping - what is it good for? a comparison of paper- and computer-based low-fidelity prototyping”. In: *CHI '03 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '03. New York, NY, USA: Association for Computing Machinery, Apr. 2003, pp. 778–779. URL: <https://doi.org/10.1145/765891.765986> (visited on 06/02/2021).
- [453] Nick Kostov and Sam Schechner. “GDPR Has Been a Boon for Google and Facebook”. en-US. In: *Wall Street Journal* (June 2019). URL: <https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219> (visited on 08/24/2021).
- [454] Keumars Afifi-Sabet. *Research unearths inadvertent GDPR business benefits*. en. Mar. 2019. URL: <https://www.itpro.co.uk/general-data-protection-regulation-gdpr/33154/research-unearths-inadvertent-gdpr-business-benefits> (visited on 08/24/2021).

- [455] Finjan Team. *Who Benefits from GDPR? Large American Tech Companies for one*. en-US. Finjan Team. Mar. 2018. URL: <https://blog.finjan.com/who-benefits-from-gdpr/> (visited on 08/24/2021).
- [456] Rob Sobers. *GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis*. en. Section: Compliance & Regulation. June 2019. URL: <https://www.varonis.com/blog/gdpr-effect-review/> (visited on 08/24/2021).
- [457] Deirdre K Mulligan and Jennifer King. "Bridging the gap between privacy and design". In: *U. Pa. J. Const. L.* 14 (2011), pp. 989–1034.
- [458] Richmond Y. Wong and Deirdre K. Mulligan. "Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019.
- [459] M.J. Muller. "Participatory design: The third space in HCI". In: *Human-Computer Interaction Handbook* 4235. January 2002 (2003), pp. 1051–1068.
- [460] Kurt Thomas et al. "SoK: Hate, Harassment, and the Changing Landscape of Online Abuse". In: *2021 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2021, pp. 247–267.
- [461] Batya Friedman, Edward Felten, and Lynette I. Millett. "Informed consent online: A conceptual model and design principles". In: *University of Washington Computer Science & Engineering Technical Report 00-12-2* 8 (2000).
- [462] Ekaterina Muravyeva et al. "Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited". en. In: *Ethics and Information Technology* 22.3 (Sept. 2020), pp. 223–238. URL: <https://doi.org/10.1007/s10676-020-09531-5> (visited on 01/07/2023).
- [463] Information Commissioner's Office. *When is consent appropriate?* en. July 2020. URL: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> (visited on 08/12/2020).
- [464] Dale Smith. *Fix 3 common Google Home music glitches before they happen*. en. May 2020. URL: <https://www.cnet.com/how-to/fix-3-common-google-home-music-glitches-before-they-happen/> (visited on 09/09/2020).
- [465] Alexander Tsesis. "The right to erasure: Privacy, data brokers, and the indefinite retention of data". In: *Wake Forest L. Rev.* 49 (2014). Publisher: HeinOnline, p. 433.
- [466] Gaurav Bansal, Fatemeh 'Mariam' Zahedi, and David Gefen. "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern". In: *European Journal of Information Systems* 24.6 (2015), pp. 624–644.
- [467] Peter Worthy, Ben Matthews, and Stephen Viller. "Trust Me: Doubts and Concerns Living with the Internet of Things". In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. DIS '16. New York, NY, USA: Association for Computing Machinery, June 2016, pp. 427–434. URL: <https://doi.org/10.1145/2901790.2901890> (visited on 08/23/2020).

- [468] Sara Cannizzaro et al. “Trust in the smart home: Findings from a nationally representative survey in the UK”. In: *Plos one* 15.5 (2020). Publisher: Public Library of Science San Francisco, CA USA, e0231615.
- [469] Mozilla Foundation. *\*Privacy Not Included: A Buyer’s Guide for Connected Products*. en. 2020. URL: <https://foundation.mozilla.org/en/privacynotincluded/facebook-portal/> (visited on 05/20/2021).
- [470] Erica Perry. *Lack Of Trust Costs Brands \$2.5 Trillion Per Year: Study*. en-US. Section: Business. Feb. 2018. URL: <https://socialmediaweek.org/blog/2018/02/lack-trust-costs-brands-2-5-trillion-per-year-study/> (visited on 05/20/2021).
