DESIGNING FOR PRIVACY IN SMART HOME DEVICES:
VULNERABILITIES, CONCERNS, AND USER-CENTRIC PRIVACY CONTROLS

by

Chola Chhetri
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
In Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Information Technology

Committee:

_____ Dr. Vivian Genaro Motti, Dissertation Director

_____ Dr. Jeff Offutt, Committee Member

_____ Dr. Paulo Costa, Committee Member

_____ Dr. Kun Sun, Committee Member

_____ Dr. Deborah Goodings, Associate Dean

Date: _____ Fall Semester 2022
George Mason University
Fairfax, VA

Designing for Privacy in Smart Home Devices

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

By

Chola Chhetri
Master of Science
George Mason University, 2011
Master of Science
Sikkim Manipal University, 2005

Director: Dr. Vivian Genaro Motti, Professor
Department of Information Sciences and Technology

Fall Semester 2022
George Mason University
Fairfax, VA

Dedication

This work is dedicated to my parents and family, whose love and sacrifice have made this journey possible.

Acknowledgments

I would like to thank my advisor Dr. Vivian Genaro Motti for her continued support and guidance throughout the research program. I would also like to thank my committee members Dr. Jeff Offutt, Dr. Paulo Costa, and Dr. Kun Sun for their feedback on the dissertation, which led to improvements of this dissertation.

I am grateful to all Human Centric Design Lab members, 2017-2022, for various insightful discussions during lab meetings that have resulted in refined user studies and better analyses. I am also grateful for their help in pre-testing various survey and interview protocols. Special thanks to reseach assistant Yoseif Berhe for the help in qualitative coding of data. In addition, I would like to thank all participants of user studies and the anonymous reviewers of my published articles which have been used in this dissertation.

I am grateful to Susanne Furman, Julie Haney, Yaxing Yao, Carol Fung, and Andrea Limbargo for their valuable advice on early stages of the privacy controls research. Furthermore, I thank all my colleagues and friends for the support and encouragement during this journey.

I am grateful to the research sponsors 4-VA (Grant No. 331065), CCI (Grant No. 223817), George Mason University Provost's Office, and Graduate Student Travel Fund for their financial support at various stages of this dissertation research. I am also grateful to the Virginia Community College System's Office of Professional Development for the prestigious Chancellor's Faculty Fellowship award.

Table of Contents

Page

List of Tables ix
List of Figures xi
Abstract xii
1 Introduction 1
1.1 Background 1
1.2 Document Organization 5
1.3 Research Components 6
1.3.1 Security and Privacy Vulnerabilities of the Smart Home 6
1.3.2 Users' and Non-Users' Privacy Concerns 6
1.3.3 Privacy Controls for SHDs 7
1.3.4 Prototype Implementation and Evaluation 7
1.4 Public Policy Impact on User Privacy 8
1.5 Major Contributions 8
2 Identifying Vulnerabilities in Security and Privacy of Smart Home Devices . . . 10
2.1 Introduction 10
2.2 Methodology 12
2.2.1 Databases and Keywords 12
2.2.2 Inclusion and Exclusion Criteria 12
2.3 Vulnerabilities of the Smart Home 14
2.3.1 Device Vulnerabilities 14
2.3.2 Application Vulnerabilities 25
2.3.3 Communication Vulnerabilities 25
2.3.4 Software Architecture Vulnerabilities 26
2.4 Solutions to SHD Vulnerabilities 28
2.5 Discussion 31

2.5.1 Open Research Areas . . . 33
2.5.2 Limitations . . . 33
2.6 Conclusion . . . 34
3 Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective . . . 36
3.1 Introduction . . . 36
3.2 Methodology . . . 38
3.3 Results . . . 39
3.3.1 Specific Concerns . . . 39
3.3.2 User Sentiments . . . 41
3.3.3 Temporal Analysis . . . 42
3.3.4 Security and Privacy Principles . . . 42
3.3.5 Privacy Protection Strategies . . . 44
3.4 Conclusions . . . 45
3.4.1 Recommendations for Privacy Enhancing Solutions . . . 45
3.4.2 User-suggested Recommendations . . . 45
3.4.3 Author Recommendations . . . 46
3.4.4 Limitations . . . 48
3.4.5 Next Steps . . . 48
4 Non-Users Privacy Concerns . . . 49
4.1 Introduction . . . 49
4.2 Related Work . . . 50
4.3 Survey Method . . . 51
4.3.1 Participants . . . 51
4.3.2 Questionnaire Design . . . 51
4.3.3 Data Analysis . . . 52
4.4 Results . . . 53
4.4.1 SHD Distribution in Participants . . . 53
4.4.2 Reasons for SHD Non-Use . . . 53
4.4.3 Privacy Concerns: Non-Users vs. Users . . . 54
4.4.4 Participant Suggestions to Improve SHDs . . . 56
4.5 Discussion . . . 58

4.6 Limitations . . . 59
4.7 Conclusions . . . 59
5 User-Centric Privacy Controls for Smart Homes . . . 61
5.1 Introduction . . . 61
5.2 Related Work . . . 63
5.2.1 Privacy . . . 64
5.2.2 Users' Concerns . . . 65
5.2.3 Privacy Controls . . . 67
5.2.4 Commercial Tools . . . 68
5.2.5 Distinction from Prior Work . . . 69
5.3 Method . . . 69
5.3.1 Interview Study . . . 70
5.3.2 Survey Study . . . 77
5.4 Results . . . 81
5.4.1 Desired Privacy Controls in SHDs . . . 81
5.4.2 Quantitative Insights on Privacy Controls Desired by Users . . . 92
5.5 Discussion . . . 94
5.5.1 Summary of Findings . . . 94
5.5.2 Some Design Factors and Sub-factors Confirm Prior Work . . . 95
5.5.3 Privacy Controls Contain Usability Heuristics . . . 96
5.5.4 Recommendations for Developers: Privacy Controls Framework . . . 97
5.5.5 Users are Limited to Developer-implemented Controls . . . 98
5.5.6 Role of Government and Third Party . . . 99
5.5.7 Limitations . . . 100
5.5.8 Future Work . . . 101
5.6 Conclusion . . . 101
6 MyCam App: Design and Evaluation . . . 102
6.1 Introduction . . . 102
6.2 Background . . . 103
6.2.1 Privacy Control Design Factors and Sub-factors . . . 103
6.2.2 Translating Privacy Control Design Factors into Design . . . 103
6.3 Method . . . 104

6.3.1 Stimulus (Prototype App) . . . 105
6.3.2 Pre-Study . . . 106
6.3.3 Interview Study . . . 106
6.3.4 Survey Study . . . 107
6.4 Results . . . 110
6.4.1 Task Accuracy . . . 110
6.4.2 User Experience . . . 111
6.4.3 Usability . . . 111
6.4.4 Perceived Information Control . . . 112
6.4.5 User Satisfaction . . . 112
6.4.6 Behavioral Intention to Use . . . 112
6.4.7 User Feedback . . . 113
6.5 Discussion . . . 113
6.5.1 Design Recommendations . . . 114
6.5.2 Limitations and Future Work . . . 114
6.6 Conclusion . . . 115
7 Conclusion . . . 116
A Glossary and Acronyms . . . 119
A.1 Glossary . . . 119
A.2 List of Acronyms . . . 121
B Interview Scripts . . . 125
B.1 Interview Protocol . . . 125
B.1.1 Screening Questions . . . 125
B.1.2 Interview Questions . . . 125
C Surveys . . . 128
C.1 Privacy Controls Survey Questions . . . 128
C.2 Prototype Evaluation Survey Questions . . . 138
D Coding Manuals . . . 143
D.1 Privacy Controls Categories, Sub-categories, and Codes . . . 144
E Additional Results . . . 148
E.1 Stacked Bar Chart Showing Frequencies of Sub-Factors . . . 148
Bibliography . . . 150

List of Tables

Table Page

2.1 Number of papers included in and excluded from the study. 13

2.2 Vulnerabilities in SHDs. 24

3.1 Number of reviews for five smart hubs. Google Home (*) reviews were extracted from bestbuy.com. All other reviews were extracted from amazon.com. 38

3.2 Codebook showing codes/themes for analyses performed in the study 39

3.3 Three examples of reviews with negative, positive and neutral sentiments . 42

3.4 Four examples of privacy concerns quoted from end users' reviews considering the lifecycle of data from collection and transmission to storage and sharing 43

4.1 SHDs used by participants. Asterisk (*) indicates no brand was reported. Data is sorted per frequency of device category. Numbers in parentheses in the third column represent the frequency of that device. Some participants used multiple devices. 54

4.2 Categories (bold) and codes of non-user (NU) and user (U) privacy concerns. Non-users were more concerned about collection of data than users (NU>U). Users were more concerned about sharing of data. 55

5.1 Summary of participant demographics and devices owned by participants. P#=Participant Number. In Gender column, M=Male, F=Female, O=Other. In Education column, H=High School or below, B=Bachelor's, M=Master's, O=Other. 72

5.2 Privacy controls categories from the thematic analysis of interviews. 82

5.3 Description of privacy control categories or factors and related sample quotes 84

5.4 Mean, median and standard deviation (SD, n=440) of the privacy controls sub-factors from the survey. Mean values below 4 are marked with an asterisk (*), indicating options less desired by survey participants. Scale reliability statistic Cronbach's α values are included in parentheses in the first column. 93
5.5 Sub-factors confirmed from prior work and revealed in the current study. . . 96
5.6 SHD Privacy Control Framework: factors and sub-factors of privacy controls expected by users. Design recommendations, under each sub-factor have been omitted in this table for brevity; they can be found in Appendix D.1. 98
6.1 Task accuracy (n=105). 110
6.2 Scale statistics (n=105) 112

List of Figures

Figure		Page
1.1	Characteristics of IoT Objects	2
1.2	Smart Home Systems based on the types of automation services they offer	3
1.3	Dissertation Research Overview	5
3.1	Top six themes in users' privacy concerns and their frequencies	40
5.1	Sticky note frames used in the online whiteboard canvas.	73
5.2	Design factors and sub-factors with their frequencies (n=215). DRC: Data-related Controls, T: Transparency, CI: Centralized Interface, DC: Device Controls, MC: Multi-user Controls, SC: Security Controls, US: User Support.	83
6.1	Privacy Controls from Literature and our Research Approach	103
6.2	Research Approach	105
6.3	Home, Settings, and Dashboard pages of the MyCam prototype app.	106
6.4	Results showing scores for the six dimensions of the UEQ scale.	111
E.1	Frequency breakdown of survey responses for the 32 sub-factors.	149

Abstract

DESIGNING FOR PRIVACY IN SMART HOME DEVICES

Chola Chhetri, PhD

George Mason University, 2022

Dissertation Director: Dr. Vivian Genaro Motti

One-sixth of the 20 billion Internet of Things (IoT) devices connecting to the Internet are smart home devices (SHD) that provide home automation. These SHDs present privacy and security threats and vulnerabilities, but users have limited privacy features available to them. Those features available are difficult to locate and oftentimes unusable. Additionally, there is little insight about what SHD users care about in terms of privacy, what controls they need to manage their privacy, and how to design more usable privacy controls focused on users' needs. To address this problem, I utilized human-computer interaction (HCI) methods and conducted seven studies involving users and non-users to study their privacy concerns, privacy control needs, and the design of privacy controls.

While studying privacy solutions, I empirically identified users' privacy control needs and presented seven design factors and 32 sub-factors reflecting those privacy controls needs. Furthermore, I created an interactive prototype design of the identified data-related privacy controls and evaluated the design for usability and perceived information control involving users. Thus, this dissertation advances the knowledge in SHD usable privacy domain by identifying SHD risks, users concerns, and privacy control needs. In addition, this work helps researchers and designers develop usable privacy controls for smart home devices. The design and findings also help technologists develop better privacy control designs for IoT devices at large.

Chapter 1: Introduction

1.1 Background

In the last decade, the Internet has expanded to include devices like light bulbs, thermostats, surveillance cameras, door locks, water taps, water pipes, shoes, televisions, beds, and sensors (used in a myriad of things such as cars, pets, and luggage). This immensely grown Internet that includes non-legacy devices, where any object has the ability to communicate through the Internet, is referred to as the Internet of Things (IoT) [1]. The term 'Internet of Things' was coined by Kevin Ashton in 1999, linking the idea of radio frequency identification (RFID) to the Internet as a way to empower computers to "see, hear and smell the world" for themselves by gathering information without human data-entry [2].

The 'things' connected to IoT have five essential characteristics: existence, sense of self, connectivity, interactivity, and dynamicity. Environmental awareness is an optional characteristic possessed by IoT devices [1]. Figure 1.1 shows description and examples of these characteristics.

IoT objects are used in homes, cities, industries, and other application areas. In this dissertation, the home IoT devices are referred to as smart home devices (SHD). The home that automates some functionality or tasks using one or more SHDs is referred to as a smart home (SH). SHDs provide a variety of functionality in smart homes. Figure 1.2 shows eight categories of SHDs based on services: entertainment, appliance, climate control, safety, power and lighting, access control, security, and other. SHDs are growing in adoption and have already exceeded the billion-device milestone. According to Gartner

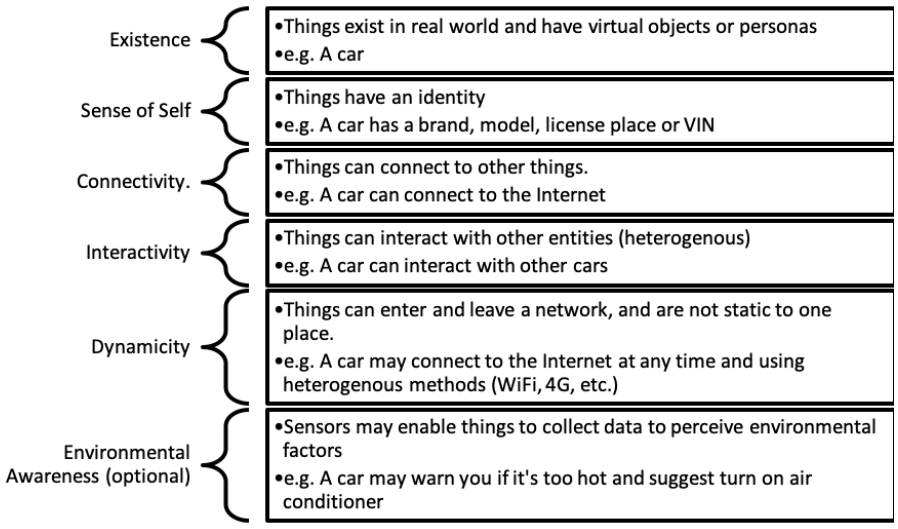


Figure 1.1: Characteristics of IoT Objects [1]

Inc., there were 8.4 billion IoT devices in the market in 2017 and one-sixth of them were smart home devices [3]. According to Business Insider, by 2025, the Internet will contain 55 billion IoT devices [4]. These numbers highlight the quickly growing IoT landscape.

Users of SHDs are largely motivated by the convenience and connectedness offerred by these devices [5]. The ability to remotely control your home devices from anywhere at anytime is a boon for many users. Users no longer have to worry about forgotten keys to their door locks and can manage their lights, thermostats, and appliances remotely. They can receive notifications when someone is home and can order their coffee-maker to brew coffee by the time they reach home from work. However, these automation features are not risk-free.

Research has shown that SHDs pose security and privacy threats to individuals as well as service providers [6–8]. Examples of such threats include baby monitor hacks and botnets

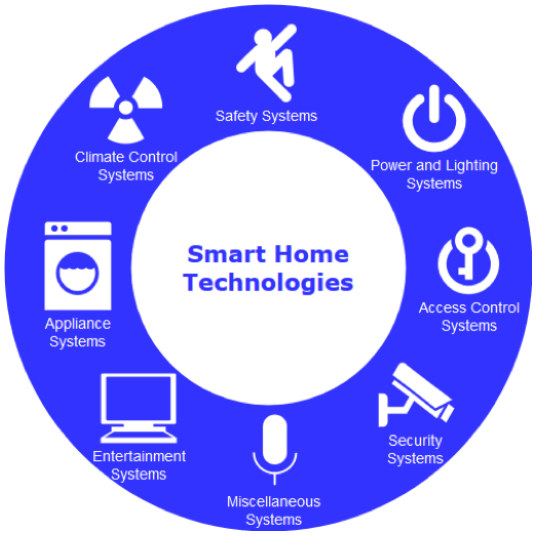


Figure 1.2: Smart Home Systems based on the types of automation services they offer

[8]. Even when home IoT devices are secured behind locked doors, they can be accessed through the Internet. SHDs can be remotely controlled through a companion mobile app. Unauthorized users, such as hackers and abusive partners, can gain remote access through vulnerabilities in the devices, such as weak authentication or no authentication. Such incidents have proven SHDs to be a bane for many users.

Hackers have been motivated by factors such as revenge and extortion. Abusive partners have hacked into and maintained control over their victims' SHDs. Social organizations dealing with victims of domestic abuse have identified cases where abusers have hijacked locks, speakers, thermostats, lights, and cameras for harassment, monitoring (listening and watching), revenge, and control of power [9].

However, solutions to tackle these issues from a user-centric approach are largely lacking. As people experience threats to their livelihoods due to SHD devices, they may decide

to discontinue using these devices or purchase ones that provide protection against these threats. Thus, by designing privacy-protecting SHDs, companies will benefit by keeping their existing customers and getting new ones who seek the privacy protection features. In a growing SHD market, vendors need to implement effective privacy controls to remain competitive in the market and to comply with existing and future legislations.

To address this gap, this dissertation focuses on understanding stakeholder privacy concerns regarding SHDs and devising solutions to address these concerns. The dissertation utilizes human-computer interaction (HCI) methods to tackle this problem.

In this dissertation research, I began by performing a systematic literature review of smart home vulnerabilities and deciphered from literature eight categories of SHD vulnerabilities. Then, through empirical study, I examined privacy concerns of SHD users by analyzing online reviews posted by verified users. Further, I examined privacy concerns of non-users comparatively with those of users through a survey study. After that, I conducted interviews and a survey study to understand the privacy control needs of SHD users and proposed a privacy control framework based on the findings. Finally, I designed a prototype app implementing the data-related privacy controls and conducted interviews and a survey study to evaluate the prototype design. The evaluation findings informed future improvements to the proposed design. Figure 1.3 summarizes the various research components that were part of this dissertation research.

Thus, this dissertation characterizes the privacy concerns of users and non-users, which are necessary to inform the design of usable privacy solutions. It further identifies factors necessary for the design of privacy features in SHDs. In addition, it presents a design of data privacy controls which helps smart home designers implement better privacy controls. Overall, this dissertation will help the smart home industry design usable and private SHDs.

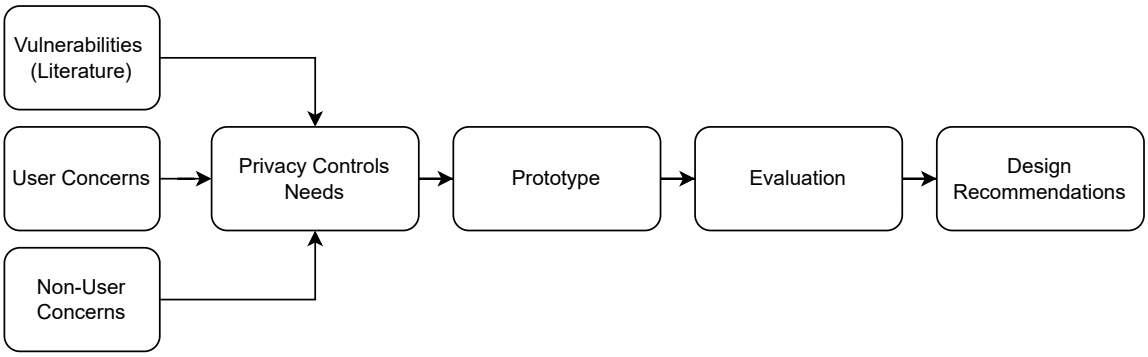


Figure 1.3: Dissertation Research Overview

1.2 Document Organization

The dissertation is composed of five papers published in a journal [10] and four conference proceedings [11–16].

Chapter 2 describes the review of literature on vulnerabilities of smart home devices and uncovers a taxonomy of vulnerabilities [14]. Chapter 3 presents an analysis of the privacy concerns of users of smart home devices [11]. Chapter 4 presents an analysis of the privacy concerns of non-users of smart home devices and compares them with the privacy concerns of users of smart home devices [15]. Chapter 5 present the empirical studies of privacy control needs of smart home devices users [10]. Chapter 6 then presents a design of the privacy controls in the form of a prototype app and the findings of the evaluation of the prototype [16]. It also makes design recommendations for future improvements. Finally, chapter 7 concludes the dissertation.

The rest of this chapter describes the dissertation research components, addresses the public policy impact on user privacy, and summarizes this dissertation's contributions.

1.3 Research Components

In this section, I will describe the various components of this dissertation research and the rationale for each research component.

1.3.1 Security and Privacy Vulnerabilities of the Smart Home

The home is a largely private space for users. However, the introduction of smart devices invades the privacy of the home user and poses threats to the residents, businesses and their services [8]. At the time of this dissertation, there was a large body of research on smart home vulnerabilities, but a systematization of the knowledge was lacking. To address this gap, I performed a systematic literature review to characterize the vulnerabilities and devise a taxonomy of SH vulnerabilities. This study also helped identify gaps and opportunities for research in the smart home domain. Chapter 2 describes the literature review methodology, the vulnerabilities taxonomy, and the identified open research areas.

1.3.2 Users' and Non-Users' Privacy Concerns

Towards the beginning of the dissertation research, only a few studies had reported SHD users' privacy concerns [17,18]. While the understanding of users' concerns was beginning, there was a lack of in-depth understanding of users' concerns. An understanding of users' concerns is necessary in order to devise solutions to address those concerns. To address this gap, I studied users' concerns by analyzing online reviews and conducting survey among users.

Similarly, very few studies have elicited non-users' concerns [19]. Drawing from Stakeholder theory, non-users are as important stakeholders as users [20]. To address this gap, I studied non-users' privacy concerns and also performed a comparative analysis with those of users. Chapter 3 describes the online review analysis methodology, privacy concerns

taxonomy, and recommendations. Chapter 4 describes non-users' concerns and the comparative analysis with the users' concerns. It further explores non-use reasons, which inform the barriers to SHD adoption and usage. The contribution of chapters 3 and 4 is to characterize user and non-user privacy concerns to inform the design of usable privacy controls.