- [471] Círculo de Directores. *The trust crisis: Facebook, Boeing and too many other firms are losing the public’s faith. Can they regain it?* es. Section: Governance. July 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 05/20/2021).
- [472] Ingolf Becker, Simon Parkin, and M. Angela Sasse. “Finding security champions in blends of organisational culture”. In: *Proc. USEC* 11 (2017).
- [473] Ingolf Becker, Simon Parkin, and M. Angela Sasse. “Combining Qualitative Coding and Sentiment Analysis: Deconstructing Perceptions of Usable Security in Organisations”. en. In: 2016, pp. 43–53. URL: <https://www.usenix.org/conference/laser2016/program/presentation/becker> (visited on 08/26/2021).
- [474] Adam Beutement, M. Angela Sasse, and Mike Wonham. “The compliance budget: managing security behaviour in organisations”. In: *Proceedings of the 2008 New Security Paradigms Workshop*. NSPW ’08. New York, NY, USA: Association for Computing Machinery, Sept. 2008, pp. 47–58. URL: <https://doi.org/10.1145/1595676.1595684> (visited on 08/26/2021).
- [475] Daniel Mikkelsen et al. *Tackling GDPR compliance before time runs out*. Tech. rep. McKinsey Global Institute, 2017.
- [476] Eyal Ronen and Adi Shamir. “Extended Functionality Attacks on IoT Devices: The Case of Smart Lights”. In: *2016 IEEE European Symposium on Security and Privacy (EuroS P)*. Mar. 2016, pp. 3–12.
- [477] Roxanne Leitão. “Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse”. In: *Proceedings of the 2019 on Designing Interactive Systems Conference*. DIS ’19. New York, NY, USA: Association for Computing Machinery, June 2019, pp. 527–539. URL: <https://doi.org/10.1145/3322276.3322366> (visited on 09/02/2020).
- [478] Ashkan Soltani. “Abusability testing: Considering the ways your technology might be used for harm”. In: *Enigma 2019 (Enigma 2019)*. 2019.

- [479] Jack Stilgoe, Richard Owen, Phil Macnaghten. *Developing a framework for responsible innovation\**. en. Pages: 347-359 Publication Title: The Ethics of Nanotechnology, Geoenvironment, and Clean Energy. Routledge, July 2020. URL: <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003075028-22/developing-framework-responsible-innovation-jack-stilgoe-richard-owen-phil-macnaghten> (visited on 01/06/2023).
- [480] Richard Owen et al. “A Framework for Responsible Innovation”. en. In: *Responsible Innovation*. Section: 2 \_eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118551424.ch2>. John Wiley & Sons, Ltd, 2013, pp. 27–50. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118551424.ch2> (visited on 01/06/2023).
- [481] René von Schomberg. “A Vision of Responsible Research and Innovation”. en. In: *Responsible Innovation*. Section: 3 \_eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118551424.ch3>. John Wiley & Sons, Ltd, 2013, pp. 51–74. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118551424.ch3> (visited on 01/06/2023).
- [482] Bert-Jaap Koops. “The Concepts, Approaches, and Applications of Responsible Innovation”. en. In: *Responsible Innovation 2: Concepts, Approaches, and Applications*. Ed. by Bert-Jaap Koops et al. Cham: Springer International Publishing, 2015, pp. 1–15. URL: [https://doi.org/10.1007/978-3-319-17308-5\\_1](https://doi.org/10.1007/978-3-319-17308-5_1) (visited on 01/06/2023).
- [483] RRI Tools Consortium. “A practical guide to responsible research and innovation: Key lessons from RRI tools”. In: *Barcelona: Milimétrica Producciones SL* (2016).
- [484] Mira Lane. *Responsible Innovation: The Next Wave of Design Thinking*. en. May 2020. URL: <https://medium.com/microsoft-design/responsible-innovation-the-next-wave-of-design-thinking-86bc9e9a8ae8> (visited on 06/13/2022).
- [485] John M. Spartz and Ryan P. Weber. “User experience as a driver of entrepreneurial innovation”. In: *2016 IEEE International Professional Communication Conference (IPCC)*. Oct. 2016, pp. 1–7.