1.3.3 Privacy Controls for SHDs

To further inform the design of privacy controls, I investigated privacy control needs of SHD users through interviews (n=25) and a survey (n=440). Results included 32 subfactors and 7 design factors for the design of SHD privacy controls, which were validated and confirmed through a large scale survey. Chapter 5 describes the methodology, study design, results and implications of the privacy controls user studies. The contribution of Chapter 5 is the privacy controls framework (PCF) which guides developers towards designing user-interface controls for privacy-respecting SHDs.

1.3.4 Prototype Implementation and Evaluation

To implement the privacy control needs reported in Chapter 5, I designed a prototype app MyCam. MyCam implemented the data-related controls from the privacy control framework aimed at providing users with control over SHD data collection, use, and sharing. Chapter 6 describes the iterative prototype design process and the user studies conducted to evaluate the prototype and make future design improvements. The contribution of Chapter 6 is the prototype app as well as design recommendations for future improvements.

1.4 Public Policy Impact on User Privacy

This dissertation tackles the problems of user privacy through design. However, policy can have a big impact on user privacy. For example, General Data Protection Regulation (GDPR) of the European Union (EU) required online providers to adhere to a set of data privacy requirements. This ensured that online service providers offered those data protection features to all EU consumers. Thus, policy can be an impactful way to ensure a certain level privacy for SHDs. This has been articulated in our Chapter 5 findings as well. There are users who think that there should be regulation on data protection in smart home devices to ensure some minimum privacy. This would act as a motivation for vendors to implement privacy features, albeit a requirement, since they would not be able to sell their non-compliant SHDs in the event that such regulation existed.

User privacy through policy or regulation can be achieved in two ways. First, new SHD data protection policies can be drafted and implemented by regulatory bodies. Alternatively, existing data protection regulations can be expanded to include SHD data. For example, the GDPR can be amended to apply to smart home data to ensure SHD data are protected. Currently, the household exemption clause allows smart home data to be remain unprotected [21]. Similarly, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) could be expanded to require the protection of health information collected by SHDs [22]. Thus, public policy can play an important role towards the design of usable and private SHDs.

1.5 Major Contributions

This dissertation makes five major contributions:

First, this doctoral research contributes a literature survey on smart home vulnerabilities. It systematizes the vulnerabilities information, provides a vulnerabilities taxonomy for the smart homes, and identifies research gaps and opportunities in the security and privacy of smart homes.

Second, this research contributes an empirical understanding of how users perceive privacy concerns about SHDs through online reviews analysis.

Third, this research contributes an empirical understanding of how non-users (an understudied smart home stakeholder category) perceive privacy concerns about smart home devices and presents a comparative analysis with those of users.

Fourth, this research identifies the privacy controls desired by users of SHDs through mixed-methods empirical studies and presents guidance for implementing user-centric privacy controls.

Fifth, this research contributes an artifact, the MyCam prototype app, and empirical evaluation and guidance on future design principles.

Research contributions in the HCI field are of seven types: Empirical, Artifact, Methodological, Theoretical, Dataset, Survey, and Opinion [23] . This dissertation makes multiple empirical contributions, one artifact contribution, and one survey contribution.

Overall, this dissertation characterizes the privacy concerns of users and non-users of SHDs. It provides insight on the privacy controls desired by users. It provides knowledge on how to design usable privacy controls in SHDs. Beyond that, it presents a design of usable privacy controls for SHDs. Thus, it helps the researcher and designer community in designing better privacy controls for smart homes. The knowledge created by this dissertation will also help develop better privacy control designs for IoT devices at large.

Chapter 2: Identifying Vulnerabilities in Security and Privacy of Smart Home Devices

2.1 Introduction

With over 20 billion Internet of Things (IoT) devices projected to be used globally by 2020, home automation is changing the way people interact and live, through the use of intelligent voice assistants, smart door locks, light bulbs, etc. [24]. Smart Home Devices (SHDs) pose threats to the security and privacy of individuals, businesses, and the society [25–27]. Unauthorized actors have hacked baby monitors [25], IoT search engines have provided public access to baby videos [28], toys have leaked parent-child conversations [29], drones have controlled home lights by flying above houses [26], and malware attacks on vulnerable IoT devices have brought down prominent Domain Name System (DNS) infrastructure affecting many large businesses, such as Dyn [27]. Information about smart home vulnerabilities (SHV) is scattered across a large number of research articles in databases. This paper systematically catalogs SHVs from research articles published in IEEE digital library and ACM digital library from 2010 to 2019.

Security vulnerabilities are closely linked with privacy, as they can lead to privacy violations. For instance, a security vulnerability may allow an adversary to hack into a baby monitor, and get audio, as well as video recordings of a child, thus violating the child's privacy. Hence, addressing SHD vulnerabilities helps resolve not only security concerns but also privacy concerns. Furthermore, unaddressed concerns leads to non-adoption and

rejection of technology, such as the past case in Netherlands, where a rollout of smart meters had led to failure [30].

To the best of our knowledge, this study is the first to systematize SHV information through literature review. Anwar et al. [31] proposed a taxonomy for smart home that broadly classifies smart home security threats into three types: (a) intentional/abuse, (b) malfunctions/failures, and (c) unintentional. Intentional threats include threats from an adversary, e.g. denial of service, identity fraud, manipulation of information, eavesdropping/traffic hijacking. Malfunctions include interruptions or disruptions caused by failures in devices, communication, network, power, third party services, and Internet. Unintentional threats are accidental abuses, such as accidental sharing of sensitive data, policy flaws, design flaws, among others [31].

Anwar's taxonomy serves as a preliminary frame for reference. However, its scope was limited to a small set of the literature (15 references) and the threats classified were non-device-specific [31]. Mosenia and Jha [32] studied 20 IoT security threats and divided them into three layers: edge nodes (computing nodes and radio frequency identification), communication, and edge computing.

Our comprehensive study of SHD vulnerabilities synthesizes 153 SHVs, categorizes them, the scope of attacks in the smart home, and identifies research areas that need further exploration. Our study is a part of research aimed at exploring SHVs and designing user-centric privacy controls for SHDs [13]. In this chapter, we report on the following:

1. We perform a systematic literature review of **1**19 articles and catalog SHV information published in selected databases (Section 3).

2. We categorize the SHVs into four categories, each category containing sub-categories. This will serve as vulnerabilities taxonomy for the smart home domain (Section 3).

3. We synthesize the solutions to SHVs from our literature review (Section 4). Some solutions are specific to a vulnerability or a device, while others are general and do not address a specific vulnerability.

4. We identify research gaps and opportunities in the security and privacy of smart homes. (Section 5)

2.2 Methodology

In this section, we describe the scope, inclusion criteria and exclusion criteria of our systematic literature review.

2.2.1 Databases and Keywords

We performed full-text literature search on IEEE Xplore Digital Library [1] and ACM Digital Library[2] from October 2018 to March 2019. We used the following keywords in the search:

- smart AND home AND vulnerabilities
  - In abstract
  - In document title

2.2.2 Inclusion and Exclusion Criteria

I read all papers in the search results to determine if they were relevant to the study. For a paper to be considered relevant, it had to discuss or contain information about smart home vulnerabilities (SHV). I read the abstract first and then the paper to determine SHV

[1] ieeexplore.ieee.org
[2] dl.acm.org

Table 2.1: Number of papers included in and excluded from the study.

Source	**# Papers**	**# Included**	**# Excluded**
IEEE	85	73	12
ACM	34	25	9
Total	119	98	21

content. If a paper did not contain SHV information, it was considered irrelevant to the study.

For each paper in the search results, the following steps were followed in order:

1. Read abstract.
2. If the abstract contains SHV information, include it.
3. If the abstract does not contain SHV information, read the paper.
4. If paper contains SHV information, include it.
5. If paper does not contain SHV information, exclude it.

Outcomes: The search in the two databases returned a total of 119 papers, of which 98 papers were included and 21 were excluded (see Table 2.1). Publication dates ranged from 2010 to 2019. ACM papers were published in 33 proceedings and one periodical. IEEE papers were published in 73 conferences and 11 journals and magazines.

For papers included in the study, a systematic cataloging of SHV information was done, following a template we developed for this purpose. In the catalog, we included the name of the vulnerability, name and type of device, explanation of the vulnerability,

solution, explanation of the solution, who implements the solution (user or developer), and drawbacks of the solution, when available in the paper.

2.3 Vulnerabilities of the Smart Home

In this section, we discuss the vulnerabilities found in the study. The cataloging process resulted in 153 SHVs. SHVs existed in various parts of the SH network, including the device, SHD applications (such as voice assistants), software architectures and frameworks, communication protocols (such as WiFi, 802.15.4, Zigbee, Routing for Low Power and Lossy Network (RPL), Precision timing protocol (PTP), etc.), smart home network, operating system (such as Android), and authentication systems (such as Zigbee Light Link).

Among the SHVs, 75 were device specific. The papers identified the devices with the vulnerability discussed. Devices with vulnerabilities included cameras (such as TP Link), Belkin motion sensor, Withings scale, light bulbs (Philips Hue, LIFX), Chromecast, Google home, Hello Barbie talking doll, Haier Smartcare, HP Envy printer, hubs/controllers, TP Link power switch, thermostat (Nest), smart meters, smart speakers, SmartThings, and Voice Control System. The 78 remaining vulnerabilities were generic (non-device-specific) and related to communication protocols, software architectures, communication, voice assistants (such as Alexa), operating systems, applications, and authentication mechanisms.

2.3.1 Device Vulnerabilities

The papers included in our study revealed vulnerabilities in SHD hardware or in the software running in the device. We divided the device vulnerabilities in eight categories:

1. Authentication Vulnerabilities

2. Information Leakage or Disclosure

3. Data Protection Vulnerabilities

4. Data Manipulation

5. Voice Interface Vulnerabilities

6. User Behavior Detection

7. Service Disruption

8. Other Vulnerabilities

Authentication Vulnerabilities

Authentication in an SHD ensures that only a legitimate user or software process have access to the device features, control and operation [33]. Authentication vulnerabilities include lack of authentication, default credentials, hard-coded credentials, leaked credentials, weak authentication, flawed authentication protocol, and de-authentication attack. We describe each of these briefly in the following sub-sections:

Lack of Authentication Ma et al. [34] showed that an attacker can post a message (text, audio, video) on the user's TV or Chromecast screen without requiring any authentication . Mahadewa et al. [35] demonstrated that any SHD in a home network can control the light bulbs available. Chromecast allowed private YouTube videos to be cast on television without requiring any authentication.

Default Credentials While the SHD industry as a whole has not caught up in implementing authentication credentials in devices [34,35], some manufacturers allow the set up of credentials, such as passwords and pins, in their devices. However, many devices run

with their default credentials [36, 37] and users are not aware of how to change them. Adversaries can easily find default credentials on the Internet. There are also search engines available that allow public access to SHDs (such as cameras) online [38]. Papers included in our study reported the use of default credentials in cameras [39, 40], routers [41], thermostats [36], plugs [42], printers [43], light bulbs and motion sensors [43]. An adversary does not need to be technically savvy to learn default credentials. They need to be able to search the Internet and have access to an Internet-connected device.

Hard-coded Credentials When credentials are hard-coded into the device and changes are not allowed, the device becomes vulnerable to attacks irrespective of other security and privacy mechanisms implemented in the device [38, 42]. SHDs with image, audio and video recording capability can easily compromise the privacy and security of individuals, if they are operate with hard-coded credentials that can not be changed by the user.

Leaked Credentials Saleh et al. (2018) demonstrated that credentials (username and password) of motion sensor and a closed-circuit television (CCTV) camera were leaked to any observer of smart home traffic. Authentication credentials were not protected from being visible to a passive observer [39].

Weak Authentication Prior research presents evidence of poorly implemented authentication, that allows an adversary to gain access to cameras [39, 43, 44]. Saleh et al. [39] conducted penetration testing on a camera used to monitor a home smart meter using the Kali[3] operating system, which allowed the investigators access to the camera using default username-password combination. This means an adversary could have full access to the smart camera without the user's knowledge. Authors claim that surveillance cameras of

[3] kali.org

this type are used to monitor smart grid for security. Vulnerable CCTV cameras, thus lead to vulnerable smart grids [39].

According to Lei et al. [44], Alexa used a voice word (analogous to a password) for user authentication. However, the person speaking the voice word did not have to be an authenticated user; it could be anyone who knew the voice word [44]. Similarly, Sivanathan et al. [43] showed that an attacker was able to send commands to control a light bulb, a power switch and a printer due to poor authentication. In another experiment, Alharbi and Aspinall [40] found that the web interface of a camera used a weak password policy, did not require complex passwords and was prone to a brute-force password attack.

Flawed Authentication Protocol In some SHDs, such as Philips hub, authentication is implemented; however, the authentication protocol used has security flaws. Mahadewa et al. (2018) found that the Philips Hue hub generates authentication tokens for all devices, whether they are authenticated or not. This results in unauthenticated and malicious devices being able to connect to Philips hub and control the smart home network or eavesdrop [35].

De-authentication attack Sun et al. [45] showed that sending 802.11 de-authentication frame to disconnect a light bulb from the access point disabled home Internet connection or forced the light bulb to connect to a rogue access point. The light bulb was designed to remember the state (on/off) in case it was disconnected, and it lacked a physical power switch (on/off). Consequently, if the attacker turned off the light bulb and then performed a de-authentication attack, the user could not turn it back on. In the same experiment, a camera was also found vulnerable to such de-authentication attacks, which could render the camera unusable to users [45].

Information Leakage or Disclosure

Papers included in our analysis show the potential of leakage of information collected by SHDs [40, 45–47]. We have divided the information leakage or disclosure-related vulnerabilities into the following 5 sub-categories:

Log File Information Leakage Alharbi and Aspinal [40] found that the Android app of a camera stored the personal information of end users (such as home address, encryption keys, and WiFi credentials) in a log file, easily accessible to an adversary. They also showed that in some SHD apps, system crashes could lead to leakage of sensitive data, such as device unique identifier (UID), email address, phone number, global positioning system (GPS) location, text messages, and log messages [40]. Johnson et al. [46] claimed that SHD vendors could write this information from Android log file to another file and malicious apps could deliberately cause crashes to obtain this information. This information could be used for user tracking, user behavior prediction, and location determination [46].

Device Information Leakage SHDs have unique identifiers, such as media access control (MAC) addresses and serial numbers. When revealed, such identifiers can be used to permanently track the device and/or its owner. Alharbi and Aspinall [40] found that cameras were revealing MAC addresses, device serial numbers, and device passwords, making it convenient for an adversary to access the camera without any sophisticated attack.

Personal Information leakage Tekeogl and Tosun [48] showed that an adversary could passively listen to a Chromecast device and obtain unencrypted information, which included google account username, video id, time, operating system (OS) name, OS version, device brand and model. In addition, they conducted black box tests to reveal the leakage of remote information (name, brand, model, OS name, and OS version) to an observer [48].

Information Disclosure Sivanathan et al. [43] showed that unencrypted messages (including audio and video) were disclosed by smart home devices, such as Belkin motion sensors, TP Link cameras, Withings scales, and Phillips Hue light bulbs. They also found that an Internet Protocol (IP) printer exposed the last scanned document to an attacker who controlled the printer via its web interface [43]. Bugeja et al. [38] found similar information disclosure vulnerabilities in 'connected' cameras .

Device and Occupant Localization Vulnerable smart cameras connected to the home network can reveal sensitive information not just about location but also about occupants in the home. Sun et al. [45] showed that an adversary could perform traffic analysis by passively sniffing home network traffic to obtain knowledge about the number of occupants and the in-house location of occupants. The attacker would also not risk being detected due to the attack's passive nature [45]. Jia et al. [49] showed that an adversary could effectively perform geo-location prediction in Google Home.

Data Protection Vulnerabilities

It is important that data in a smart home be protected. The data life cycle in a smart home includes collection from SHDs, transmission to hub or cloud, storage in hub or cloud, and processing [11]. In our categorization, data protection vulnerabilities include lack of encryption, weak encryption, and weak server-side protection.

Lack of Encryption True end-to-end encryption, when implemented well, can provide confidentiality of data in transit and also at rest in a storage device or cloud. Most smart phones today have feature of encryption; however, this feature may not be enabled by default [50]. Zhang et al. [51] mentioned that most phones lacked encryption, which allowed an adversary to obtain SHD data easily in case the adversary established physical

or remote access to the phone controlling SHDs. Alharbi and Aspinall [40] found that a Ring doorbell smart camera lacked encryption of video stream from the camera to server.

Weak Encryption Encryption is a commonly discussed solution for sensitive data protection [52]. However, weakly implemented encryption can provide an additional attack vector in case an adversary were to break the encryption. For instance, Sivanathan et al. (2017) showed that a TP Link power switch could be easily broken into due to weak encryption [43]. Encryption vulnerabilities found in the literature review also included plain text key exchange in camera apps [40] and clear text communication from device to cloud in a Chromecast device [48].

Weak Server-side Protection Attackers could easily steal personal information and listen to conversations in a Hello Barbie talking doll due to the lack of data protection in the server [43]. Server-side data protection is an important issue. Users of SHDs tend to trust their vendors in protecting their data [11]. If data related to users is breached, companies not only lose trust of their customers but also bear huge financial losses [53].

Data Manipulation

This category of SHD vulnerabiities includes vulnerabilities that allow an adversary to change configurations, alter data or modify applications in a home network. Pricing cyberattack falls under this category.

Pricing Cyberattack Past research has demonstrated that an adversary could change the data regarding electricity usage by gaining access to a smart meter [49, 54]. This could result in altered utility bills (e.g. higher electricity bills) for a smart meter user and an attacker could reduce his/her bill but increase community peak energy usage as well as

other users' energy bill [49]. Various detection frameworks have been proposed to solve this problem. Researchers have evaluated vulnerabilities in some presented frameworks, such as the lack of net metering in detection frameworks [54].

Voice Interface Vulnerabilities

The domain of smart speakers and voice enabled devices has presented new vulnerabilities in the SHD domain. This category includes vulnerabilities in devices with Voice User Interface (VUI).

Voice Command Attack According to Alanwar et al. [55], audible voice commands (generated by devices such as televisions) and inaudible voice commands (generated by malicious speakers) were able to activate smart speakers and force them to perform actions even when the legitimate user was not present. An adversary with access to speaker-enabled devices in a smart home network could issue malicious commands, leading to fake transactions, burglary, or other unintended actions. For example, in 2015, Amazon Echo devices in users' homes played Christmas music in response to a television advertisement for Alexa, which confused and frustrated many users [56].

Hidden Command Attack Voice commands can be hidden in a way that they appear as noise to human ears. Meng et al. [57] found that an attacker was able to conduct a spoofing attack on a Voice Command System (VCS) and issue a hidden voice command to an SHD. Hence, what appears as noise to a user could be a command given by an adversary to open a garage door, unlock the house or turn up the thermostat [57].

Inaudible Command Attack Meng et al. [57] also found that voice commands can be made inaudible to the human ears. A spoofing attack in which an attacker inputs inaudible

voice commands to a VCS is known as inaudible command attack [57].

Replay Audio (RA) Attack Replay audio attack is a spoofing attack in which the attacker uses pre-recorded voice of a user to fool the voice control system of an SHD [57]. Malik et al. [58] found that smart speakers such as Amazon Echo and Google Home were subject to replay attacks, in which an adversary could place fake orders, reveal personal information (such as the owner's name), and control IoT devices, such as smart doors.

User Behavior Detection

Apthorpe et al. [59] showed that an observing entity, such as a service provider or an adversary, can analyze traffic generated from SHDs to predict the user presence (i.e. whether a user is at home), sleep patterns, appliance usage patterns, occupancy patterns (i.e. how frequently a user is at home), and the frequency of user motion. In this chapter, we refer to this inference as user behavior detection.

Pattern-of-Life Modeling Beyer et al. [60] set up a test bed network including a camera, outlet, motion sensor, and television, and used pattern-of-life analysis tool to analyze data leakage. They found that an adversary could infer the types of SHDs used in the home, identify events (such as user presence), track the user, map the smart home network, and gain access to the home [60].

User Presence Detection Gong and Li [61] showed that smart meters with differential transmission schemes (DTS) were vulnerable to user presence detection and that an adversary eavesdropping the traffic could infer whether the user is at home. DTS is a method for tracking electricity usage of a consumer by reporting power consumption to the utility company only when consumption changes. Since transmission frequency is proportional to

power consumption, the attacker can reveal user presence by observing this transmission [61]. Li et al. [62] discussed a similar attack on smart meters and called it Presence Privacy Attack (PPA).

Service Disruption

Any vulnerability on SHD that can cause partial or complete interruption of access to SHD or its service is categorized as Service Disruption. Hence, this category includes jamming, denial of service, impersonation, and replay.

Jamming An adversary can disrupt network communication by introducing powerful jamming signals leading to interruption of service and battery drains [63]. Jamming attacks were previously demonstrated using smart meters [64].

Denial of Service Denial of Service (DoS) attack on 802.15.4 media access control (MAC) in Zigbee devices was shown to cause disruption of service [65].

Impersonation Smart meters were shown to be vulnerable to impersonation, where an adversary could introduce rogue (or fake) device to appear legitimate [64].

Replay In LIFX lightbulb system, an attacker was able to intercept and replay User Datagram Protocol (UDP) packets to eavesdrop the network and control a light bulb [35]. Feng et al. [66] showed that an attacker could replay pre-recorded video frames without motion to replace those with motion, to compromise the alert or alarm system of security cameras and hide the malicious behavior.

Other Vulnerabilities

Twenty-six other vulnerabilities were found in various SHDs. In Table 2.2, we show the names of these additional vulnerabilities, the devices they were found in, and the references to related articles.

Table 2.2: Vulnerabilities in SHDs.

Vulnerability	**Device**	**Reference**
Access to remote data	Nest thermostat	[36]
Account lockout mechanism	camera	[40]
Authorization code compromise	Google Home	[67]
Brute-force attack	plug (Edimax SP-2101W)	[42]
Cross-protocol vulnerability	cross-protocol devices	[43]
Cross-site request forgery	camera	[38]
Cross-site scripting	camera	[38]
Design flaw	Haier SmartCare	[68]
Device scanning attack	plug (Edimax SP-2101W)	[42]
Firmware attack	plug (Edimax SP-2101W)	[42]
Flawed/lacking TLS implementation	camera	[40]
Home Area Network ID (HANID) conflict	smart meter	[69]
Intrusion	smart grid	[70]
Key management (SILDA protocol)	smart grid	[71]
Lack of control to administration commands	hub	[35]
Light bulb attack	lightbulb	[72]
Mis-response to discovery request	hub, Chromecast	[35]
Overprivilege	SmartThings	[73]
Over-privileged app	Camera	[40]
Rogue controller injection	Z-wave controller/gateway	[74]
SEP vulnerabilities	Smart grid	[75]
SH network compromise	Google Home	[67]
Spoofing attack	plug (Edimax SP-2101W)	[42]
Unnecessary open ports	camera	[40]
Unprotected WiFi hotspot	light bulb	[35]
Use of insecure underlying protocols	hub	[35]

2.3.2 Application Vulnerabilities

SHDs are usually controlled by users through associated applications running on smartphones. We found two application vulnerabilities in our literature review: home network infiltration [76] and data leakage [77].

Home Network Infiltration Malicious apps can make their way through app stores and then to the home network to cause larger attacks such as distributed denial of service (DDoS) [76].

Data Leakage Ahmad et al. [77] showed that mobile OSs, such as Android, had limitations that allowed data leakage from end-user devices to vendor servers as well as unintended recipients.

2.3.3 Communication Vulnerabilities

In this section, we discuss data leakage and protocol vulnerabilities.

Traffic Analysis Sanchez et al. [78] showed that even with proper encryption, an attacker could analyze WiFi traffic to infer sensitive information, such as inventory of SH devices, device functions and relationships, and user behavior.

Protocol Vulnerabilities Past research has revealed weaknesses in the RPL protocol [79] and proposed improvements [79, 80]. Fan et al. [81] discussed time synchronization issues in PTP protocol (also called IEEE 1588 Precision clock synchronization protocol), which could cause inaccurate device functions due to device receiving wrong time information.

Past research also shows the possibility of the following six attacks on SHD communication:

- Jamming: An adversary can disrupt the network communication by introducing strong jamming signals leading to denial of service attack as well as SHD battery

drains [63].

- Guaranteed Time Slot (GTS) attack: An attacker can disrupt the communication between SHD and its gateway, causing collision, corruption and retransmission of packets. This leads to a loss of communication and DoS attack [63].

- Acknowledgement (ACK) attack: An attacker eavesdrops communication, hijacks packet and sends fake ACK to trick the sender. This leads to the attacker taking control over the smart home network communication [63].

- XMPPloit: XMPPloit can force a SHD to not encrypt the communication, allowing eavesdropping and data leakage [63].

- Eavesdropping: Unencrypted communication allows an attacker to decipher sniffed communication causing a breach of confidentiality [82].

- Denial of Service: Attacker can use malicious traffic to render the home network unresponsive and the user cannot access the home network services [82].

2.3.4 Software Architecture Vulnerabilities

Liu et al. [83] found the following ten vulnerabilities in the Joylink home automation architecture:

WiFi Credential Theft WiFi credentials were transmitted after being encoded one character at a time following the IP address. This allowed an adversary to easily steal WiFi credentials and access home WiFi without authentication [83].

Vulnerable Crypto Key Management The Joylink architecture utilized a vulnerable key generation technique and a local adversary could launch a man in the middle (MiTM) attack [83].

Traffic Decryption The Joylink architecture utilized a vulnerable crypto key management technique and a local adversary could launch MiTM attack and decrypt all traffic, thus allowing breach of confidentiality of sensitive information [83].

Device Hijacking The Joylink architecture utilized a weak communication security and a local adversary can obtain the MAC address of a user device, log into its own cloud account, hijack the device and control it remotely [83].

Out of Band Device Control An attacker was able control the SHD by creating a fake server, without accessing the cloud account or the app [83].

Device Impersonation The Joylink architecture's lack of authentication allowed an attacker to log in to a cloud account, activate a user device with a spoofed MAC address that was easy to obtain due to poor crypto management [83].

Firmware Modification The Joylink architecture's lack of verification of downloaded firmware made it vulnerable to malicious firmware from attackers [83].

Visible Data Communication Control commands and uploaded data were visible to an observer, that could lead to private information being revealed [83].

WiFi Credentials on the Cloud WiFi credentials were uploaded to the cloud server, even when there was no need for this private user information to be sent to the cloud [83].

Weak Key The Joylink architecture used a timestamp value as an Advanced Encryption Standard (AES) key, made it easy for an adversary to predict the key (due to a small key space) and to reveal information collected by the SHD app [83].

Reverse engineering and source code analysis of SmartApps performed by Fernandes et al. [84] showed that more than half of the 499 apps were **over-privileged**, and apps retained unnecessary permissions even when the user denied them. OpenHAB[4] and IoTOne were presented as solutions to this issue [73].

[4]https://www.openhab.org/

Web attacks, such as **SQL injection** and **unauthorized access to sensitive data**, were possible due to poor use (or exploitation) of Application Programming Interfaces (API) in the Spring framework, an open source framework for apps [85].

2.4 Solutions to SHD Vulnerabilities

In this section, we discuss the solutions to SHD vulnerabilities proposed by investigators int the past.

Solutions to **authentication vulnerabilities** in SHDs included the use of the following four authentication mechanisms [35, 39, 39, 42–44]:

1. Requiring the use of credentials, such as username-password combination
2. Enforcing the change of credentials
3. Protecting the authentication credentials
4. Ensuring that the authentication protocols used are up-to-date, strong and unbroken

Two-factor authentication has been investigated as a potential approach to strong authentication in SHDs. Crossmand and Liu [86] proposed Smart Two-Factor Authentication, in which a company gives its user a smart card that produces (and stores) a token for two-factor authentication at the request of the user. Researchers have recommended that SHDs must have a physical switch for the user to manually turn the device on/off, and a default fail-over state so that an adversary can not render the device unusable [45].

Three main solutions to **information leakage and exposure** include limiting or restricting the use of personal information for logging and debugging purposes [40], protecting sensitive device information [40], and encrypting sensitive information [40, 51, 74].

Data collected by SHDs needs to be protected in all stages: collection, transmission (device to hub, hub to cloud), storage (in hub or cloud), and processing. Encryption is often used to protect data, but it needs to be implemented without flaws and encryption keys need to be protected too [36, 40, 51, 74, 82, 87]. Salami et al. [87] proposed the Lightweight Encryption for Smart homes (LES), an encryption technique with low overhead and computation requirement, and identity-based stateful key management. Further research is needed though to evaluate the use of such encryption techniques in various categories of SHDs.

Maintaining data integrity in smart meters is crucial for the accuracy of electricity bill and protection of smart meters and the smart grid from data manipulation attacks. Various pricing cyber attack detection frameworks have been proposed, such as the Electricity Pricing Manipulation Detection Algorithm [88], partially observable Markov decision process (POMDP) based smart home pricing cyberattack detection framework [54], and single event detection technique based on support vector regression [89].

As a solution to audio vector attacks, Alanwar et al. [55] proposed EchoSafe, a sound navigation ranging (SONAR) based active defense mechanism, that checks for the presence of the user as soon as the smart speaker is activated, to ensure that commands are executed only if the user is present nearby (in the room). To protect from hidden and inaudible command voice attacks, Meng et al. [57] proposed Wivo, a tool that authenticates the voice input with mouth motions of the user (liveness detection). Replay attack detection approaches include higher-order spectral analysis (HOSA)-based replay attack detection approach [58] and Wivo [57].

User presence attack and behavior inference attack are usually mitigated by introducing fake traffic into a user's smart home network to minimize the likelihood of an inference to occur. Beyer et al. [60] proposed a technique called MIoTL (Mitigation of IoT Leakage),

which introduces fake traffic to the home network using (a) a device shadow to protect from identifying and classifying devices, and (b) a MAC shadow to mitigate user tracking. Gong and Li [61] proposed a similar approach for addition of null packets to the smart meter traffic during idle times to emulate busy times, confuse the observer, and mitigate user presence detection. Li et al. [62] proposed a similar method called Artificial Spoofing Packet(ASP), which added dummy packets to the transmission to trick an eavesdropper and mitigated user presence detection.

To mitigate denial of service attacks in the Zigbee protocol, Whitehurst et al. [65] proposed integrity checks on received packets (including acknowledgments) to make it difficult for an adversary to forge packets. Namboodiri et al. [64] proposed SecureHAN to combat jamming, impersonation, replay, and repudiation attacks. Feng et al. [66] showed that video replay attack in cameras could be thwarted by hardware isolation of the motion detection module.

To prevent home network infiltration via SHD apps, developers could employ network traffic analysis [76]. Data leakage through apps could be prevented by restricting app downloads only from home automation app stores, and by establishing fine grained policies to improve the communication between home automation apps and non-home-automation apps [46].

Lastly, five articles in our literature review present intrusion detection systems (IDS) as a method of protecting the home network [69, 90–93]. The proposed IDS solutions are presented as proofs of concept and prototypes. SHD users will benefit from fully functional tools available for consumer use.

2.5 Discussion

The systematic literature review showed 153 vulnerabilities in 75 devices. We found little consensus in the naming of the vulnerabilities. So, we categorized them based on vulnerability characteristics and similarities of the attacks. Based on the architectural components these vulnerabilities were found in, the smart home network presents many attack surfaces making it harder to fully protect the home network from adversaries. The attack surface of a home network includes:

- smart home device, including hardware, operating system, and applications
- communication protocols, that run on the SHD, controller or hub, and home router or gateway
- smart phones used to control SHDs, including phone hardware, operating system, and applications
- home automation software or software framework
- software securing the home network

The attack surface increases as the number of devices and features in the smart home grows. New methods of attack are also introduced, such as home burglary and fake orders through attacks on VUI [94]. Thus, providing security and privacy in the smart home is challenging.

It is clear that the authentication vulnerabilities category was the largest, with 8 subcategories. The lack of authentication poses threats to a smart home. An attacker may be able to control someone's door lock, garage door opener, thermostat or coffee maker and issue malicious commands. Evidently, there is a need for SHD manufacturers to implement

authentication properly to address this issue and allow only authorized users to control an SHD.

In section 2.3.1, we presented that research literature showed default credentials vulnerability was found in 7 SHDs. It is argued that market competition and the pressure to create low-cost SHDs in a short time frame has led to the issues lacking or poorly implemented authentication, which provide an additional (and easy) vector for adversaries to enter into the private home network. Baby monitor hacks [25] and Mirai botnet [95] that appeared widely in news were primarily possible due to default credentials. In order to prevent large scale attacks like Mirai in the future, default credentials vulnerability must be addressed in all SHDs. The issue of lack of authentication can be addressed by manufacturers requiring authentication credentials in their SHDs, and by developers requiring the user to change default credentials during device setup [40, 41].

Past user studies have shown that users care about data protection and their privacy, but trust the vendors to provide appropriate data security and privacy protection [11,25,29]. Manufacturers need to reduce vulnerabilities in their SHDs by following secure development practices and also use up-to-date, secure protocols for communication with other devices to reduce cross-protocol vulnerabilities.

It is challenging for SHDs with limited memory and computational power to locally encrypt data before sending to a cloud server. The data in transit, thus, risks potential breach of confidentiality. So, encryption techniques suited for such environments need to be evaluated.

Next, we will summarize open research areas in the area of smart home security and privacy, and discuss the limitations of our work.

2.5.1 Open Research Areas

We have identified the following open research areas in the security and privacy of SHDs:

- Security analyses of SHDs, protocols, and software frameworks, especially of newer models, to find out vulnerabilities and develop solutions.
- Authentication mechanisms suitable for low power, low-resource, low-cost SHDs.
- User-centric methods of enforcing change of default credentials and setting up strong credentials.
- Secure methodologies for storing and managing credentials in the smart home network.
- Data protection techniques, such as encryption, customized to SHD environment.
- Study of whether data manipulation attacks, similar to those in smart meters, are possible in other SHDs, and development of solutions, if necessary.
- Development and evaluation of solutions to voice interface vulnerabilities, as VUI attacks are evolving with the popularity of voice interfaces.
- Best practices in data protection at various stages of data life cycle including use, rest and transit.

2.5.2 Limitations

Our study has several limitations. Our study excludes papers not published on ACM and IEEE databases. It does not include research papers about SHD vulnerabilities from other databases that did not appear in the selected databases. Another limitation is that we

have included articles published only in English and not included articles published after March 2019.

Moreover, the literature search keywords were chosen to match the goal of our study as much as possible. However, the search keywords used might have left out articles that included SHV information but did not use the selected keywords.

Finally, many manufacturers and vendors do update their software with patches as soon as a vulnerability is published, and protocols with flaws are updated. Thus, a limitation of our paper is that some vulnerabilities may no longer exist. However, the vulnerabilities information, categorization and taxonomy will serve as a basis for future research in newer types, brands and models of SHDs and their components.

2.6 Conclusion

We performed a systematic literature review to study 153 SHD vulnerabilities from 98 papers, categorized the vulnerabilities based on their characteristics, and proposed a taxonomy for the attacks. We also discussed solutions to these vulnerabilities from research literature and presented potential opportunities in the area of SHD security and privacy research.

A smart home is a mix of heterogenous devices, controllers, protocols, and software from wide variety of vendors and manufacturers. In addition to the efforts of adding security and privacy tools to SHDs, more research is necessary to design SHDs with security and privacy in mind. A combination of built in security and privacy features with home network protection tools can make mitigation stronger.

Most of the solutions proposed are prototypes, not fully functional tools ready for consumer use. SHD users will benefit from deployable tools. Future work should focus on developing more working solutions that can be made available to the consumers for the

protection of the smart home.

Chapter 3: Eliciting Privacy Concerns for Smart Home Devices from a User-Centered Perspective

3.1 Introduction

The Internet of Things (IoT) includes smart home devices that automate user tasks at home. According to a report from 2017, there exist 8.4 billion connected gadgets [3] and the IoT field is expected to continue growing. Smart home technologies, a subset of IoT devices, are also expected to face significant growth. Business Insider Intelligence estimates that 1.8 billion smart home devices were sold by 2019, generating an estimated annual revenue of $490 billion [4]. In 2017, the estimated sale of smart home technologies in the United States (US) was 39 million units (35.9 million devices and 3.1 million hubs). Based on these data, one in every ten US households has at least one smart home device [96].

The primary motivator for users of smart home devices is the convenience that such devices offer. These technologies also promise comfort, control, safety and security [96]. However, the rise in adoption of smart home technologies presents new challenges to security and privacy [6, 7]. In 2016, the Mirai botnet affected hundreds of thousands of IoT devices —including Internet Protocol (IP) cameras, Digital Video Recorders (DVRs), routers, printers and Voice over Internet Protocol (VoIP) phones. In this attack, a large scale distributed denial of service (DDOS) against multiple targets was executed. Targets of this attack included Krebs on Security, Lonestar Cell and Dyn, a popular Domain Name System (DNS) provider. The DDoS on Dyn affected popular services such as Amazon,

Github, Netflix, Paypal, Twitter and Reddit [27].

As the number of smart home devices grows, attacks of such nature are also likely to grow, not only in scale but also in sophistication [97]. Do users know about it? Are users concerned? What are they primarily concerned about? To address such questions, further investigation focusing on users concerns about smart home privacy is needed.

Previous studies about user adoption of smart speakers found privacy as the primary reason for non-adoption of these devices and adopters placed value on their privacy [98]. Privacy concerns of users are positively correlated to their perception of privacy importance [99]. More specifically, in a study of fitness trackers, privacy concerns of users were found to be directly related to their valuation of data collected by the tracking devices [100]. Privacy behaviors also depend on context and evolve over time [101]. However, little work has been done to understand privacy concerns of smart home users [17,102]. Understanding the privacy concerns of users of smart home devices helps stakeholders, investigators, and vendors to develop hardware and software solutions that are better suited to address privacy concerns of users. Improving smart home technologies with privacy-enhanced solutions has potential to boost user confidence and trust in such technologies [102, 103].

To elicit privacy concerns from a user-centric perspective, we analyzed thoroughly privacy-related online reviews of users of smart home hubs – including Amazon Echo [104], Google Home [105], Wink Hub 2 [106], and Insteon Hub [107]. One hundred twenty eight reviews posted between October 2016 and October 2017 and expressing privacy concerns were retrieved and classified according to their contents, security principles involved and temporal dimensions regarding the automation process and information lifecycle, from data collection to sharing.

This chapter contributes an understanding of smart home users' privacy concerns and

Table 3.1: Number of reviews for five smart hubs. Google Home (*) reviews were extracted from bestbuy.com. All other reviews were extracted from amazon.com.

Device	**Number of Reviews (n=66,656)**
Amazon Echo Dot 2	57,079
Google Home *	6,902
Samsung SmartThings Hub	1,856
Wink Hub 2	558
Insteon Hub	261

provides a discussion on how to improve the design of smart home devices with privacy-enhanced solutions.

3.2 Methodology

To analyze privacy concerns of users, five mostly-used smart hubs were selected, namely Amazon Echo Dot 2, Samsung SmartThings Hub, Google Home, Wink Hub 2 and Insteon Hub [108, 109]. There was no single portal containing customer reviews of smart home devices. Therefore, we selected amazon.com and bestbuy.com as our sources as they contained the largest number of user reviews on these selected products (n=66,656). Table 3.1 shows the number of reviews and the source for the five selected devices.

We filtered out the reviews that did not include the keyword 'privacy'. Our resulting dataset included 128 reviews: 120 for Amazon Echo, six for Google Home, one for Wink Hub 2, and one for Insteon Hub. No privacy-related reviews were found for Samsung SmartThings hub [110]. The reviews in our data set dated from October 2016 to October 2017 and included reviews that were classified as verified purchases by amazon.com and bestbuy.com.

Table 3.2: Codebook showing codes/themes for analyses performed in the study

Concern	**Sentiment**	**Temporal**	**Principle**
	Positive	Collection	Confidentiality
Specific	Neutral	Transmission	Integrity
Non-specific	Negative	Storage	Availability
		Sharing	Authentication

We extracted and coded the reviews manually, and analyzed the qualitative data. For sentiment analysis, the reviews were manually read and then coded as positive, neutral or negative. For temporal analysis, the reviews were coded based on the life cycle of data in the smart home architecture, namely collection, transmission, storage and sharing. For security principle analysis, the reviews were coded based on the security principles confidentiality, integrity, availability and authentication. Table 2 illustrates the codebook showing the main themes of coding.

Our methodology was inspired by [111], an analysis of privacy concerns in user comments on wearable devices involving exploratory and empirical methods.

3.3 Results

3.3.1 Specific Concerns

While 33% of the reviews were general, in which the users mentioned privacy concerns but did not specify their privacy concern in detail, 67% of the users specified precisely what their privacy concerns were. The top privacy concern was that these devices were always listening to their conversations. Five other privacy concerns sorted per order of popularity were: (1) tracking of users, their actions and preferences, (2) storage of conversations and

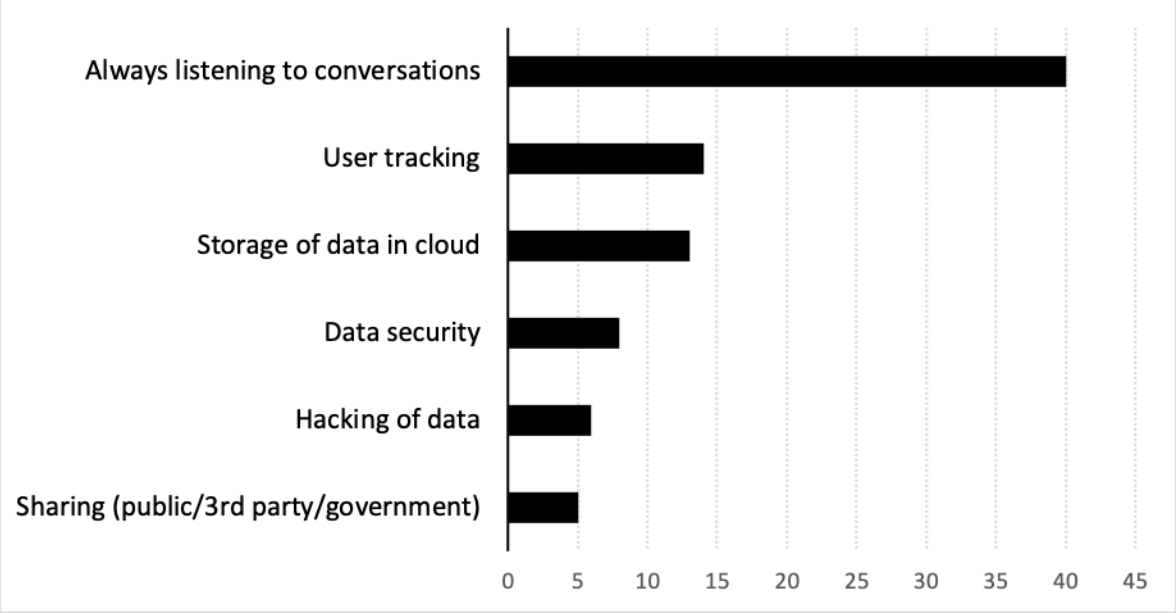


Figure 3.1: Top six themes in users' privacy concerns and their frequencies.

their transcripts (for audio conversations) in the cloud, (3) the lack of security of such content in the cloud, (4) the potential of private conversations to be hacked, and (5) the likelihood of such information to be subject to legal discovery by law enforcement and eventually disclosed publicly. Figure 3.1 depicts these concerns and their frequencies of occurrence.

The identified concerns resonate with recent studies that discuss and demonstrate various smart home vulnerabilities, such as network observing, tracking, eavesdropping, user behavior prediction, data leakage, data theft, identity theft, social engineering, disruption or denial of service and software exploitation [97, 112, 113].

Users in our analysis were concerned that microphone-enabled smart home devices were recording private conversations, background conversations and noise. Such contents

included personal conversations, such as family members speaking to one another, and conversations not directed to the device. For example, Amazon Echo is expected to record only conversations following the wake-up word 'Alexa'; however, users reported to find recordings of private conversations not including such wake-up word.

According to one user, "Echo thinks my TV is talking to it. Very often, without the word Alexa being said the Echo will start jabbering or playing a song while watching TV." Another user reported that when he/she checked the history of the requests made to Alexa, he/she found many recordings of strange people talking that did not live in the house. He/she mentioned that "It even randomly records things in my house like my dog barking, the TV audio and a regular conversation without requesting 'Alexa'... I'm either going to send it back or keep it turned off unless I want to use it. I don't want the world to know what's being said in the privacy of my home and I don't want to hear what's going on in their homes. Very scary."

Users expressed that they believed the features and convenience offered by smart home technologies outweighed their privacy concerns, which led them to use smart home technologies despite their privacy concerns.

3.3.2 User Sentiments

We analyzed the sentiments expressed by users in their privacy concerns, by coding them as negative, neutral or positive. We found that user sentiments associated with privacy concerns are mostly negative (74%). Among the remaining 26% reviews, three quarters (75%) expressed positive sentiments and the rest of them were neutral. Examples of reviews are shown in Table 3.3.