- [486] Seda Gürses, Carmela Troncoso, and Claudia Diaz. “Engineering privacy by design reloaded”. In: *Amsterdam Privacy Conference*. 2015, pp. 1–21.
- [487] Ivan Flechais, M. Angela Sasse, and Stephen Hailes. “Bringing security home: a process for developing secure and usable systems”. In: *Proceedings of the 2003 workshop on New security paradigms*. ACM, 2003, pp. 49–57.
- [488] Effie Law et al. “Towards a shared definition of user experience”. In: *CHI '08 Extended Abstracts on Human Factors in Computing Systems*. CHI EA '08. Florence, Italy: Association for Computing Machinery, Apr. 2008, pp. 2395–2398. URL: <https://doi.org/10.1145/1358628.1358693> (visited on 03/27/2020).
- [489] Anu Mäkelä and J. Fulton Suri. “Supporting users’ creativity: Design to induce pleasurable experiences”. In: *Proceedings of the International Conference on Affective Human Factors Design*. 2001, pp. 387–394.

- [490] Jakob Nielsen and D. Norman. *User Experience-Our Definition*. Nielsen Norman Group [Online]. Available at: [http://www.nngroup.com/about ...](http://www.nngroup.com/about...), 2011.
- [491] Lauralee Alben. “Quality of experience: defining the criteria for effective interaction design”. In: *interactions* 3.3 (1996). Publisher: ACM New York, NY, USA, pp. 11–15.
- [492] ISO DIS. “9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems (formerly known as 13407)”. In: *International Standardization Organization (ISO). Switzerland* (2010).
- [493] Lydia Kraus. “User experience with mobile security and privacy mechanisms”. Thesis. Technical University of Berlin, July 2017. URL: [https://www.qu.tu-berlin.de/fileadmin/fg41/kraus\\_lydia.pdf](https://www.qu.tu-berlin.de/fileadmin/fg41/kraus_lydia.pdf).
- [494] CNSS Instruction. “4009, “National Information Assurance Glossary,” Committee on National Security Systems, May 2003”. In: *Formerly NSTISSI 4009* (2003).
- [495] Action Plan. *Plan 2010-2015 for Canada’s Cyber Security Strategy*.
- [496] Claudia Canongia and Raphael Mandarino. “Cybersecurity: The new challenge of the information society”. In: *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions*. IGI Global, 2012, pp. 165–184.
- [497] Oxford Dictionaries. “Cybersecurity”. In: *Retrieved from Oxford Dictionaries: http://www.oxforddictionaries.com/definition/english/cybersecurity* (2014).
- [498] Department of Homeland Security. *A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security*. Oct. 2014. URL: [http://niccs.us-cert.gov/glossary#letter\\_c](http://niccs.us-cert.gov/glossary#letter_c) (visited on 03/28/2020).
- [499] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. “Defining cybersecurity”. In: *Technology Innovation Management Review* 4.10 (2014).
- [500] Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in computing*. Prentice Hall Professional Technical Reference, 2002.
- [501] Dave Wichers. “Owasp top-10 2013”. In: *OWASP Foundation, February* (2013).
- [502] Daniel J. Solove. “Understanding privacy”. In: (2008).
- [503] Edward L. Godkin. “Libel and its legal remedy”. In: *J. Soc. Sci.* 12 (1880), pp. 69–80.
- [504] Richard A. Posner. *The economics of justice*. Harvard University Press, 1983.
- [505] Alan F. Westin. “Privacy and freedom”. In: *Washington and Lee Law Review* 25.1 (1968), p. 166.
- [506] Margaret Rouse. *What is data privacy (information privacy)? - Definition from WhatIs.com*. en. Library Catalog: [searchcio.techtarget.com](http://searchcio.techtarget.com). URL: <https://searchcio.techtarget.com/definition/data-privacy-information-privacy> (visited on 03/11/2020).
- [507] M. G Michael and Katina Michael. *Ubervveillance and the social implications of microchip implants: emerging technologies*. English. OCLC: 843857020. 2014.