Table 3.3: Three examples of reviews with negative, positive and neutral sentiments

Sentiment	Sample Reviews
Negative	"I am a bit paranoid that such a device will support furthering the evolution in the loss of privacy." "There's no privacy because every question that is asked is seen on the Alexa app which it should be private. I am disappointed with it."
Positive	"We love it even though we were initially concerned about it eavesdropping and related privacy issues."
Neutral	"For those concerned about privacy (like a few of my friends) just unplug when you don't want the device to listen in on your conversations or activities."

3.3.3 Temporal Analysis

In general, smart home devices collect information from users, transmit to a remote server on the cloud for storage, processing, and sharing. In a smart home, the life cycle of data ranges from collection and transmission to storage and sharing.

Based on our investigation, data collection stands out as the stage that concerns users the most. As Table 3.4 illustrates, about half (49%) of the 128 reviews analyzed mentioned the user concern was related to data collection, followed by storage (23%), sharing (9%), and transmission (2%).

3.3.4 Security and Privacy Principles

The breach of the four main security principles—Confidentiality, Integrity, Availability [114], and Authentication [115]— results in critical consequences for users. Confidentiality deals with keeping data secret from unauthorized parties using techniques like encryption.

Table 3.4: Four examples of privacy concerns quoted from end users' reviews considering the lifecycle of data from collection and transmission to storage and sharing

Stage	**Examples/Tasks**	**Sample Reviews**	**Percentage of Reviews (n=128)**
Collection	Devices with microphones and sensors collect data	"It is connected to the internet and listens and records all of the time, not just when you talk to it." "Everything you say to it is recorded... even things you don't say to it"	49%
Transmission	Collected data is usually transmitted to a remote server or cloud for storage	"Records and uploads your conversations automatically" "I would prefer to remove the cloud or any data sent which is collected, retained and resold as I have no need to control outside my network and have ways I can connect to my local network remotely without their spying servers being involved."	2%
Storage	Data is stored in a remote server or cloud	"This device records and stores everything it hears offsite forever." "RECORDS everything you ask it. It keeps the text of what you ask, but it also actually keeps the audio recording of what you asked it"	23%
Sharing	Vendors may share this retained data to third parties or collected data may be requested by law enforcement	"I attempted to read all of the terms and conditions but soon found out that agreeing to them means that third parties can end up with my voice print!" "It is another window into your privacy so that they can build a more precise profile on you for marketing purposes."	9%

Integrity deals with prevention of tampering of data. Availability ensures data is available to authorized parties when necessary and authentication checks credentials of parties trying to access data [116]. An insight into the principles that concern users the most can direct research and development focus towards those areas. As expected, users did not clearly utilize these terms in their reviews. Hence, we coded and mapped the reviews to these principles. Content of some reviews did not fall into any of the four principles. Such reviews could not be coded for this analysis but were still used for other analyses. Among the 73 reviews that were successfully mapped to a principle, 90% were related to confidentiality and 10% were related to authentication. None were directly related to integrity and availability. Thus, confidentiality of data was a leading privacy concern of users of smart home devices.

3.3.5 Privacy Protection Strategies

Users of smart home devices who expressed concern about privacy seemed to adopt individual controls to address their concerns. Our analysis revealed that users concerned about privacy adopt three major approaches. The first approach consists in deleting the history of audio and text data when possible. According to users, a common drawback of such products is the inability to delete collected and stored data in bulk. Having to delete large collection of data one-by-one is a major annoyance for users.

The second approach consists in turning off the device when it is not in use. Devices with the ability to turn off the microphone seemed to be the favorites for concerned users. Switching the microphone off or even the entire device when not in use is a user practice to prevent disclosure and misuse of private information mainly by ensuring that the device is not listening and recording private conversations that are not directed to it.

The third approach was deciding to use a product from a vendor who has demonstrated

to advocate for data privacy. Users expressed confidence with companies that stood up against providing data to law enforcement. For instance, one user expressed confidence in trusting the vendor to fight for the privacy of user data: "I also trust this vendor and they have shown to fight for users' data privacy so far."

3.4 Conclusions

3.4.1 Recommendations for Privacy Enhancing Solutions

Online reviews in the dataset analyzed included six suggestions for enhancing privacy in smart home technologies. We discuss those suggestions and also add our own recommendations for privacy-enhanced smart home technology solutions. Author recommendations are based on team discussion and experience. Recommendations in both categories are presented next in alphabetical order.

3.4.2 User-suggested Recommendations

Advocacy. Users asked vendors to advocate for more data protection. Such protection can be ensured by utilizing and informing users of techniques used to safeguard data from insider and outsider attackers. Users mentioned they trust vendors that stand up against the release of data collected to third parties.

Interface. Another user suggestion is that vendors provide a user-friendly interface with the ability to view, manage and delete data collected by the devices.

Local Control. Users suggested that vendors develop locally controlled hubs for smart home automation instead of using the cloud. A local storage hub will eliminate the need to store data in the cloud and elevate user trust by eliminating privacy concerns related to data stored in the cloud.

Policy. Users showed interest to understand what data is collected, how the data collected is or will be used, and who has access to it. Users suggested vendors clearly state the policies regarding collection, storage, sharing and protection of data.

Safeguarding. Users were concerned about protection of data in the cloud by the vendors. They suggested that vendors take steps, such as encryption, to protect their data from being hacked.

Trust. Users mentioned that they prefer the ability to control the collection of smart home data. Users expressed frustration over the inability to control the data collection and recordings. They suggested that vendors provide a way to manage and especially to delete the collected data.

3.4.3 Author Recommendations

Accuracy. Manufacturers of smart home technologies must address programming flaws and lack of accuracy, for example, accuracy in recognizing wake-up words (words that activate a voice enabled smart home device) and eliminating false positives.

Authentication. Smart home devices should provide mechanisms to authenticate the user to avoid unwanted users from using the devices or accessing their services in an unauthorized manner.

Data Protection. Vendors should employ data protection techniques, such as encryption, to safeguard data in all stages of its lifecycle —collection, transmission, storage, and sharing.

Opt In. Data collection is necessary for vendors to improve the services offered to users. However, users are concerned about excessive data collection and have questioned it. Vendors can address such concern by providing users with the option to opt-in for such data collection. Making data collection an opt-in rather than mandatory can bring in more

users who would otherwise not utilize such devices due to privacy concerns.

Policy. Providers of smart home technologies can gain higher consumer confidence by clearly stating what data they collect from the smart home device, how they transmit the data collected, how they handle smart home data and what measures they take to safeguard the data for ensuring its confidentiality and privacy.

Regulatory Framework. The data collected from smart homes should be subject to data protection law or regulation. A legal framework for the protection of data collected by smart home devices is necessary. Industry-level guidelines and best practices in smart home data protection are needed to make the smart home domain more secure and more private. The user-vendor-government trio needs to work collectively to preserve privacy in the age of smart homes. Past research [117] has also shown that users expect strong legal protection of their data.

Stop Technique. When a device is recording conversations, it is essential for the device to know when to stop recording. If a device does not know when to stop recording the conversation, it can record private conversations not directed to it. We recommend introducing a stop word (for example, 'thank you', 'bye bye', bye [name of device], etc.) or a stop technique. Such a method can be beneficial in informing the device of the end of the conversation, indicating it to stop recording or collecting data. An indicator light is recommended as a method of informing users of the recording action.

Visibility. Placing the on/off switch in a visible location and an indicator light depicting the recording action can elevate the comfort level of concerned users. Live status may also be helpful concerning collection of data.

3.4.4 Limitations

The extraction, reading and coding of reviews was performed manually. The resulting dataset contained more reviews provided by Echo consumers than other devices. Thus, there may be a bias towards Echo. The study focuses on analyzing privacy concerns of only consumers that chose to write an online review for the product purchased. Demographic analysis was not feasible as the online reviews lacked such information but the users posting online comments are known to be mostly tech savvy, young, and literate [118]. .

Privacy may be addressed without explicitly mentioning it. This study was limited to the content analysis of reviews that explicitly mentioned the word 'privacy'. Another limitation is that users who post comments tend to have more extreme opinions about those devices.

3.4.5 Next Steps

In this chapter, we analyzed privacy concerns of smart home device users to shed light into privacy concerns of actual consumers and we discuss recommendations for making the devices more privacy preserving. We expect this chapter to motivate researchers, developers and manufacturers to develop privacy-enhanced smart home solutions.

We will further explore smart home privacy concerns through complementary research methods including responses from an online survey. It is likely that people who are concerned about privacy are choosing not to use such technologies [5]. The next chapter will elaborate on an analysis of concerns of non-users of smart home devices comparatively with those of users.

Chapter 4: Privacy Concerns about Smart Home Devices: A Comparative Analysis between Non-Users and Users

4.1 Introduction

The growth of Internet of Things (IoT) devices worldwide has led to an increase in home devices that are connected to the Internet, either directly or through a centralized device, such as a hub or controller [119]. In this chapter, we refer to these home IoT devices as smart home devices (SHDs). Participants who report using SHDs are referred to as users and those who report not using SHDs are referred to as non-users. Both users and non-users can be subject to environments such as rental spaces and common spaces with IoTs. Such people whose become part of data collected by smart devices in hotels, rentals and other common spaces are referred to as bystanders or accidental users [120]. We did not include bystanders in this study.

Researchers have characterized privacy risks in SHDs [14] and privacy concerns of SHD users have been widely studied [11,13,121–123]. However, SHD non-user concerns have been understudied compared to those of users [19, 124–126]. Drawing from Stakeholder theory [20], non-users are as important stakeholders of SHDs as users. An in-depth exploration of non-user privacy concerns is lacking, to the best of our knowledge. Exploring non-user concerns provides academia, industry and policymakers an opportunity to address open concerns, making SHDs safer, facilitating SHD acceptance [127], and bridging the digital divide [128] by turning non-users into users [129, 130].

To fill this gap, we conducted a survey to analyze the privacy concerns of SHD non-users, and explored non-use reasons and participants suggestions for SHD improvement. We compared non-user privacy concerns with those of users. Our study makes two contributions:

- We provide in-depth understanding of privacy concerns of SHD non-users.
- Our results provide novel insight into how SHD users' privacy concerns differ from those of non-users so that SHD designers can address their concerns in future designs.

4.2 Related Work

In the SHD domain, non-user concerns are understudied so far. It is likely because non-users are difficult to locate and recruit for studies and experiments and are not as coherently grouped as users [127]. At the time of writing this chapter, literature lacks studies focused specifically on non-user privacy concerns. However, some prior studies have included non-users among other participants of user studies. Liao et al. [124] explored reasons for non-adoption of intelligent personal assistants. Lau et al. [19] interviewed 17 non-users of smart speakers to explore why they decided not to buy a smart speaker. Yao et al. [126] included three SHD non-users to explore perceived benefits and risks. Yao et al. [125] included seven SHD non-users in their co-design study of 25 participants. This chapter aims to provide novel insights into privacy concerns of SHD non-users and compares them with those of users.

4.3 Survey Method

All survey-related documents and correspondence materials were approved by our institution's Institutional Review Board (IRB). We recruited participants using snowball sampling and random sampling methods. We announced the study through emails, university newsletters, and twitter. We have shared the questionnaire online [131].

4.3.1 Participants

A total of 93 participants responded to the survey. We discarded two off-topic and incomplete responses and included the remaining 91 responses in our analysis. Nearly 45% (n=41) reported not using any SHD and 55% (n=50) reported using at least one SHD. In this chapter, we refer to the former group of respondents as 'non-users' and the latter as 'users'. Among the 91 participants, 42.9% were female and 51.6% were male. Nearly 43% were 18-29 years old, 26.4% were 30-39, 14.3% were 40-49, 8.8% were 50-59, and 9.9% were 60 years or above. 42.9% reported to be White, 26.4% Asian or Pacific Islander, 9.9% Black or African American, 8.8% Hispanic or Latino, and 12.1% other. 36.3% had a Post-graduate (MS, PhD, etc.) degree, 24.2% Bachelor's, 18.7% High School, 15.4% Associate's, and 3.3% Other. About 57% of our participants had an educational background related to technology (computer science or information technology) and nearly 43% had a non-technology background.

4.3.2 Questionnaire Design

The participants were first presented with an informed consent form and an option to continue or exit the survey. If they continued, they were presented with a basic definition of the term 'smart home' to ensure a common understanding among participants. The survey was titled "Smart Home Survey" to avoid bias recruiting participants concerned about

privacy. To prevent invoking privacy-related opinions, the word 'privacy' was not used in the questionnaire until the middle of the questionnaire where specific privacy concerns were asked.

We utilized skip logic and presented a subset of different questions depending on whether the participants answered 'yes' or 'no' to first question, "Do you use a smart home device?". If a participant responded 'yes' (user), we asked them about number and type of SHDs, use reasons, concerns, suggestions and demographics. If a participant responded 'no' (non-user), we asked them them about non-use reasons, concerns, suggestions and demographics.

We avoided binary questions to prevent introducing acquiescence bias [132]. To ensure validity, questions were inspired or adapted from related work [99, 133–135]. The questionnaire design followed multiple iterations for evaluation and refinement. Questions were tested and revised multiple times for clarity. We pilot tested the survey with three participants, received feedback, and revised it. Participants did not receive any monetary compensation.

4.3.3 Data Analysis

For open-ended responses (non-use reasons, privacy concerns, and suggestions), two researchers conducted thematic analysis using open coding with selective (or axial) coding [136]. We familiarized ourselves with the data by reading the responses and coded each sentence independently by observing the concept present in the response. We then generated categories by observing the similarity of concept in the codes. We achieved an inter-rater reliability of 0.89 using Cohen's kappa. For codes that were different between coders, we discussed and agreed on revised codes. Finally, we agreed on all codes and ensured that the codes were correctly assigned to categories, leading to a final codebook.

We then conducted descriptive and inferential statistical analyses to summarize non-use reasons, suggestions and privacy concerns. We also performed quantitative analysis to compare the privacy concerns between non-users and users.

4.4 Results

This section reports on the SHD distribution of the user group, reasons for non-use of SHDs, privacy concerns, and suggestions made by participants.

4.4.1 SHD Distribution in Participants

Participants reported using 87 SHDs in total. The SHD data includes 11 types of devices (such as cameras and locks) and 20 brands of SHDs (such as Amazon Echo and Google Home). About 66% (n=33) of respondents reported using a single SHD and 34% of them (n=17) reported using multiple (2 to 8) devices. Table 4.1 lists the device type, brand or model, and the respective number of participants. The majority of the participants used intelligent speakers (Amazon Echo or Google Home). This distribution is representative of current SHD market in the United States [135].

4.4.2 Reasons for SHD Non-Use

Most non-users reported their non-use reason to be privacy concerns (68%). Other non-use reasons included lack of interest in SHDs (32%), cost (22%), lack of perceived usefulness (12%), insecurity or potential of hacking (10%), and perceived difficulty of usage (7%).

Table 4.1: SHDs used by participants. Asterisk (*) indicates no brand was reported. Data is sorted per frequency of device category. Numbers in parentheses in the third column represent the frequency of that device. Some participants used multiple devices.

Smart Device	**Total (n=87)**	**Frequency Breakdown by Brand**
Speaker	38	Amazon Echo (25), Google Home (13)
Hub	15	Samsung SmartThings (14), Vera (4), Nexia (1)
Thermostat	11	Nest (7), Radio (1), Emerson Sensi (1), Carrier Infinity touch (1)
Camera	6	Arlo (2), Canary (2), Kuna (1), Blink (1)
Light	5	Philips Hue (3), Halo (1)
Door bell	4	Ring (4)
Plug	3	Kasa smart pug (1), Wemo (1)
Vacuum	2	Roomba 960, Eufy (1)
Door lock	1	*
Television	1	*
Security System	1	*

4.4.3 Privacy Concerns: Non-Users vs. Users

Thematic analysis resulted in 17 codes and three thematic areas of privacy concerns. Table 4.2 shows the themes and breaks down the percentage of non-users, users, and total participants for each code.

The first theme was 'data collection concerns' which included five codes: recording audio/video, tracking occupancy, listening to private conversations, monitoring usage/behavior, and identity theft. About 34% of the privacy concerns codes were categorized under this theme. This category included participant concerns regarding the initial temporal data collection feature where the SHD collects data by constantly listening to the user (such as in case of IPAs) and recording audio, video or both. Most of these concerns

Table 4.2: Categories (bold) and codes of non-user (NU) and user (U) privacy concerns. Non-users were more concerned about collection of data than users (NU>U). Users were more concerned about sharing of data.

Privacy Concerns	**Non-Users (%)**	**Users (%)**	**Total (%)**
Collection of Data			
Recording audio/video	24.39	20.00	21.98
Tracking occupancy	9.76	2.00	5.49
Listening to private conversations	4.88	2.00	3.30
Monitoring usage/behavior	4.88	0.00	2.20
Identity theft	2.44	0.00	1.10
Sharing of Data			
Selling data	4.88	10.00	7.69
Third party data access	7.32	8.00	7.69
Leakage without consent	2.44	6.00	4.40
Marketing data	0.00	4.00	2.20
Protection of Data			
Hacking potential	21.95	12.00	16.49
Data handling	7.32	4.00	5.49
Protecting data	2.44	4.00	3.30
Secondary use	2.44	2.00	2.20
Aggregation	0.00	2.00	1.10
Data abuse	0.00	2.00	1.10
Data loss	0.00	2.00	1.10
Fraud likelihood	0.00	2.00	1.10

were about recording audio or video. Participants were also concerned about SHDs listening to private conversations and those being purposefully or accidentally being recorded. They were also concerned about the consequences of data collection where the SHD allows tracking, such as occupancy, and monitoring the usage behavior or related patterns.

The second theme was 'data sharing concerns' which included 22% of the privacy concerns under four codes: selling data, third party data access, leakage without consent, and marketing data. Participants raised concerns about the selling of SHD data to business

partners or data brokers, third party (e.g. government) access to SHD data, leakage of the data, and the potential of the data being used in marketing.

The third theme was 'data protection concerns' which included eight codes: hacking, data handling, protecting data, secondary use, aggregation, data abuse, data loss, and fraud. About 32% of the codes fell in this category. Participants were mostly concerned about the risks of SHD devices (and data) being hacked and improper handling of data by the SHD company. For example, one participant wrote:

> "My concerns are [...] being hacked and used against me in some way. Such as smart locks, someone could hack it to unlock my doors, or with smart thermometers if it was hacked that person would be able to tell if I was home or not." (P1)

Chi-square test between non-users and users showed that the privacy concerns of non-users differed significantly ($\chi^2 = 8.46, p < 0.05$) from users. Non-users reported higher level of concerns in data collection and data protection themes than those of users (46% vs 24% and 34% vs 30% respectively). This is likely because privacy was a major reason for non-use and collection of data is the first stage in the SHD data life cycle that raises privacy concerns. However, non-users reported fewer concerns in the data sharing theme than those of users (15% vs 28% respectively). This is likely because user participants are already having their data collected by SHDs in use, which naturally raises concerns about how data will be shared for marketing and other purposes.

4.4.4 Participant Suggestions to Improve SHDs

The thematic analysis of participants' suggestions for developers resulted in four main themes: (a) data anonymization and minimization, (b) data protection and security, (c)

transparent data use policies, and (d) user-centric practices.

Data Anonymization and Minimization

This theme included twenty suggestions that SHD devices collect only anonymized data and not include any personal information such that SHD users cannot be tracked. Five participants suggested that anonymization should be 'guaranteed' before data is sent to the cloud. Three participants suggested that vendors provide SHD users the choice to opt out of data collection and monitoring.

Data Protection and Security.

Fifteen participants suggested that manufacturers build devices so that they are less likely to be hacked. Participants suggested developers to study how their devices could be hacked by conducting vulnerability testing, researching cybersecurity incidents and improving security on their devices. Participants suggested providing to the devices more computing power to overcome the limitations to implement security technologies in them. In the words of one participant, "put security first." Six participants suggested developers use encryption to protect the data collected. Three participants suggested manufacturers to allow third party verification on their devices so that users can be confident about SHD security. Participants also suggested implementing authentication, such as passwords, in SHDs.

Transparent Data Use Policies.

Transparency was the main theme of suggestions from twelve participants. Eight participants sought "more transparency and control over their data," and clarity on "how

providers use collected data, how they store, and share the data." Twelve participants suggested that manufacturers inform the users clearly and succinctly (using not only text, but also images and videos) on "data usage, data collection, handling of breaches and technical issues, and research data." Several participants also suggested that manufacturers educate consumers about the potential privacy risks in their devices and the ways to mitigate risks.

User-centric Practices.

Six responses contained users as the primary theme. Among these, four participants suggested that developers put users' interests and concerns first, not their own. For example, one participant wrote: "If they [vendors] can do anything to minimize the risks on the devices, they should do it—not put their own interests first and use it to their own advantage." Another participant emphasized the need to put consumers first: "Develop with consumer in mind." Participants sought features to control privacy and desired visible indicators of recording or data collection. For example, one participant wrote:

> "Give users options. Add features providing users the ability to control their privacy. Make it visible when recording, if the device is recording. Make their information accessible." (P56)

4.5 Discussion

We found that privacy was a major reason for non-use of SHDs and that SHD non-users had privacy concerns regarding SHDs. Based on our empirical analysis of user and non-user privacy concerns, it is evident that non-user privacy concerns are as important as those of users. We argue that addressing non-user privacy concerns will help reduce tension between users and non-users, especially in shared spaces, such as apartments. Another

novel finding was that data collection and protection concerned non-users the most and data sharing concerned users the most. Our explanation is that users trade off privacy concerns for motivations (reasons) for use. We suggest that future development of SHDs should consider these privacy issues regarding data collection, protection and sharing, so that users can continue to reap the benefits of SHDs with increased confidence and decreased concerns, and non-users can consider using SHDs to reap the benefits of SHDs. Designers, manufacturers and developers should take this primary concern into consideration in the design, development and enhancement of SHDs to gain consumer trust and increase product adoption.

4.6 Limitations

Our findings are skewed more towards educated users, but reflect the current SHD user population that largely includes educated and tech-savvy early adopters [19]. Secondly, survey instruments have a tendency to measure attitudes rather than actual behavior. So, the findings reflect reported attitudes rather than actual user behavior. Despite these limitations, we believe that our study provides valuable insights into SHD privacy concerns, and breaks ground into understanding reasons for SHD non-use and privacy concerns of non-users.

4.7 Conclusions

In this chapter, we reported our work aimed at understanding user and non-user privacy concerns regarding SHD devices. We analyzed the privacy concerns reported as well as reasons for use and non-use of SHDs. Our findings indicate that both users and non-users of SHDs are concerned about privacy violations caused by SHDs. Non-users of SHDs are

concerned about data collection and its protection, and users are concerned about how their data might be shared and (ab)used by companies. While users reap the benefits of SHDs through usage, their usage is not concern-free. Privacy-concerned users are trading off privacy with other benefits. Enhanced data practices, data protection, and transparency from SHD device manufacturers as well as application providers can lead to more confident users and attract non-users towards usage.

Chapter 5: User-Centric Privacy Controls for Smart Homes

5.1 Introduction

Smart home devices (SHDs) provide consumers with convenient services and safety features through smart locks, smart bulbs for light controls, baby monitors with surveillance cameras, and entertainment through smart TVs and speakers [137]. In general, Internet of Things (IoT) devices are considered SHDs as long as they are used in the context of a private household [138, 139]. SHDs have gained popularity in recent years. As consumers invest more in home automation services, SHDs are expected to reach the homes of more than 1.4 billion people by 2024 [140]. SHDs vary in the device format and specific purposes, however their overarching goal is to facilitate everyday life activities with convenient features, services on demand, information and resources [141]. With the growth of high speed 5G networks, the smart-home ecosystem is also expected to continue growing [142]. SHDs bring disruptive changes to traditional industries [143] thanks to: (1) their intimate and inconspicuous presence on users' lives, (2) large potential to collect data –continuously and from multiple streams– and (3) capability to adapt the environment and services with features and information that meet users' needs on demand.

Locks, cameras, and speakers are examples of Internet-connected devices in a smart home. They serve as intelligent personal assistants that make the home "smarter" by bringing convenient services to residents [144]. SHDs are not only continuously collecting data from users and their surroundings, but also exchanging information directly through the web, often with third-party commercial services on the cloud, such as Google, Amazon,

or Apple [145, 146]. The requests for web services and data exchange pose risks to users' privacy and security [147, 148]. Such risks affect not only smart home residents, but also their guests and bystanders [149].

By having access to multiple data streams in a continuous way, many SHDs access information that is private, confidential, and personally identifiable. When aggregated, the analysis and processing of data streams altogether lead to inferences about users' behaviors and predictions. Data access, forecast, and inferences summed with the transmission of private information from users to external services exacerbate privacy risks for end users [112, 150] and security threats of SHDs [151]. Although US users are willing to exchange personal information to obtain tangible benefits, they are also cautious about disclosing personal information and feel dissatisfied with the current approach adopted by industry with regard to the usage of data collected [152].

Many researchers have conducted studies to decipher users' threat models of SHDs and privacy concerns regarding SHDs. However, even though smart home devices are widespread, the design of effective privacy controls remains an open challenge. To devise user-centric privacy controls for smart homes, joint efforts that combine technical [153,154] and legal aspects [155] as well as socio-technical and user-centric approaches [102,156,157] are needed. Technical studies have examined network defenses, cryptographic models, and machine learning models to classify suspicious activities [158–160]. Socio-technical studies have examined user perspectives through interviews, surveys, participatory design, and focus groups [161–163].

Despite substantial advances focused on understanding users' concerns [5, 151, 164], there is limited translation of users' privacy concerns into user interface and design decisions for customizable privacy controls. So, an in-depth investigation into privacy controls expected by users is necessary to suggest practical design recommendations to aid the

development of privacy-enhanced SHDs.

Thus, to investigate SHD privacy controls desired by users, we interviewed 25 participants and analyzed the interviews' transcripts. We performed thematic analysis of privacy controls expectations of users, resulting in seven design factors and 32 sub-factors from the coding of user interface controls desired by users. We used the interview findings to inform the design of a survey deployed to 440 US adults to confirm the findings of the interviews.

The contributions of this chapter are: (1) unpacking the privacy controls desired by users of SHDs, and (2) devising a privacy control framework to help developers implement user-centric privacy controls.

5.2 Related Work

The adoption of smart home devices grows thanks to their reduction in price and increasing popularity. As electronics become smaller, home appliances also integrate more sensors, amplifying their potential for data collection and embedded 'intelligence.' Smart devices include thermostats, energy monitoring switches, personal assistants, doorbells, smart locks and smart lights. By collecting users' data, such devices become more integrated in users' lives, providing them with convenient services. Despite their advantages, SHDs also lead to several privacy concerns due to their information processing capabilities, heavy reliance on continuous data collection, and exchange of information with external services. The novelty of SHDs also challenges the implementation of privacy-enhanced technologies, since privacy risks are not always known and regulatory practices are either limited or lacking. For example, the General Data Protection Regulation (GDPR) of European Union (EU) is seen as a strict data protection regulation, but it allows the exclusion of domestic data practices through its household exemption clause [21]. In other words, the exemption allows smart home data to be remain unprotected. In the US, there are many data protection

regulations, such as Health Insurance Portability and Accountability Act (HIPAA), but they fall short in protecting even the health information collected from SHDs due to the inadequate definition of 'protected health information' [22].

The scientific literature reports several contributions dedicated to investigate privacy concerns from a user-centric perspective. Prior work has focused on both characterizing users' concerns and addressing it with technical contributions and privacy controls. Concerning the methodological approaches employed in usable privacy, prior studies collected data using multiple methods, such as: interviews [102,156], surveys [154,157], focus groups [13], analysis of online reviews [11], co-design [5, 151] and evaluation [164], case studies [153, 155] and systematic reviews [14, 142].

5.2.1 Privacy

The concept of privacy has been widely studied. According to Clarke, there are four dimensions of privacy: privacy of a person, privacy of personal behavior, privacy of personal communication and privacy of personal data [165]. Due to privacy being a multidimensional [99, 166, 167] and contextual concept [168], the research community has tackled it from different angles, covering mathematical aspects for differential privacy [169], conceptual, economical costs of privacy risks [170,171], legal [138], technical [154], behavioral [161] and cultural aspects [146, 157].

Information privacy is defined as combination of privacy of personal communication and privacy of personal data [172]. Information privacy manifests itself in various levels. The information privacy concerns multilevel framework argues that information privacy concerns (IPC) involve four constructs (individual IPC, group IPC, organizational IPC, and societal IPC), each impacted by multiple factors, such as individual differences, group dynamics, organizational environment, and government involvement [172].

Solove's taxonomy of privacy harms is widely used to understand and characterize various privacy problems [173]. It identifies the major activities leading to privacy violations and categorizes them into four groups: (1) information collection (surveillance and interrogation), (2) information processing (aggregation, identification, insecurity, secondary use and exclusion), (3) information dissemination (breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation, and distortion), and (4) privacy invasion (intrusion and decisional interference) [173].

5.2.2 Users' Concerns

Using online questionnaires, Cannizzaro et al. [157] surveyed more than 2000 UK residents to understand trust aspects in the context of smart home. They acknowledged the risks to privacy and security of the smart home residents but found lack of clarity in the consumers' perspectives about the meaning and value proposition of a smart home [157].

Researchers analyzed reviews of smart home hubs and found that users of smart home hubs were concerned about data collection and leakage of private conversations [11]. Bleaney et al. [174] applied machine learning algorithms to analyze Amazon reviews and identified safety concerns around baby products. Similarly, Winkler et al. [175] extracted Amazon reviews using smoke word list and identified safety concerns about toys. Linden et al. [118] conducted a review analysis of pet wearables and found that users mentioned privacy concerns.

Researchers have interviewed users and found that privacy concerns of users are associated with loss of control, attacks to data and services, trade-offs between functionality and security, and societal implications [5, 102, 149, 151, 156, 162]. With 42 interviews, Zimmermann et al. [151] provided recommendations for privacy in SHDs. Zheng et al. [5] interviewed 11 participants and found that perceived convenience and connectedness lead

consumers to purchase and use SHDs. Their results also indicated that privacy-related behaviors include the choice of manufacturer and Internet provider [5]. The concerns identified were related to advertisers and government. The usage of the data by external entities depend on perceived benefits. The trust on vendors is not verified and the risks of inferences are unknown for non-audio/visual devices. Recommendations have also been provided [5]. Mao [162] interviewed five participants and found that the risk of privacy breach is tied to secret data collection and that lack of controls is a barrier for adoption.

Birchley et al. [156] interviewed 20 participants. They found that the concerns around physical privacy reduce the acceptance of SHDs. They recommended that users should not be burdened with a lot of controls, since privacy risks cannot necessarily be resolved by them even when an option to choose is provided [156]. Zeng et al. [102] interviewed 15 participants and noted gaps in users' threat models due to a poor understanding of technical aspects of smart homes. Their analysis of the interviewees' responses indicates that users were aware of some security issues and applied ad hoc mitigation strategies [102]. Additionally, imbalance of power between the home administrator and residents with regards to privacy controls was also noted [102]. Because privacy in the context of a smart home affects bystanders as well, Marky et al. [149] interviewed guests or visitors. The 21 young adults interviewed shared concerns similar to those of residents; however, they lacked an understanding about data usage or potential controls [149].

Although there is no instrument to measure information privacy concerns specific to smart home users, prior work used Internet Users' Information Privacy Concerns (IUIPC) [176] to gauge the level of privacy concerns among participants. The IUIPC is a 10-item Likert scale that measures privacy concern using three constructs: awareness, control and collection. In our work, we used this validated scale to measure participants' level of privacy concern.

5.2.3 Privacy Controls

From a technical perspective, Lin and Bergmann [154] surveyed privacy solutions and listed key requirements for SHDs. According to them, a gateway architecture is appropriate to manage resource-constrained devices. They also recommend automatic updates of firmware to maintain a secure operating system [154].

Past research has identified lack of privacy controls as a barrier for SHD adoption [177,178]. Some solutions have been developed in this regard. For example, Emami-Naeini et al. [179] proposed prototype privacy labels to help users integrate privacy into their IoT device purchase decisions. Privacy labels facilitate regulations, however they serve as a proxy to indicate how privacy-compliant a device is and do not fully address the issues.

As smart home technologies become more pervasive, the threats, risks and implications to users' privacy increase [180]. Still, due to the novelty of the technology, users' concerns are not fully understood [11]. In addition, privacy risks in smart homes are unclear and mitigation and prevention strategies are unknown [13]. Stakeholders have little to no guidance when implementing new technologies. Strategies to incorporate privacy by design are lacking, as well as evaluation approaches. Prior research shows that user behavior is poorly understood [14], yet it is important to consider users' mental models and attitudes to devise privacy-enhancing controls that are more likely to be accepted, adopted and used in an effective and sustained way.

Research into privacy controls that are desired by users has recently gained momentum. Yao et al. [148] performed a co-design study to identify six factors for privacy designs of smart home privacy controls: data transparency and control, security, safety, usability, system intelligence, and modality. This study is a starting point to contribute to user-centric solutions for privacy controls in SHDs. In another study that examined privacy perceptions of smart home bystanders, Yao et al. [120] made three design suggestions for

privacy: transparency, expressing preferences, and different modes. Haney et al. [181] interviewed administrators and users to investigate user concerns, mitigations and wish lists. They found that users desired data collection transparency, privacy and security controls, security feature transparency, and assistance [181]. In a study aimed at understanding smart home adoption and clustering consumers purchase considerations, Barbosa et al. [182] also examined desired privacy features of consumers and coded them as: control, transparency, access control, consent, strong security, no data collection, no third parties, deletion, identity protection, offline mode, and guarantees of privacy and security.

Study on SHD privacy controls is growing. Design factors, wish lists and feature categories have been explored, but gap exists in how to translate those design factors into user interface design. This chapter describes a study that aims to bridge this gap by generating factors and sub-factors containing privacy controls that can be translated into user interface design [12].

5.2.4 Commercial Tools

There are a few commercial tools available for users to manage privacy in the context of a smart home. For example, Trutzbox [183] is a tool that offers end-to-end encryption, content filter, firewall, antivirus, intrusion prevention, and tracking protection for Internet users [183]. Although not designed specifically for the smart home environment, this tool provides features that a smart home network could benefit from. However, this tool is available only in the German market. Similarly, another tool Fing [1] provides an app and a hardware box that monitors home networks to detect presence, find open ports, and block unrecognized devices; however, it lacks other privacy-specific solutions.

Aretha [184] was developed as a privacy assistant that includes a network aggregator,

[1] https://www.fing.com/

tutor and firewall features; however, this tool was for research purposes only. Similarly, another software designed for research purposes is IoT Inspector[2] which can find IoT devices in the network, display domain names that IoT devices are communicating with, and provide a visualization of network traffic [185].

5.2.5 Distinction from Prior Work

Literature shows that users and researchers have expressed the need for privacy controls. While prior research has found that users seek transparency, security, privacy and the like, user-centric privacy controls for user interface design of smart home devices are sparse. To bridge this gap, this chapter focuses on deciphering the user interface controls desired by participants to mitigate their privacy concerns. Through in-depth interviews, we decipher the privacy controls expected by SHD users. This chapter presents 7 design factors and 32 sub-factors analyzed from over two hundred requirements for privacy of SHDs. We also complement and validate the findings of the interviews through a survey. Adopting a user-centric approach, we develop a privacy control framework that guides designers towards creating privacy controls that meet users' privacy expectations in SHDs.

5.3 Method

We used the sequential mixed-methods approach [186], in which the findings from interviews informed the design of a survey. We describe the design of both studies in this section.

[2]https://iotinspector.org/

5.3.1 Interview Study

To investigate privacy concerns about SHDs and privacy controls expectations of users, we conducted 25 semi-structured interviews. Semi-structured interviews provide a degree of standardization and consistency, while allowing the in-depth investigation of participant responses and seeking clarifications when necessary [187]. Pilot interviews were conducted before finalizing the interview protocol to test for clarity and make adjustments. The pilot interviews were not included in the analyses.

Recruitment

Participants were recruited from the Northeast region of the US. The study was announced online in Twitter and our university's event listserv. The announcement included the informed consent, an option to sign up for the study, and an option to provide contact information for interview. The participants who consented to participate first completed the demographic form, then answered five questions about their experience and privacy concerns about SHDs. Lastly, they explained their specific concerns about privacy per room (kitchen, living room, bedroom, bathroom, and overall) and were prompted to think about the device(s), sensor(s), information collected, information shared, and services that could use the collected data. The interview was concluded after discussing design recommendations for users of SHDs to gain control over their privacy. Each participant received a USD 20 gift card as compensation.

Participants

Among the 25 participants, 52% (n=13) identified as female, 44% (n=11) as male, and 4% (n=1) as other. Participants' age ranged from 21 to 45 years (M=26.68; SD=5.77). Regarding ethnicity, 36% (n=9) participants reported to be Asian-descendent, 28% (n=7)

declared themselves as White (Caucasian), 12% (n=3) were Black (African-American), 12% (n=3) were Hispanic, 8% (n=2) selected two ethnicities (White and Hispanic), and 12% (n=3) selected other.

Concerning the highest educational degree attained, 48% (n=12) participants had a Bachelor's degree, 36% (n=9) had a Master's degree, 8% (n=2) had High School degrees, and 8% (n=2) selected Other. We summarize the participant demographics and the devices owned by participants in Table 5.1.

As shown in Table 5.1, participants owned a variety of devices, such as smart assistants (Amazon Alexa, Google Home), smart lamps (Philips Hue), and smartwatches (Fitbit). Smart speakers were owned by most participants: 72% (n=18). The number of devices per participant ranged from 0-8, with an average of 2.6. Such devices were used frequently (daily, weekly or even a few times a day).

Procedure

The interviews were conducted during October and November of 2020. The online announcement included a link to an online form with an informed consent form to participate in the study and a permission to allow us to contact them for scheduling an interview. Prior to the interview, participants also provided consent for recording. The interview was conducted through Webex[3] and lasted about 60 minutes. Miro[4] (a collaborative tool that serves as a whiteboard) was used to illustrate two examples of smart homes, to frame the study protocol structuring the topics used, and to annotate the participants' comments using digital sticky notes. Figure 5.1 illustrates the template with the frames used in the study.

The first part of the interview included the following questions:

[3]https://www.webex.com/
[4]https://miro.com/

Table 5.1: Summary of participant demographics and devices owned by participants. P#=Participant Number. In Gender column, M=Male, F=Female, O=Other. In Education column, H=High School or below, B=Bachelor's, M=Master's, O=Other.

P#	Gender	Age	Education	Devices
P1	M	18-25	B	Fire Stick, Echo
P2	M	26-35	B	Fire TV cube, LIFX light bulb
P3	F	18-25	M	Alexa, smart plug
P4	F	26-35	B	Nest Hub, Nest Hub Max, Nest thermostat
P5	F	18-25	B	Google Home Mini
P6	M	18-25	M	Alexa
P7	F	18-25	O	Google Home Mini
P8	F	18-25	B	Google Homes, lights
P9	M	26-35	M	Amazon Echoes, Google Nest, smart plugs, Google AIY voice kit, Philips Hue lightbulb, LG smart TV
P10	F	26-35	B	Alexa
P11	O	26-35	B	security camera, Google Nest Mini, Amazon Echo
P12	F	18-25	B	Google Home Mini
P13	M	26-35	B	Google Nest Mini, Amazon Echo, smoke detector, Brava Oven, light bulb
P14	M	18-25	M	Amazon Echo, smart plugs, light switches, Google Home, Apple Homepod Mini, ESP 8266 Microcontroller, Web camera, HomeKit
P15	F	36-45	M	Google Nest, doorbell, Google Nest fire alarms, Google wireless mesh router, Google Homes
P16	F	18-25	B	Amazon Echo, Google Home
P17	M	18-25	H	TV, Echo
P18	F	18-25	B	TV, Home
P19	M	26-35	M	Google Home mini
P20	M	18-25	M	home security system
P21	F	26-35	M	Google Nest Mini (referenced as Google Dot), Philips Hue light bulb
P22	F	36-45	M	low tech thermostat
P23	M	18-25	H	Amazon Echo , Ring doorbell
P24	M	26-35	B	Amazon Echo, Google Home, smart lights, home security camera, Nest thermostat, smart TV, smart plugs
P25	F	26-35	M	smart plug, smart lights, Alexa, Siri

(a) Sticky notes template for privacy concerns by rooms

(b) Sticky notes for privacy concerns by data life cycle

(c) Sticky notes for privacy controls

Figure 5.1: Sticky note frames used in the online whiteboard canvas.

1. What is a smart home?

2. What devices do you use?

3. What are the benefits of these devices for you?

4. What are the privacy concerns you have, if any?

5. What are the privacy controls you use, or would like to use?

In the second part of the interview, to dive in depth into privacy concerns, we began the online collaborative session by presenting two illustrations of a smart home. One image showed a three-dimensional picture of a two-floor house with several examples of devices and another image illustrated a two-dimensional house plan with sensors spread across the rooms. The images served to ensure that all participants had a consistent understanding of smart homes, considering the broad definition of smart home. Once the SHD concept was explained, participants were invited to think about each room of the house individually (i.e., the kitchen, living room, bedroom, bathroom, or the house in general) as indicated in Figure 5.1a in which they explained their specific privacy concerns related to devices, sensors, data collected, network (data sharing), and services (data usage).

After sharing their specific concerns, participants worked on the sticky notes as shown in Figure 5.1b) where they described privacy risks by data life cycle. Specifically, participants described what they considered to be high, medium, or low risk in the process starting with data collection in a smart home, going through transmission and storage, and concluding with data usage. In the last part of the interview, participants suggested recommendations to design controls thinking about best practices and features that should be available in smart home devices. Figure 5.1c shows the empty online sticky note template that was used for this purpose.

The interviews were video and audio recorded. The transcripts have been used for data analysis. Also, the post-it notes were extracted for analysis in a comma separated value (CSV) file and screenshots were used for storing the notes. To ensure accessibility, participants who joined by phone could see the shared screen of the moderator with the Miro board but they did not have to type in the sticky notes if they were not comfortable doing so and preferred to speak. Participants who were more comfortable typing refrained from speaking out loud their concerns unless they wanted to provide clarifications or detailed information. Overall, 22 participants preferred to express themselves verbally instead of typing. For three participants who chose to type, the moderator asked them to clarify comments when necessary and took notes to minimize the gap between written and verbal comments.

Ethics

Prior to data collection, the study protocol was approved by the institutional review board (IRB) of the host institution. Informed consent for participation in the study was obtained from all participants. Consent was also received from participants prior to audio recording. Confidentiality and anonymity of all participants were ensured by removing any identifiable information from transcripts. We referred to participants by alphanumeric codes that included participant (P) numbers, which are used in the Results section to cite quotations.

Data Analysis

I transcribed the audio recordings thoroughly. The transcripts were then verified by Yoseif Berhe, a research assistant at the Human Centric Design lab. Our approach to thematic analysis was based on the widely used Braun and Clarke [188] method and included the following steps recursively:

1. Immerse with the data and identify items of interest.
2. Generate codes.
3. Develop themes: Organize codes into potential themes. Examine relationship between themes.
4. Review potential themes.
5. Define and name the themes.
6. Produce the report.

Two researchers initiated the qualitative data analysis by first going over a few transcripts multiple times to get familiar with the audio and transcripts and then coding five interviews together to generate an initial codebook. The rest of the interviews were then coded iteratively by the two researchers in small batches of three interviews. In each iteration, two researchers coded three interviews independently and then met to resolve differences in code application and agree on new codes to consolidate the codebook. The iterations continued until all 25 interviews were coded. Between the two coders, we achieved an inter-rater reliability of 0.89 using Cohen's kappa [189], and all disagreements were resolved by consensus. The researchers then examined relationships and patterns among the codes and grouped them into categories and sub-categories, using affinity diagramming. Affinity diagramming [190] was employed to group the codes, and to find similarities and differences across codes.

To analyze privacy controls desired by participants, we followed inductive thematic analysis [188], where the researchers generated the themes from the data using the methods described above. The privacy controls codes, sub-categories (or sub-factors), and categories

(factors) along with their frequencies are detailed in Appendix D.1. The analysis of privacy concerns into a concerns taxonomy are published in [191].

5.3.2 Survey Study

The goal of the survey was to gain quantitative insights on privacy controls expectations of participants. The survey was deployed using Amazon Mechanical Turk (AMT)[5] which is a crowdwork platform widely used to recruit participants for surveys. In this platform, a survey can be deployed as a human intelligence task (HIT). To ensure quality responses, the survey was restricted to participants from the United States who had task approval rating of 95% or above and had completed at least 100 tasks in this platform.

Design

The survey consisted of questions on what privacy controls were expected by participants in smart home devices. Based on the 32 sub-factors of privacy controls from the interview results, the researchers constructed statements about the privacy controls that were presented to survey participants in the form of Likert scale questions. We went through multiple iterations of questionnaire development. Although the initial designs included a variety of questions, such as Yes/No and selection, the research team reached a consensus on Likert scale questions based on the research goal of complementing the findings of the interviews by gaining quantitative insights and also testing quantitatively the scale reliability of our interview categories. We reviewed the questionnaire to ensure that the essence of the related sub-factor was captured in each question.