- [508] 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*. IET, 1992, pp. 277–278.
- [509] A. V. Berlo et al. “Design Guidelines on Smart Homes, A COST 219bis Guidebook”. In: *Brussels, Belgium: Eur. Commission* (1999).
- [510] Danny Briere and Pat Hurley. *Smart homes for dummies*. John Wiley & Sons, 2011.
- [511] Nicola King. *Smart Home - A definition*. DTI Smart Homes Project. Sept. 2003. URL: [https://www.housinglin.org.uk/\\_assets/Resources/Housing/Housing\\_advice/Smart\\_Home\\_-\\_A\\_definition\\_September\\_2003.pdf](https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf) (visited on 03/27/2020).
- [512] Lalatendu Satpathy. “SMART HOUSING: TECHNOLOGY TO AID AGING IN PLACE-NEW OPPORTUNITIES AND CHALLENGES.” PhD Thesis. Mississippi State University, 2006.
- [513] 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), pp. 1190–1203.
- [514] 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](https://doi.org/10.1007/1-85233-854-7_2) (visited on 03/21/2020).
- [515] 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), pp. 327–345. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-5885.2011.00801.x> (visited on 03/21/2020).
- [516] *s.v. “innovation,”* en. Library Catalog: [www.merriam-webster.com](http://www.merriam-webster.com). URL: <https://www.merriam-webster.com/dictionary/innovation> (visited on 03/15/2020).
- [517] Steven Maranville. “Entrepreneurship in the Business Curriculum”. In: *Journal of Education for Business* 68.1 (Oct. 1992). Publisher: Routledge \_eprint: <https://doi.org/10.1080/08832323.1992.10117582>, pp. 27–31. URL: <https://doi.org/10.1080/08832323.1992.10117582> (visited on 03/15/2020).
- [518] Henry Edison, Nauman Bin Ali, and Richard Torkar. “Towards innovation measurement in the software industry”. In: *Journal of Systems and Software* 86.5 (2013). Publisher: Elsevier, pp. 1390–1407.
- [519] Per Frankelius. “Questioning two myths in innovation literature”. en. In: *The Journal of High Technology Management Research* 20.1 (Jan. 2009), pp. 40–51. URL: <http://www.sciencedirect.com/science/article/pii/S1047831009000054> (visited on 03/15/2020).
- [520] Sarah Mennicken and Elaine M. Huang. “Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them”. en. In: *Pervasive Computing*. Ed. by Judy Kay et al. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2012, pp. 143–160.

- [521] Shrirang Mare et al. “Consumer Smart Homes: Where We Are and Where We Need to Go”. In: *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications*. HotMobile ’19. Santa Cruz, CA, USA: Association for Computing Machinery, Feb. 2019, pp. 117–122. URL: <https://doi.org/10.1145/3301293.3302371> (visited on 07/29/2020).
- [522] Blase Ur, Jaeyeon Jung, and Stuart Schechter. “The current state of access control for smart devices in homes”. In: *Workshop on Home Usable Privacy and Security (HUPS)*. Vol. 29. HUPS 2014, 2013, pp. 209–218.
- [523] Rick Wash and Emilee Rader. “Too much knowledge? security beliefs and protective behaviors among united states internet users”. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015*. 2015, pp. 309–325.
- [524] Serge Egelman, Raghudeep Kannavara, and Richard Chow. “Is This Thing On? Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI ’15. Seoul, Republic of Korea: Association for Computing Machinery, Apr. 2015, pp. 1669–1678. URL: <https://doi.org/10.1145/2702123.2702251> (visited on 07/31/2020).
- [525] Eun Kyoung Choe et al. “Living in a glass house: a survey of private moments in the home”. In: *Proceedings of the 13th international conference on Ubiquitous computing*. UbiComp ’11. Beijing, China: Association for Computing Machinery, Sept. 2011, pp. 41–44. URL: <https://doi.org/10.1145/2030112.2030118> (visited on 07/29/2020).
- [526] Blase Ur, Jaeyeon Jung, and Stuart Schechter. “Intruders versus intrusiveness: teens’ and parents’ perspectives on home-entryway surveillance”. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2014, pp. 129–139.