In the survey, we also asked participants to complete the Internet Users' Information Privacy Concerns (IUIPC) questionnaire [176] and provide demographic information. We

[5] mturk.com

included an open ended question at the end of the survey to gather participant feedback on issues experienced while completing it. We analyzed each response.

Pilot. We conducted a pilot test of the survey with six volunteer participants and used their feedback to clarify some wordings, minimize technical jargon, and improve the survey flow. This resulted in a refined version of the questionnaire. Data from the pilot study were not used in the final analysis.

Phase 1. We conducted the study in two phases. In phase 1, we collected 50 responses and reviewed all responses. We read and inspected each response manually to determine the quality of responses and to find out if improvements need to be made. We aimed at using participant feedback from this phase to improve the survey and fix any issues to enhance the survey. Phase 1 resulted in no changes to the survey design.

Phase 2. The survey was then deployed to a larger sample of participants to collect a total of 495 responses. Participants were compensated with USD 1.50 for completing the survey.

Survey Workflow

Participants were first presented with information about the study and its informed consent form, with options to agree to participate in the study or deny and quit. To ensure that participants are on the same page, we presented a Wikipedia-adapted definition of smart home[6] that we simplified by reducing technical jargon. The definition also included three pictures of smart home devices. The entire survey protocol is included in Appendix C.1.

Participants were then asked to identify three pictures of smart home devices correctly out of five pictures presented to them. Participants who did not choose the devices correctly were excluded from the study. This qualification method was inspired from a prior paper

[6]https://en.wikipedia.org/w/index.php?title=Smart_home

[182]. Participants were then asked whether they owned and used smart home devices. They were asked how many and what type of devices they owned. Participants who did not use at least one SHD were excluded from the study. This exclusion criterion was inspired by a prior paper [181] to ensure high-quality responses.

Expectations of Privacy Controls. We then asked questions about what privacy controls participants wanted in smart home devices. The privacy controls questions were designed as 5-point Likert scale questions where participants rated their level of agreement with each specific privacy control presented. The privacy control questions represented the privacy control sub-factors from the interview findings discussed in Section 5.4. We have included all the survey questions in Appendix C.1

IUIPC and Demographics. To gauge the level of internet privacy concerns among our participants, we asked participants to answer a IUIPC questionnaire [176] that consists of ten 7-point Likert questions on three dimensions of information privacy concern: awareness, control and collection. Lastly, we asked participants about their demographics: gender, age, education, income, household size, marital status and occupation.

Data Analysis

We collected a total of 495 responses. We inspected the responses and discarded nine responses because the open-ended responses were simple copy-paste from the Internet, did not contain meaningful responses, or contained numeric entries only. Open-ended questions were used for quality checking and excluded from the data analysis. We examined the responses from participants who missed the attention-check questions and discarded all 46 responses that missed one or both attention-check questions.

Consequently, we included 440 responses in our analysis. We performed quantitative analyses on the resulting data. We have made the resulting dataset available online [192].

We applied descriptive statistics on participant demographics, SHD types, number of SHDs, privacy control expectations and IUIPC scale items. We performed reliability analysis on the privacy controls categories using Cronbach's alpha reliability coefficient.

Participants

Research shows that MTurk population is mostly college graduate [193]. Past reports show that SH users in the US are also mostly college graduate, young males [194]. Our participant pool also reflects these characteristics probably because we have included only SHD users in our survey. We provide a summary of our participant demographics below.

Gender Identity and Age. 39.1% identified as female, 60.7% male, and 0.2% preferred not to disclose. Mean age was 38.2 years with a median of 35 and standard deviation of 10.5. About 8.6% were 18-25 years old, 42.5% were 26-35 years old, 26.8% were 36-45 years old, 14.1% were 46-55 years old, and 8% were above 55 years old.

Education and Income. 62.5% of participants reported having a Bachelor's degree, followed by master's degree (24.5%), some college but no degree (7%), associate (2.7%), high school (2.5%), professional (0.5%) and less than high school (0.2%). 19.3% of participants reported earning no more than $30K, 43.2% no more than $60K, 25.4% no more than $90K, and 12.1% over $90k.

Household Size and Marital Status. The average household size was 3.45 (Median=4, SD=1.17). Among the participants, 81.6% reported being married, 15.2% never married, 2% divorced, and 1.1% widowed.

Occupation. Participants reported a diverse set of occupations, including manufacturing, sales, teaching, legal, software development, insurance, software engineering, web design, nursing and accountant. 13% of respondents provided a computer or IT-related occupation.

Device Ownership and Usage. The average number of devices used by participants was 4.76 (Median=4, SD=5.04). Similarly, the average number of devices owned by participants was 4.29 (Median=4, SD=3.59). The most popular type of device owned and used was a voice assistant, followed by security cameras.

IUIPC Scores. We added up the score for the responses to the questions within each corresponding dimension. The average Awareness score was 15.5 (Median=15, SD=3.56, Min=6, Max=21). The average Control score was 15.4 (Median=15, SD=3.24, Min=6, Max=21). The average Collection score was 20 (Median=20, SD=4.56, Min=6, Max=28).

5.4 Results

In this section, we describe the results of our qualitative and quantitative analyses. First, we describe the SHD privacy controls desired by the interview participants. Then, we describe the quantitative insights gained from the survey participants.

5.4.1 Desired Privacy Controls in SHDs

In this section, we describe the privacy controls expected by our interview participants. The thematic analysis resulted in 215 codes, which were grouped into 32 sub-categories and 7 categories. The codes are the privacy control expectations of users, which are coded as user interface features. The categories and sub-categories inform the design factors and sub-factors respectively.

Thus, we categorized the participants' expectations of privacy controls into seven design factors: Data-related Controls, Transparency, Centralized Interface, Device Controls, Multi-user Controls, User Support, and Security Controls. Table 5.2 lists the design factors in order of frequency of codes in each category. We visualize the design factors, sub-factors and their frequencies in Figure 5.2. We describe each design factor in this section, provide

Table 5.2: Privacy controls categories from the thematic analysis of interviews.

Privacy Controls	%	n=215
Data-related Controls	39.5	85
Transparency	19.5	42
Centralized Interface	16.3	35
Device Controls	13.0	28
Multi-user Controls	5.1	11
User Support	3.3	7
Security Controls	3.3	7

participant quote examples for each design factor in Table 5.3, and provide a listing of all design factors, sub-factors and design recommendations in Appendix D.1.

Data-related Controls

Twenty-two participants expressed that they would like SHDs to provide end users with options regarding controlling data collection, transmission, storage and usage. About 40% (n=85) codes fell in this category. By observing the variation in concepts in data-related controls, we divided participants' data control expectations into ten sub-categories: Choice (11%, n=24), Monitor (7%, n=16), Deletion (7%, n=14), Do not share (4%, n=8), Consent (3%, n=6), Opt out (2%, n=5), Complete control (2%, n=4), Opt in (1%, n=3), Limit (1%, n=3), and Local storage (1%, n=2).

Participants whose privacy control expectations fell under the first sub-category 'choice' desired to have options to choose what data are collected by the SHD, what data become part of user profile, what data are shared between devices in a home network, what data are transmitted, what data are shared, what data are used and how. They also sought options for choosing when a SHD records or listens, when data are collected and deleted. Other

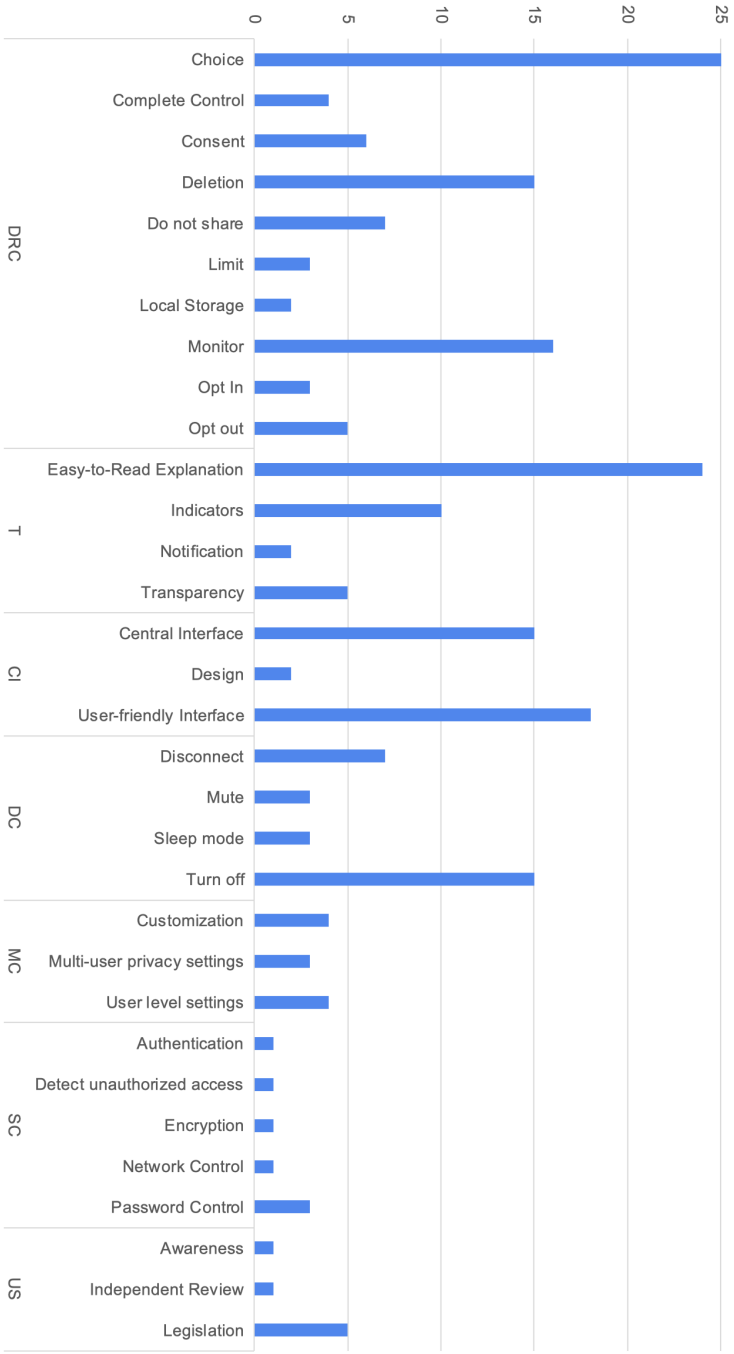


Figure 5.2: Design factors and sub-factors with their frequencies (n=215). DRC: Data-related Controls, T: Transparency, CI: Centralized Interface, DC: Device Controls, MC: Multi-user Controls, SC: Security Controls, US: User Support.

Table 5.3: Description of privacy control categories or factors and related sample quotes

Factors	Description	Sample Quotes
Data-related Controls	Control over data collection, transmission, processing, storage	"If there is any kind of app or anything that might help me to control the monitoring of data my self and the data being transferred to somewhere else, so I can see like what happened to my data." (P20)
Transparency	Features providing information, policy, disclaimer, indicators showing that device is on and/or in action, and notifications.	"I just think it should be more open about. Okay, this is the data we're keeping. This is what we throw away. So, mostly I'd like the terms and conditions of things to just be more straightforward and open about all the privacy." (P23)
Centralized Interface	Centralized interface providing smart home device controls.	"Having a centralized area to be able to control where it's very intuitive and I just can turn devices on/off or other things, maybe something like that would be better." (P15)
Device controls	Hardware and software features to control operation of the device or its capabilities, such as powering a device on or off.	"If I could, like, control them from the app and just say, like, stop them all from listening to us at once. Or if I could say to [device] to stop listening. That might already be a thing, but we, I just don't know it. That might be nice, so an easier way than getting up and turning it off." (P8)
Multi-user Controls	Controls allowing owners to manage users, their preferences and data in a household	"When I was sharing, like, a smart TV with my parents, if I were watching something on Netflix that I don't want them to see, that would be something that I would be concerned about and I want controls for." (P7)
User Support	Help, promote user awareness, and troubleshoot problems.	"Companies should provide training, ensuring every customer knows how to use, say, the mute button" (P01)
Security Controls	Controls about the security of the device, such as preventing unauthorized access.	"Mostly, what I want regarding privacy is that the information may not be easily leaked. So, what i really want is having the fingerprint and the password, so the company and others cannot access your information." (P18)

choices desired included no default social media sharing, option to not make information public, and not storing payment information.

Fourteen participants sought privacy controls that allow them to monitor and audit what data are collected, who they are sent to, and opt in (or out) of data collection. We placed them under sub-category 'monitor'. For instance, one participant highlighted the desire to have options to limit (or not collect) private information:

> "Not collecting a lot of data of private things, more like a cell phone, you know there's not much that can be done about it, so that would be better." (P10)

Participants who desired monitoring features wanted to audit collected data, view activity, view logs, view audio and video files, and view access logs. For example, a participant who sought monitoring and auditing controls desired options to view what data are collected and what logs are maintained, but mentioned the lack of such features in a current SHD:

> "I don't think there is any way for me to see all the telemetry data that gets sent out to [companies]. If I could basically see, like a telemetry log that I know exactly what they're sending." (P24)

Participants in this category also desired options to delete data. We placed them under the sub-category 'deletion'. Automatic deletion of data after a certain period was also a desired feature. Other deletion features included deleting logs (of audio, video), data files one-by-one as well as in large batches, deleting personal information, deleting data after a period authorized by the user, and notifying the user with an option to keep or erase the information.

Participants also expressed benefits of not only providing the choice to the users, but collecting less data. One participant mentioned the lesser the data collected, the lesser the

likelihood of damage due to data breaches:

> "I need to be able to see the telemetry data if it gets sent and ideally, it shouldn't be sent on this. There's a good reason to because otherwise that status for all and increases the probability of damage from a data breach." (P24)

We found research evidence connecting secret data collection with data breaches [162]. Another participant who wanted to have control over data desired to have an option of visibility of data transferred and used later:

> "If there is any kind of app or anything that might help me to control the monitoring of data myself and the data being transferred to somewhere else, so I can see like what happened to my data." (P20)

The fourth sub-category included the participants' expectations about 'do not share' features, where participants wanted to be able to not share usage statistics, personal information, and other collected data with the SHD vendor. Two participants also wanted this feature to be default, with an option to share the information when desired.

The fifth sub-category was related to 'consent', where participants desired that SHD vendors asked for the user's consent before: (a) collecting any data, (b) using collected data, (c) transferring those data, (d) sharing data, and (e) updating data.

The sixth sub-category 'Opt out' included five participants who wanted to opt out of data collection that seemed to be lacking in their SHDs.

The seventh sub-category of data-related controls included 'complete control', where four participants desired complete control over their data.

The eighth sub-category 'Opt in' included the needs of three participants who wanted to have data collection opted out by default and wanted that vendors provided options for users to opt in to data collection when the users so wished.

In the ninth sub-category, participants desired options to 'limit' the collection of data, for example, with options to pick what data to allow for collection.

The final sub-category 'local storage' included two participants who sought the option to store and manage data locally in their own home network.

Transparency

About 20% (n=42) of the codes fell under the theme of transparency. In this category, 16 participants desired clarity in SHD companies' data collection and usage policies, clear visual indicators when being recorded, and expected data to be available to review. Participants expected openness from companies in this regard:

> "I just think it should be more open about. Okay, this is the data we're keeping. This is what we throw away. So, mostly I'd like the terms and conditions of things to just be more straightforward and open about all the privacy." (P23)

We divided the codes in this category into four sub-categories: easy-to-read explanation (11%, n=24), indicators (5%, n=10), transparency (2%, n=5), and notification (1%, n=2).

Participants desired an easy-to-read explanation on terms of service, privacy policies, what data are collected, why data are collected, what data are stored and where, how data are used, how long are data retained, what data are shared and under what conditions, with whom data are shared, who has access to data, device capabilities, consent, and benefits and drawbacks of sharing the data, for example if a particular added service would be available by sharing. Among participants who sought transparency on what data is collected, who uses it, and for what reasons, P03 expected options to see transcripts for voice data:

> "If you had [a voice assistant], show a transcript or show whatever you said to

it, however that can also give a feeling of less security." (P03)

Another transparency sub-category was indicators. Participants desired to have hardware as well as software indicators for audio recording, video recording, device status (on). Hardware indicator examples include LED lights and software indicators include visible buttons or icons on the user interface.

In addition to indicators, two participants also desired status notifications, such as through voice and visible text display, when SHD is recording audio or video. The term 'transparency' was also used by participants five times.

Centralized Interface

Among all, 15 participants desired a user-friendly, centralized interface that allowed various controls to different smart home devices:

> "Having a centralized area to be able to control where it's very intuitive and I just can turn devices on/off or other things, maybe something like that would be better." (P15)

About 16% (n=35) codes were related to centralized control interface. We categorized them into user-friendly interface (8%, n=18), central interface (7%, n=15), and design (1%, n=2).

Participants desired an interface which is easy to use and provides options to control SHDs in a centralized way. They wanted this interface to be intuitive, child-friendly, elderly-friendly, and mobile. One participant preferred this interface to be voice-activated. Features expected in this central interface included displaying all devices, data practices and disclaimers, viewing data, managing data, visualizing data, and training/tips for the

user. Two participants also expressed that the design of the interface should be centered on privacy and focused on the safety of the user.

Device Controls

Participants expressed the need for hardware and software options to turn off the devices and to turn on/off the recording or listening features of the devices. Fourteen participants desired options to isolate or disconnect the device or its recording capability. We divided these device controls into four sub-categories: turn off (7%, n=15), disconnect (3%, n=7), mute (1%, n=3), and sleep mode (1%, n=3).

Participants who desired options to turn off desired capabilities to turn individual devices off, turn all devices off through a button or switch, turn all devices off for a selected period (for example, for a certain period at night), turn listening feature off, and turn recording feature off. For example, one participant, who owned and used multiple intelligent speakers, desired option to turn them off all at once before going to bed:

> "If I could, like, control them from the app and just say, like, stop them all from listening to us at once. Or if I could say to [device] to stop listening. That might already be a thing, but we, I just don't know it. That might be nice, so an easier way than getting up and turning it off." (P8)

Participants desiring 'disconnect' features wanted options to disconnect SHDs from the Internet and wished SHDs asked permission before connecting to a network. Participants also expressed desire for a switch or an option to perform 'hardware disconnect' of a microphone. We learned that hardware disconnect is a feature, similar to one used by Apple[7], where the microphone is disabled in the hardware level so that a malicious software

[7] www.apple.com

can not invoke the microphone. One participant desired the option to connect SHDs to separate network than the home Internet.

For devices with microphone capabilities, participants wished they had a mute button. Among participants who desired SHDs to not listen to every private conversation, three wished for a 'sleep mode' in SHDs. For example:

> "Well, I definitely want them to not hear each and every word that we say [...], but I don't know how they enable it, may be a sleep mode." (P06)

Multi-User Controls

Seven participants whose desired privacy controls fell in this group sought options for them to customize privacy settings for multiple users. About 5% (n=11) of the codes fell in this category, which included desired features, such as add/remove users, anonymize collected data, optimize privacy settings, do not share (with other users), multi-user privacy settings, option to give permission to family members, schedule SHD operation, display data only for authenticated user, and segregate data by users.

For example, P08 mentioned interest in "curating my own" consumer profile, by editing preferences and interests. Another participant (P07) who desired multi-user privacy settings in a smart television wanted to keep things private from other family members:

> "When I was sharing, like, a smart TV with my parents, if I were watching something on Netflix that I don't want them to see, that would be something that I would be concerned about and I want privacy controls for." (P07)

User Support

Among the participants, four participants expressed the need for regulation and third party certification. This category included 3% (n=7) codes: better data rights, legislation

on data protection, mandatory deletion requirement, right to delete, user awareness, and independent review/certification of privacy features in SHDs.

Participants desired user training and simplistic design of devices so that users can configure themselves, without the need for professional help. As P01 noted, companies should train their users on privacy features of their SHDs:

> "Companies should provide training, ensuring every customer knows how to use, say, the mute button." (P01)

We also found that participants are finding newer avenues to learn about privacy practices. For instance, P08 expressed having to learn security controls through TikTok videos, such as to control the sharing preferences of usage behavior to not be disclosed with SHD vendor.

Security Controls

This category included 3% (n=7) codes, which were related to user authentication and protecting data from leakage. Six participants' desired features fell in this category, which included options to generate and use password in the SHD, fingerprint authentication, detect unauthorized access to the SHD, control who is allowed to the home network, and data encryption. For instance:

> "Mostly, what I want regarding privacy is that the information may not be easily leaked. So, what I really want is having the fingerprint and the password, so the company and others cannot access your information." (P18)

5.4.2 Quantitative Insights on Privacy Controls Desired by Users

From the interviews, we found a number of privacy controls which are desired by users. However, it may be difficult for developers to implement all of them. It is important to know which privacy controls are more important to users. Thus, we present our survey results here to inform which privacy controls were more desired by users. These results may help developers prioritize controls in the implementation. The survey findings may also complement and validate our interview findings.

In Table 5.4, we show the mean, median and standard deviation of the privacy controls from our survey results in which 440 participants rated whether they wanted a particular privacy control on a scale of 1 (Strongly Disagree) to 5 (Strongly Agree) and we show a graph in Appendix E.1. The median score for all privacy controls is 4 (Agree) and the average score for most privacy controls is 4 or above, indicating that the privacy controls that were presented to our survey participants were generally desirable. Since the privacy controls that we presented to the survey participants resulted from our interviews, this confirms and validates our privacy controls findings from the interviews.

The top six privacy controls desired in our dataset were User-friendly Interface (Mean: 4.25), Access Detection (Mean: 4.21), Indicators (Mean: 4.20), Monitor activity ((Mean: 4.20), Consent (Mean: 4.18), and Independent Review (Mean: 4.18). The least desired privacy control in this dataset was Disconnect (Mean: 3.83), probably because the participants assumed they could achieve "disconnect" by simply turning off the SHD.

We tested the scale reliability of our categories using Cronbach's alpha (α) reliability coefficient [195]. We achieved α=0.89 for the category of Data-related Controls, which demonstrated a high internal consistency for the 9 items included in it. As shown in table 5.4, the coefficients for other categories were Transparency-related Controls ($\alpha = 0.88$), Central Interface ($\alpha = 0.69$), Device Controls ($\alpha = 0.85$), Multi-user Controls ($\alpha = 0.74$),

Table 5.4: Mean, median and standard deviation (SD, n=440) of the privacy controls sub-factors from the survey. Mean values below 4 are marked with an asterisk (*), indicating options less desired by survey participants. Scale reliability statistic Cronbach's α values are included in parentheses in the first column.

Categories	Sub-factors	Mean	Median	SD
Data-related Controls (Cronbach's $\alpha = 0.89$)	Choice	4.11	4	0.92
	Consent	4.18	4	0.97
	Deletion	4.00	4	1.09
	Do_not_share	3.96*	4	1.03
	Local_storage	4.01	4	0.98
	Limit	4.08	4	0.94
	Monitor	4.2	4	0.98
	Opt_in	4.00	4	0.99
	Opt_out	4.05	4	1.01
Transparency-related Controls (Cronbach's $\alpha = 0.88$)	Easy_to_read_info	4.15	4	0.87
	Indicators	4.20	4	0.96
	Privacy_policy	4.04	4	0.97
	Notification	4.11	4	1.01
Central Interface (Cronbach's $\alpha = 0.69$)	Central_interface	4.15	4	0.85
	User_friendly_interface	4.25	4	0.90
	Design	4.16	4	0.95
Device Controls (Cronbach's $\alpha = 0.85$)	Disconnect	3.83*	4	1.13
	Mute	3.90*	4	1.12
	Sleep	3.86*	4	1.12
	Turn_off	3.92*	4	1.07
Multi-user Controls (Cronbach's $\alpha = 0.74$)	Multi_user_settings	3.97*	4	0.85
	Maximum_default_privacy	4.19	4	0.95
	Customization_user_level	3.96*	4	0.94
	User_level_settings	3.88*	4	1.04
Security Controls (Cronbach's $\alpha = 0.83$)	Authentication	4.12	4	0.95
	Access_detection	4.21	4	0.91
	Encryption	4.08	4	0.98
	Network_control	4.15	4	0.94
	Password_control	4.14	4	0.92
User Support (Cronbach's $\alpha = 0.68$)	Training	4.00	4	0.89
	Independent_review	4.18	4	0.96
	Legislation	4.05	4	0.94

Security Controls (α = 0.83), and User Support (α = 0.68). Similarly, α=0.68 was the lowest scale reliability value obtained, which is considered good for three items. Thus, based on the survey results, our categories demonstrated good internal consistency for the privacy controls items included, as a high coefficient indicates good internal consistency of items in the scale and is dependent on mean of inter-item correlation as well as number of items in the scale [196].

5.5 Discussion

In this section, we summarize our findings, present recommendations for users and developers, and discuss limitations and suggestions for future research directions.

5.5.1 Summary of Findings

Our findings suggest seven design factors and 32 sub-factors for privacy controls desired by participants, which were generated from qualitative and quantitative analysis of SHD users' needs. The results presented inform how to design user interface controls for privacy features of SHDs. We also quantified the sub-factors by rigorously designing a questionnaire based on Likert scale. The quantitative insights thus obtained may help developers prioritize controls during implementation.

Since this study's focus is on the user-centric privacy controls for SHDs, we ensured our codes are semantically formatted in a way that can be translated into a user-interface feature when implemented by a developer. For example, rather than using a code 'choose', we used the code 'choose what data to delete'. Our study's unique contribution is this set of privacy controls or codes with granularity and specificity necessary to translate them into user-interface design.

The goal of this study was to uncover privacy control design factors, sub-factors and

privacy-related user interface controls for SHDs comprehensively so that they can be used by developers in user interface design. In the following sub-sections, we discuss our factors and sub-factors in light of prior research. We also share additional insights gained during analysis, and discuss a privacy control framework and the role of third party or government.

To the best of our knowledge, prior work has uncovered factors and sub-factors of desired privacy features; however, our work extends the knowledge by uncovering user interface controls desired by users in a format that can be translated into design. In order to confirm and extend research in the domain, we used the same names of design factors and sub-factors from prior related work when they existed in prior literature. We now situate our findings with prior work.

5.5.2 Some Design Factors and Sub-factors Confirm Prior Work

Some of the design factors and sub-factors in this paper confirm findings from prior work. During our thematic analysis, we familiarized ourselves with past literature and used similar terminology when possible. In Table 5.5, we list the factors and sub-factors revealed from this study and those from prior work on privacy controls of SHDs to the best of our knowledge.

Yao et al. [148] recommended data transparency and control, safety, and security among six design factors in their paper. Although they did not have sub-factors, we find that some of our sub-factors were included in their work: transparency, delete, multiple users, notice, do not record, and easy interface [148]. Some sub-factors are similar to Barbosa et al. [182]: transparency, access control, consent, security, no data collection, deletion, offline operation. Some of our factors and sub-factors are also similar to the wish list in Haney et al. [181]: transparency (data collection and security feature), security and privacy controls, and user assistance.

Table 5.5: Sub-factors confirmed from prior work and revealed in the current study.

Design factor	Sub-factors from prior work	Sub-factors from this study
Data-related Controls	Deletion [182], Consent [182], Local storage [148, 182], Limit [120], Choice [148]	Monitor, Do not share, Opt out, Opt in
Transparency	Transparency [148, 181, 182]	Easy-to-read explanation, Indicators, Notification
Centralized Interface	User-friendly interface [148, 151], Design [197]	Central interface
Device Controls	Sleep mode [148]	Turn off, Disconnect, Mute
Multi-user Controls		Multi-user privacy settings, Privacy by default, User level privacy, User level settings
User Support	Awareness [181], Legislation [148, 181, 182]	Independent review
Security Controls	Password control [148,181,182], Authentication [148, 182], Access detection [148, 151]	Network control, Encryption

5.5.3 Privacy Controls Contain Usability Heuristics

It should be noted that some privacy control sub-factors contain usability heuristics, which are principles of user interface design [198]. Visibility of system status [198] is a usability heuristic that is contained in our 'visibility' sub-factor. Similarly, match between system and the real world [198] is a usability heuristic that suggests designers should use language that is familiar to the user (rather than technical jargon) and is contained in the 'easy-to-understand information' sub-factor. In addition, help and documentation [198] is a usability heuristic that is contained in the sub-factor 'awareness'. Thus, we observe that participants' needs of privacy controls also contain the needs of usability.

5.5.4 Recommendations for Developers: Privacy Controls Framework

The privacy controls that have been uncovered in this study are desired by users. These users' expectations can be fulfilled when implemented by developers. In this subsection, we identify the privacy controls that can be implemented by developers. Based on our results, we recommend the following privacy controls framework for developers interested in developing privacy controls in their SHDs. The privacy controls framework consists of the design factors, sub-factors and user interface design recommendations. We list the factors and sub-factors for the privacy control framework in Table 5.6 and the design recommendations (or user-interface controls) under each sub-factor can be found in the Appendix D.1. We included all actionable design recommendations from our findings that can be translated into a user interface (UI) feature by developers. For example, we did not include complete data control, because this is a concept rather than a UI item, but included all the choices regarding data control under factor 'choice', e.g. choose what data are shared between devices.

We recognize that the privacy controls desired may be implemented in different elements of the smart home device or network: the SHD device, its app, or SHD vendor's website. For each design factor in Table 5.6, we also identify the SH component where the privacy controls can be implemented.

The recommendations of our work can be implemented by developers of individual smart home devices by incorporating them in the design of the device. These recommendations can also be useful to developers of products, such as Fing [8], that are designed to manage smart home devices.

[8] https://www.fing.com/

Table 5.6: SHD Privacy Control Framework: factors and sub-factors of privacy controls expected by users. Design recommendations, under each sub-factor have been omitted in this table for brevity; they can be found in Appendix D.1.

Design factor	Sub-factor	Where
Data-related Controls	Choice, Deletion, Do not share, Consent, Local storage, Monitor, Opt out, Limit, Opt in	App, Device
Transparency	Easy-to-read explanation, Indicators, Notification	App, Device, Website
Centralized Interface	User-friendly interface, Central interface	App, Device
Device Controls	Turn off, Disconnect, Mute, Sleep mode	Device, App
Multi-user Controls	Multi-user privacy settings, Privacy by default, User level privacy, User level settings	App, Website
User Support	Awareness, Independent review	App, Website
Security Controls	Password control, Access detection, Authentication, Network control, Encryption	App, Device

5.5.5 Users are Limited to Developer-implemented Controls

SHD users are limited to the privacy controls that are implemented by developers. For example, a user may be interested in viewing what data are collected; however, if that feature was not implemented by the developers, the user would not be able to do so. Thus, the privacy expected by SHD users can come to fruition only when the privacy controls are implemented by developers. Thus, we recommend developers our privacy control framework as a guide towards privacy-related user interface controls and implement features that apply to their devices. We recognize that our framework is comprehensive, device-agnostic and flexible, guiding developers to implement privacy controls relevant to their devices.

We recommend that developers not only implement privacy controls discussed in this section but also make users aware of what privacy controls have been implemented, how

users can use these controls, and the implications of these controls to the users.

5.5.6 Role of Government and Third Party

As prior work has enlightened [181] and our participants have articulated, government's role in encouraging some level of privacy preservation is useful. Participants have expected regulations that ensure privacy of SHD users. The role of government is deemed essential because privacy preservation is often not in the best interest of manufacturers. For example, limiting collection may be in the best interest of users but not for manufacturers since those data could be deemed useful in purposes such as marketing. Thus, government regulations regarding deletion of personal information, protection of stored data, and proper use of personal information have been expected by participants.

Similarly, an independent, third-party organization could provide verification or certification of privacy features, which would allow novice users the confirmation that the SHD contains the privacy features claimed by the vendor. Displaying certified privacy features could also be beneficial to SHD vendors in gaining the trust of privacy-concerned users.

Although privacy self-management through notice and choice are desirable, the effectiveness of privacy self-management by users is impacted by two factors: (1) the complexity of data collection and usage by highly networked systems, and (2) users' cognitive abilities to make informed decisions by combining the various options picked, choices made, and consents provided. Solove [199] identified four major problems leading to ineffective privacy self management: uninformed individuals, skewed decision-making, scale (of technology), and aggregation. Thus, privacy self-management should be adopted with care, and privacy management should be complemented through other techniques, such as limiting data collection and privacy by design.

5.5.7 Limitations

The interview participants were mainly young adults, mostly educated, and living in the US. So, typical to any in-depth interview analysis, our results may not be generalizable to populations from other cultures and other parts of the world. The participant pool was not representative and factors such as age, technical proficiency, years owning SHD, education level, and nationality may affect the results of the study. For example, prior research has shown that age [200] and gender [201] can affect technology adoption. Moreover, the interviews were audio-recorded and conducted as a one-on-one conversation. Therefore, the participants may have felt uncomfortable sharing information that could be embarrassing for them. To minimize the effect, we did not collect any personal information, provided an informed consent according to the approved study protocol, and allowed the use of pseudonyms and cameras to be turned off during interview.

In addition, the recruitment was done online, which may have excluded participants with low digital literacy. The usage of Webex and Miro may also limit the access, so we allowed participants to use their phone to join the interview, in case this approach was more comfortable for them. Thus, our participant population uncovers privacy expectations of early adopters. Finally, our study does not include privacy concerns and expectations of non-adopters of SHDs.

Regarding the survey, the crowdwork platform presents some limitations. As with prior studies using AMT [182], our AMT sample is not representative of the US population, but it represents the SHD user population, which is mostly college graduate, young, and technology- or Internet-savvy. AMT workers also have more information online [202] and likely exhibit privacy concerns not representative of the US population. We also acknowledge that our studies measure users' attitudes, which are known to differ from actual behavior, known as 'privacy paradox' in privacy research [203].

5.5.8 Future Work

We studied privacy control expectations with participants from the US. Future studies could investigate other populations around the world. Follow up experimental studies could be conducted to validate our findings in other cultural and international contexts. Follow up studies could also develop prototypes and applications to assist developers and users with privacy controls.

We presented a privacy control framework intended to guide SHD developers. Future studies could explore such frameworks for specific devices. For example, a set of privacy guidelines could be devised for camera developers and users of smart cameras.

5.6 Conclusion

Privacy remains a major concern for mass adoption of SHDs [161]. Researchers and developers need to work towards developing privacy enhancing SHDs to address this issue. To decipher privacy control expectations of users, we conducted in-depth interviews with 25 users and analyzed their responses. We then inductively analyzed participants' expectation of privacy features in SHDs to generate seven design factors and 32 sub-factors that can be translated into user-interface design. We complemented and validated the findings through a survey. Furthermore, we recommended design guidelines for developers through a privacy control framework. Developers may use the recommended framework to incorporate user-centric privacy controls in their SHDs, and users may utilize the developer-implemented privacy controls to manage their privacy in SHDs. The findings and recommendations in this study contribute to a broader understanding of users' needs of privacy controls and ways to address them.

Chapter 6: MyCam: Designing and Evaluating a Prototype for Data-related Privacy Controls in a Smart Home

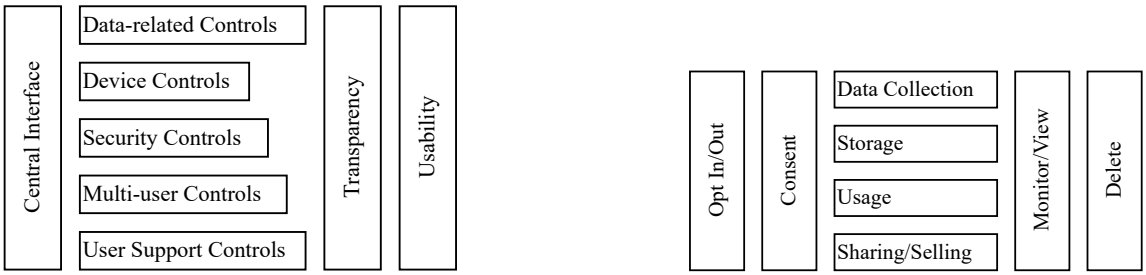
6.1 Introduction

Researchers and security experts have identified vulnerabilities and concerns in smart home devices (SHDs) or home Internet of Things (IoT) devices [204]. Although users are known to have inadequate and inaccurate mental models of smart device risks, they have expressed concerns [5]. In fact, privacy has been identified as one of the primary reasons for non-use of SHDs [5].

Researchers have further identified privacy concerns of users and made design recommendations for the development of privacy controls to address those concerns [18,120,148]. However, few studies have translated the design recommendations and needs into designs that can address the privacy concerns.

To fill this gap, we designed a prototype of a user interface implementing the design factors elicited from prior literature [10]. For the prototype, we followed an iterative design approach. We evaluated the prototype for user experience, usability, perceived information control, user satisfaction and intention to use. Evaluation user studies included interviews (n=10) and survey (n=120). For the purpose of this study, we framed the prototype as an app for a camera. However, the proposed design may serve as a design pattern for other home IoT systems.

We contribute the design of data-related privacy controls for home IoT systems and design recommendations to further improve the design.



(a) Privacy Controls Framework (b) Data-related Controls

Figure 6.1: Privacy Controls from Literature and our Research Approach

6.2 Background

6.2.1 Privacy Control Design Factors and Sub-factors

In Chapter 5 and a prior paper [10], we empirically identified seven design factors for implementing privacy controls in smart home designs: data-related controls, device controls, transparency, multi-user, central interface, support and security controls. We illustrate the design factors in Figure 6.1a. The vertical bars represent constructs that affect all factors defined in horizontal bars. We described these factors in Chapter 5. It is noteworthy to emphasize that users preferred a centralized interface to manage their privacy in an easy-to-use manner [205].

6.2.2 Translating Privacy Control Design Factors into Design

Transparency with regard to online privacy has been widely investigated, with one popular approach being privacy labels. There has been research about online privacy labels [204,

206], which has even recently been adopted by Apple[1] and Google[2] in their app stores. Examples of privacy label work include privacy nutrition label [206], GDPR-based privacy label for IoT devices OnLITE [207], and security and privacy label with device factors [208]. Similarly, prior work has investigated the designs of user notifications to enhance transparency [209].

Prior work has explored the design of *multi-user* controls. In a prior paper [18], researchers developed and evaluated multi-user settings for a smart home app. In another prior paper [205], authors proposed a design space for privacy choices and use-case design of a privacy choice platform app IOTAssistant.

While designs towards *transparency*, *multi-user settings*, *device controls*, and notice and choice have been explored, designs of *data-related controls* are sparse. So, this work focuses on the design of data-related privacy controls using the Privacy Control Framework [10] and design factors from section 6.2.1 as a foundation. For this purpose, we drew from literature [Chapter 5] the following data-related privacy control *requirements*: Opt-in (or out), Consent, Data collection, Storage, Usage, Sharing or selling, Monitor or view, and Delete [5, 18, 120, 148, 163, 181, 205]. We illustrate these requirements in Figure 6.1b.

6.3 Method

We designed a prototype to implement the user requirements of data-related privacy controls. Then, we conducted user studies to evaluate the prototype and gain insights into design improvements. Fig 6.2 visualizes our research approach.

[1] apple.com
[2] google.com

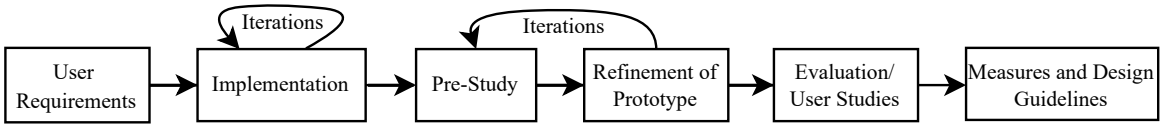


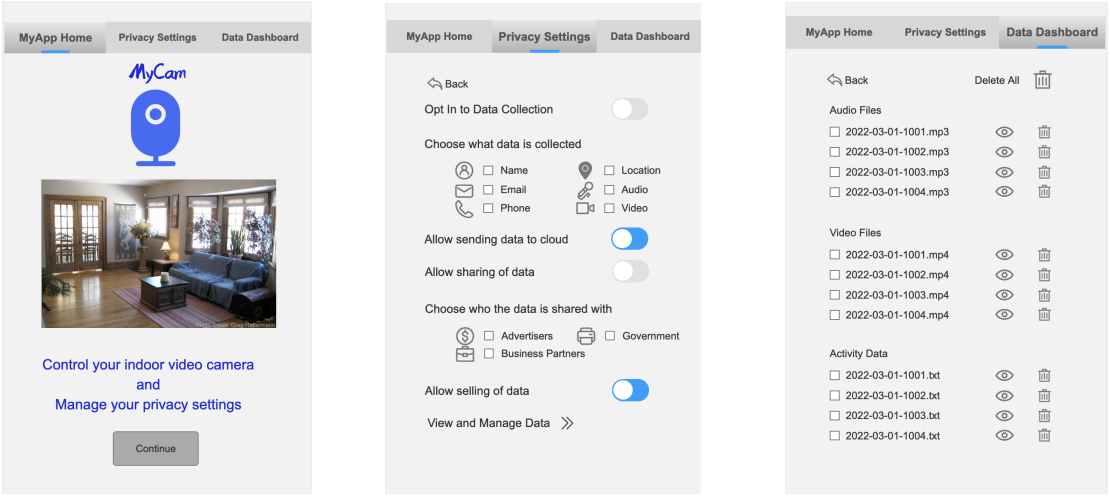
Figure 6.2: Research Approach

6.3.1 Stimulus (Prototype App)

We designed a prototype implementing the data-related privacy controls requirements using Mockplus[3]. The initial design was a result of a brainstorming session in our lab among multiple researchers involved in interface design and a feedback session involving designers working in our lab. We followed multiple design iterations of the prototype by reviewing the design among researchers and developers in our laboratory. We will explain the final iteration of the prototype, which was used in the evaluation user studies.

The prototype app, called MyCam, consisted of three pages: MyCam Home, Privacy Settings, and Data Dashboard. The home page contained the app logo, a view of the camera footage, a brief explanation that user can control the camera and manage privacy settings, and a continue button to navigate to the privacy settings page (See Fig. 6.3a). The privacy settings page consisted of the data-related controls: opt-in to data collection, control what data type is collected, allow (or disallow) sending/sharing/selling of data, choose who data are shared with, and a link to data dashboard for viewing and managing data (See Fig. 6.3b). The data dashboard page displayed all audio, video and other activity files with options to view and delete the data individually or all-at-once (See Fig. 6.3c). In addition, each page contained a horizontal navigation bar with three buttons at the top of

[3]mockplus.com



(a) MyCam home page (b) Settings page (c) Data dashboard page

Figure 6.3: Home, Settings, and Dashboard pages of the MyCam prototype app.

the interface.

6.3.2 Pre-Study

We conducted a pre-study with four lab members to elicit feedback on the prototype design and to pilot test the user studies (interview and survey). We used the feedback to improve the prototype and user study protocols. The results of the pre-study are not included in the analyses.

6.3.3 Interview Study

We conducted semi-structured interviews with 10 participants recruited via twitter in March 2022 . Interview protocol was reviewed and approved by George Mason University's institutional review board (IRB). Interview questions included demographics and

questions on feedback and evaluation of the prototype. Interview and survey protocols are available online [210].

Participants were given 5-10 minutes to familiarize themselves with the app. We gave them nine tasks to complete. Then, we asked them questions about their perception of the prototype: like, dislike, challenge, gaps, effectiveness (whether it meets privacy requirements) and improvements. Finally, we debriefed and thanked the participants. Participants were compensated with a gift card of US$25 for their participation in the interview. Average interview time was 45 minutes.

We qualitatively analyzed the interviews. We did not perform quantitative analysis on interview data due to the small sample size. Interviews allowed us to probe deeper into the perceptions of participants and understand the problems that participants experienced while using the prototype. We analyzed the interview transcripts for recurring patterns or themes. The interview findings were used to inform the recommendations for future designs.

Participants

Of the 10 participants, 5 were male and 5 were female. Four were 25-34 years of age, 4 were 35-44 years and 2 were 18-24 years. Three were Hispanic, 3 were Asian, 2 were African-American and 2 were White.

6.3.4 Survey Study

To gather user perception about MyCam, we deployed a survey in which we embedded the app and requested participants' opinions and feedback on the app. We designed the evaluation questions from standard instruments or psychometrically validated Likert scales.

Measurements

We used the User Experience Questionnaire (UEQ) scale (26 items) to measure user experience [211]. To measure usability, we used the System Usability Scale (SUS) questions (10 items, 5-point Likert) [212]. User satisfaction was measured using a 4-item scale adapted from [213]. Perceived information control scale (5 items) was adapted from [214] and intention-to-use scale (3 items) was adapted from [215]. Unless otherwise noted, all items were designed as 7-point Likert items.

Procedure

We framed the study as an evaluation of a prototype app. The study was approved by our George Mason University's Institutional Review Board (IRB) prior to the survey. We recruited 120 participants using the crowd-sourcing platform Mechanical Turk (MTurk), which is widely used by researchers to conduct security and privacy studies (see [182] and [193]. We screened out participants to ensure good quality responses. We used screening criteria similar to Barbosa et al. [182]. Participants had to be adults living in the United States, had an approval rating of 95% and completed a minimum of 100 tasks with MTurk. Research shows that MTurk sample is diverse and its perception is US representative [193].

Participants were presented with the informed consent. If they agreed to participate, they received demographic questions followed by the prototype embedded in the survey with an external link in case the embed failed. Participants performed a set of nine tasks and reported their completion status. After that, they received open-ended questions on feedback and improvement and closed-ended measurement questions. Finally, we debriefed and thanked the participants.

Interface Interaction/Task Selection

We asked the participants to perform the following tasks in the prototype app and report their completion status:

- TASK1 Click Continue on MyCam Home page to go to privacy settings page.
- TASK2 Turn on Opt In to Data Collection.
- TASK3 Select from name, email and other data you would allow MyCam to collect about you.
- TASK4 Turn off Allow sending of data to the cloud.
- TASK5 Turn on Allow sharing of data.
- TASK6 Choose who you would allow the company to share the data with (advertisers, government, or business partners).
- TASK7 Turn on (or off) Allow selling of data.
- TASK8 Click View and Manage Data to go to the data dashboard. Select the fist audio file 2022-03-01-1001.mp3. Delete this file.
- TASK9 Go to the MyCam Home page.

Participants

A total of 120 participants completed the survey and were compensated US$1.50 for completing the survey. With an average completion time of seven minutes, the rate averaged about $12.85 an hour. We excluded 15 responses that (a) did not pass the attention check questions, (b) contained copy-paste answers for an open-ended question, (c) had patterned

Table 6.1: Task accuracy (n=105).

Task#	1	2	3	4	5	6	7	8	9
Accuracy	0.981	0.952	0.971	0.962	0.943	0.971	0.933	0.733	0.524

or lined-up answers, or (d) had extremely low survey completion time (< 3 minutes) resulting in low quality responses. We included the remaining 105 responses in the analysis.

Among 105 participants, 59% were male and 41% were female. Most of the participants were 25-34 years (48%), followed by 35-44 years (30%), 45-54 years (11%), 18-24 years (5%) and 55+ years (6%). About 94% were employed full-time and rest were part-time or unemployed.

6.4 Results

In this section, we describe the results of our evaluation studies.

6.4.1 Task Accuracy

Most survey participants reported completion of the given tasks. The accuracy of tasks 1 to 7 ranged from 93% to 98% (see Table 6.1). The low accuracy of task 8 (73%) is likely due to the lack of interactive functionality of the delete button. Similarly, the low accuracy of task 9 (52%) is likely due to the lack of *back-to-home* button on the dashboard and our reliance on the top navigation bar to return to home.

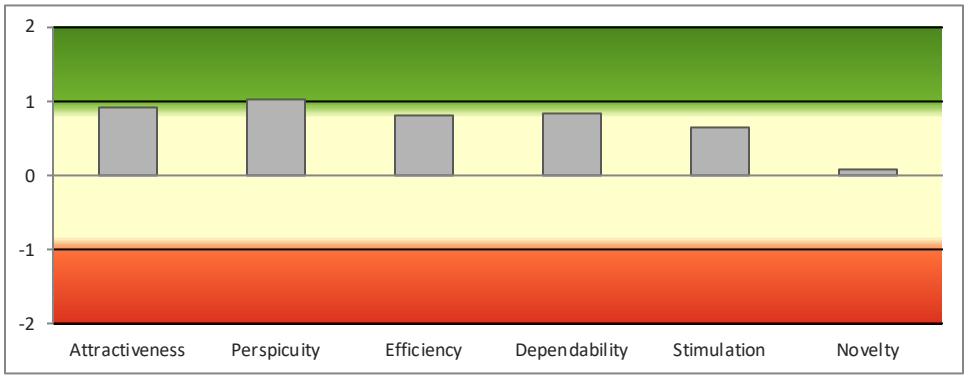


Figure 6.4: Results showing scores for the six dimensions of the UEQ scale.

6.4.2 User Experience

The UEQ instrument measures six dimensions of user experience: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. Mean score below -0.8 is negative, between -0.8 and 0.8 is neutral, and above 0.8 corresponds to a positive evaluation. MyCam was evaluated *positive* for attractiveness (Mean μ =0.91 and Variance σ^2=1.44), perspicuity (μ=1.02, σ^2=1.58), efficiency (μ=0.82, σ^2=1.42), and dependability (μ=0.83, σ^2=1.08). It was evaluated *neutral* for stimulation (μ=0.65, σ^2=1.38) and novelty (μ=0.07, σ^2=0.95) (see Fig. 6.4).

6.4.3 Usability

We used the commonly used SUS scale to measure the usability of the prototype [212]. The average overall SUS score from survey participants (n=105) was 62.5 (Min=37.5, Max=100) which is about average [216]. The benchmark average SUS score for a website is 68. Although we were unable to find a benchmark for home IoT apps, SUS scores show

Table 6.2: Scale statistics (n=105)

Scale	Number of items	Mean (μ)	SD (σ)	Cronbach's α
Perceived information control	5	4.37	1.28	0.88
User Satisfaction	4	5.14	1.46	0.91
Behavioral Intention to Use	3	5.40	1.28	0.85

that our prototype needs improvement in usability.

6.4.4 Perceived Information Control

Survey participants rated the prototype's perceived information control above average (μ=4.37, σ=1.28) and the scale demonstrated good internal consistency (α=0.88) (See Table 6.2).

6.4.5 User Satisfaction

The satisfaction scale scores of survey participants for the prototype design were good (μ=5.14, σ=1.46). The scale showed good internal consistency (α=0.91).

6.4.6 Behavioral Intention to Use

Most survey participants reported an intention to use a privacy control system similar to our prototype. The 3-item intention-to-use scale was rated good (μ=5.40, σ=1.28) and showed good internal consistency (α=0.85).

6.4.7 User Feedback

We qualitatively analysed feedback from interview participants. We do not report the findings quantitatively due to the small sample size (n=10). We found three areas of concern in our prototype design from thematic analysis of the interviews:

Lack of transparency and the state of confusion Since MyCam app did not present information on what information is collected, used, shared or sold, participants stated confusion on how to decide on what privacy settings may be appropriate for their needs. They also stated confusion on how much they could trust these settings would actually be honored by the company.

Overwhelming and Burdensome Participants mentioned that providing too many options to choose from can easily overwhelm them and create a sense of burden.

Colors and Beautification Some interview participants suggested that the app looks old-fashioned and conventional, which is also highlighted by the UEQ scale results of the survey. They suggested using a theme color to identify the app uniquely.

6.5 Discussion

The results of interviews and survey show that MyCam app was evaluated by participants with good perceived information control, user satisfaction, and intention to use. The usability and user experience scores were satisfactory allowing room for improvement. Based on these findings, we discuss some design recommendations for improvement of the MyCam app design.

6.5.1 Design Recommendations

Complement data-related controls with transparency features. In order to address the lack of transparency as stated in section 6.4.7, we suggest that transparency mechanisms be utilized in conjunction with data related controls. A combination of our design with notice and choice designs presented in [205] may be useful in this regard. Improvements can also include integration of labels [206] and notifications [209] with the data-related privacy designs.

Tiered Privacy Approach for Managing User Burden. The provision of a large number of privacy controls may give users a sense of control but it lowers usability. In [5], authors call for reducing burden of privacy on users. Thus, we recommend a balanced approach to reduce the user burden while providing privacy control. In this regard, we suggest a tiered privacy settings approach involving three options: high privacy, medium privacy, and low privacy. Each of these options will customize privacy equivalent to many user clicks. For example:

High privacy: Collection OFF, sharing OFF, communication ENCRYPTED.

Medium privacy: Collection ON, sharing OFF, communication ENCRYPTED.

Low privacy: Collection ON, sharing ON, communication ENCRYPTED.

Usability. Although we envision our prototype to be useful to the design community as a reusable design pattern for privacy settings of home IoT and potentially other devices, it should be enhanced with an accessible color theme.

6.5.2 Limitations and Future Work

While a large body of privacy research utilizes MTurk, the representation has been debated. Recent literature shows that MTurk sample may not be US representative but their

perceptions may be representative [193]. Thus, we utilized a mixed-methods approach to enhance the validity of findings. Another limitation is that the user studies results may not be generalizable to non-US populations.

In our future work, we aim to improve the design of MyCam by implementing the above design guidelines and evaluate how they meet the user needs. We also aim to implement the data-related privacy controls designs in the context of other smart home devices, such as voice speakers, baby monitors, thermostats, etc. Future studies should also conduct studies with non-US populations.

6.6 Conclusion

We proposed the design of privacy settings for home IoT devices based on user requirements of data-related privacy controls from prior work. We implemented a prototype and evaluated various aspects of it through qualitative and quantitative user studies. User studies showed that the prototype provided good perceived information control, user satisfaction and intention-to-use. We identified that the prototype can be improved to provide better user experience. We also discussed some design recommendations to further improve the design.

Chapter 7: Conclusion and Future Work

Through this dissertation, I have explored how to design privacy controls for smart home devices (SHD). I have systematized the state of the art in privacy vulnerabilities of the smart home. I have developed insights on the privacy concerns of the users as well as non-users of the smart home. I have conducted studies to understand the privacy control needs of smart home users. Additionally, I have implemented the privacy control needs and developed MyCam to inform the design of privacy controls for SHDs. I have also evaluated the MyCam design to inform future improvements to the design.

This dissertation advances the field of HCI with knowledge about SHD vulnerabilities, SHD users' privacy concerns and privacy controls needs, and the design of privacy controls. Researchers and developers can use the empirical findings about the smart home privacy control needs to design and develop privacy controls in smart home devices. Similarly, designers can use the prototype to inform the design of their privacy control features while designing such controls in their SHDs.

Thus, this dissertation has characterized the privacy concerns of users and non-users, which are necessary to inform the design of usable privacy solutions. It has further identified factors necessary for the design of privacy features in smart home devices. In addition, it has presented a design of data privacy controls which helps smart home designers implement better privacy controls. This will help the highly evolving smart home industry design usable private smart home devices.

The user studies conducted for evaluation of MyCam prototype showed that it meets users' privacy control needs and that users would be interested in using the privacy controls

presented by the prototype design. However, the application can be better designed to enhance its usability and user experience. In light of this, Chapter 6 made some design recommendations for future improvements based on the evaluation results.

Thus, for future research, one possible direction is to improve the design of the app in terms of usability and user experience. This can be achieved by collaborating with user experience (UX) designers and experts. A further study could explore designs to reduce user burden, such as privacy presets. Presets allow users to pick a range of privacy options through one click or a slider bar. This can make the privacy controls less burdensome and more usable.

In addition, the smart home domain will also benefit from research that applies the design of MyCam in the context of other SHDs (such as thermostats, baby monitors, and voice speakers) and evaluate the design in those contexts. Future studies could integrate the design presented in this dissertation with other privacy control types, such as transparency-related controls, which were described in Chapter 5.

Another possible direction for future research is to evaluate vulnerabilities of existing smart home devices through technical analyses of current security and privacy controls. Investigating for flaws in existing protocols, software frameworks, and authentication mechanisms, as well as developing new ones, can help the smart home industry manufacture more secure and private SHDs. Other useful areas of research include technical solutions for safeguarding smart home data, such as secure data transmission and data protection technologies.

Evaluating current privacy interfaces of existing SHDs can also be useful in identifying implementation gaps. Identifying the gaps in implementations of privacy controls based on the presented framework will benefit the designers in improving their designs of privacy controls.

Finally, the studies reported in this dissertation included participants only from the United States. Future studies could investigate other populations around the world. Follow-up experimental studies could be conducted to validate the findings of this dissertation in other cultural and international contexts.

Appendix A: Glossary and Acronyms

A.1 Glossary

Internet of Things The term Internet of Things was coined by Kevin Ashton [2]. Although the original term referred to RFID-enabled devices connected to the Internet, currently the term includes any physical object with sensors that are connected to the Internet.

Smart Home A home containing IoT devices that automate user tasks and allow remote control of user tasks, such as a smart camera that allows user to monitor the safety of the home. Examples: Amazon Echo, Google Home, Nest Thermostat, etc.

Privacy Privacy is defined in various ways. According to Clarke (1999), "privacy is often thought of as a moral right or a legal right, but it's often more useful to perceive privacy as the interest that individuals have in sustaining a personal space, free from interference by other people and organizations" [165]. Westin defined privacy as an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others" [217].

Information Privacy Information privacy is defined as combination of privacy of personal communication and privacy of personal data [172]. The information privacy concerns multilevel framework argues that information privacy concerns (IPC) involve four constructs (individual IPC, group IPC, organizational IPC, and societal IPC), each impacted by multiple factors, such as individual differences, group dynamics, organizational environment, and government involvement [172].

Solove's Taxonomy Solove's taxonomy of privacy harms is widely used to understand and characterize various privacy problems. It identifies the major activities leading to privacy violations and categorizes them into four groups: (1) information collection (surveillance and interrogation), (2) information processing (aggregation, identification, insecurity, secondary use and exclusion), (3) information dissemination (breach of confidentiality, disclosure, increased accessibility, blackmail, appropriation, and distortion), and (4) privacy invasion (intrusion and decisional interference) [173].

Privacy Control A privacy control is "an administrative, technical, or physical safeguard employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks" [218]. The privacy controls discussed in this dissertation are mainly technical.

A.2 List of Acronyms

ACK Acknowledgement

ACM Association for Computing Machinery

AES Advanced Encryption Standard

AMT Amazon Mechanical Turk

API Application Programming Interface

ASP Artificial Spoofing Packet

CCTV Closed-circuit Television

CSV Comma Separated Values

DDoS Distributed Denial of Service

DNS Domain Name System

DoS Denial of Service

DVR Digital Video Recorder

EU European Union

GDPR General Data Protection Regulation

GTS Guaranteed Time Slot

HANID Home Area Network Identification

HCI Human-computer Interaction

HIPAA Health Insurance Portability and Accountability Act

HIT Human Intelligence Task

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

IP Internet Protocol

IPA Intelligent Personal Assistant

IPC Information Privacy Concerns

IRB Institutional Review Board

IUIPC Internet Users' Information Privacy Concerns

LED Light Emitting Diode

LES Lightweight Encryption for Smart homes

MAC Media Access Control

MIoTL Mitigation of Internet of Things Leakage

MITM Man in the Middle

MTurk Amazon Mechanical Turk

NU Non-User

OS Operating System

PCF Privacy Controls Framework

POMDP Partially Observable Markov Decision Process

PPA Presence Privacy Attack

PTP Precision Time Protocol

RA Replay Audio

RFID Radio Frequency Identification

SEP Smart Energy Profile

SH Smart Home

SHD Smart Home Device

SHV Smart Home Vulnerabilities

SILDA Secure, Intuitive and Low-cost Device Authentication

SONAR Sound Navigation Ranging

SUS System Usability Scale

SH Transport Layer Security

TV Television

U User

UDP User Datagram Protocol

UEQ User Experience Questionnaire

US United States

UX User experience

VCS Voice Command System

VoIP Voice over Internet Protocol

VUI Voice User Interface

WiFi Wireless Fidelity

Appendix B: Interview Scripts

B.1 Interview Protocol

B.1.1 Screening Questions

1. Do you currently use a smart home device? [Yes/No]

2. How many smart home devices do you use? [1-5+]

3. What smart home devices do you use?

B.1.2 Interview Questions

[Informed Consent] [Permission to Record]

1. (Introduce the app) Many smart home device users like to manage privacy of their data. We have designed privacy settings of an app for possible use with a smart home device.

   Imagine you have an indoor video camera and the app you are about to see provides privacy settings regarding your data collected by the camera, stored by the company and shared or sold by the company. We are calling this app MyCam. At this stage, we are in initial design phase. Your feedback will help improve the design of this app.

   Today, you will be evaluating the privacy settings of this MyCam app designed to provide privacy controls to the smart home device user. I will provide you a link to the app. (Give the link to the participant).

   Please take a few minutes to browse through the MyCam app and familiarize with it.

2. (When participant is done familiarizing with the MyCam app, ask them to share their screen, so the interviewer can see the participant's interaction with the MyCam app.) Please perform the following tasks in the MyCam app:

   - TASK1 On the About page, we introduce you to the MyCam app. Read the introduction. Feel free to ask any questions. When done, Click Continue to go the privacy settings page. Did this work for you?

     BROWSEAPP The privacy settings page gives you options to manage your data privacy. We will now ask you to perform the following tasks in the app.

   - TASK2 This app gives you choice to opt in to data collection. Imagine that you want to opt in to data collection. Now in the MyCam app, please turn on Opt In to Data Collection. Did this work for you?

   - TASK3 Continuing with the hypothetical scenario that you would allow the MyCam to collect data about you. Please pick what data you would allow the MyApp to collect about you. Pick from name, email and other options you are given. Did this work for you?

   - TASK4 Imagine that MyApp gives you the choice of allow (or disallow) sending of data to the cloud. Did this work for you?

   - TASK5 MyCam app may share your data with business partners and other entities if you turn on sharing. Assume you are comfortable with allowing sharing of your and turn on Allow sharing of data. Did this work for you?

   - TASK6 Choose who you would like the company to share the data with (advertisers, government, business partners). Did this work for you?

   - TASK7 Click View and Manage Data to go to the data dashboard. Select the fist audio file 2022-03-01-1001.mp3. Delete this file. Did this work for you?

- TASK8 Go to the About page. Did this work for you?

3. What do you like about the app?
4. What do you dislike about the app?
5. What were your challenges in using the app ?
6. How can we improve the app?
7. How does the app meet your privacy control requirements?
8. How can this app to better meet your smart home privacy needs?
9. Now I'd like to ask you to take a few minutes to give us your assessment of the app. We have designed a questionnaire for this purpose. (Provide link to the participant. Allow time to complete the questionnaire.)
10. (Debrief and thank the participant).

Appendix C: Surveys

C.1 Privacy Controls Survey Questions

1. Smart home involves the control and automation of home appliances such as washer/dryers, ovens or refrigerators/freezers as well as lighting, ventilation, air conditioning (HVAC), heating (such as smart thermostats), and security. When connected with the Internet, smart home devices are an important constituent of the Internet of Things ("IoT"). The user interface for control of these devices uses wall-mounted terminals, tablet or desktop computers, mobile phone application, or Web interface that may also be accessible through the Internet.

   Below you can see example diagrams of three smart home devices: *(Pictures of Amazon Echo, Nest Doorbell, and Smart TV were shown).*

2. From the given pictures, select the pictures of smart home devices. Please select all that apply. *(Options included pictures of a Nikon SLR camera, Nest learning thermostat, standard Philips blender, Google Home smart speaker, Philips Hue smart light bulb and hub).*

3. Do you currently use a smart home device? [Yes/No]

4. *(If "Yes" selected in 3)* What smart home devices do you use? Please check all that apply.

   - Security camera
   - Doorbell camera
   - Baby monitor

- Pet technology
- Motion sensor
- Smoke detector
- Leak sensor
- Smart lock
- Door/window alarm
- Garage door
- Smart light
- Switch/plug
- Voice assistant
- Audio/speakers
- Thermostat
- Smart/automation hub
- Other (Please specify)

5. *(If "Yes" selected in 3)* How many smart home devices do you use? (Please specify)

6. *(If "Yes" selected in 3)* For how long have you used smart home devices?

    - ¡1 year
    - 1-2 years
    - 3-5 years
    - 5+ years

7. Do you currently own a smart home device? [Yes/No]

8. *(If "Yes" selected in 7)* What smart home devices do you own? Please check all that apply.

    - Security camera
    - Doorbell camera
    - Baby monitor
    - Pet technology
    - Motion sensor
    - Smoke detector
    - Leak sensor
    - Smart lock
    - Door/window alarm
    - Garage door
    - Smart light
    - Switch/plug
    - Voice assistant
    - Audio/speakers
    - Thermostat
    - Smart/automation hub
    - Other (Please specify)

9. *(If "Yes" selected in 7)* How many smart home devices do you own? (Please specify)

10. *(If "Yes" selected in 7)* For how long have you owned smart home devices?

- ¡1 year
- 1-2 years
- 3-5 years
- 5+ years

11. *(Open-ended question)* What privacy concerns do you have regarding smart home devices, if any? Provide as much detail as possible.

12. *(Open-ended question)* What actions do you take to address the privacy concerns regarding smart home devices?

13. In an app for users of smart home devices, what features would you like to manage your privacy? Select all that apply.

    - Manage data collection, use and sharing
    - View privacy policy, terms and related information
    - Control smart home devices, such as turning them off
    - Monitoring data and opting in or out
    - Manage multiple users and their accounts
    - Learn about features and their implications
    - Secure the devices with password and other features
    - Other (Please specify)

    (In questions 14-21, words capitalized and in parentheses represent the sub-factors and were not shown to participants.)

14. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:

- To choose what data is collected, used and shared. (CHOICE)
- To provide consent for any data collection, use and sharing (CONSENT)
- To delete collected data, audio and video files. (DELETION)
- To not share information about me and how I use my smart home device. (DO NOT SHARE)
- To store data locally in my device or my home network and not in the cloud. (LOCAL STORAGE)

15. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - I want to have information on device capabilities, what data is collected, and how is is protected and shared. (INFO)
    - I want to see and know when smart home device is recording and collecting data. (INDICATOR)
    - I want to see an easy-to-read explanation of privacy policy of the company. (PRIVACY POLICY)
    - I want to be notified when my personal information is used. (NOTIFICATION)
16. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - Disconnect the device from the Internet. (DISCONNECT)
    - Mute my device. (MUTE)
    - Put my device to sleep. (SLEEP)
    - Turn off all devices at once. (TURN OFF)

- *(Attention Check Question)* Paying attention to the survey. Please select 'Somewhat disagree' to this option.

17. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - To limit what data is collected. (LIMIT)
    - To monitor what data is collected. (MONITOR)
    - By default no data should be collected. I want to sign up for data collection when needed. (OPT IN)
    - I want to stop data collection when needed. (OPT OUT)

18. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - To create and manage multiple users in my home network. (MULTI USER SETTINGS)
    - Default settings should maximize privacy. (PRIVACY BY DEFAULT)
    - One users data are not seen by other users of my home network. (USER LEVEL PRIVACY)
    - Each user to set their own privacy settings. (USER LEVEL SETTINGS)

19. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - Tips and training on how to use the smart home device. (TRAINING)
    - To know if an independent third party company has reviewed and certified the privacy features of the device. (INDEPENDENT REVIEW)

- Government regulation requiring protection of data and privacy. (LEGISLATION)

20. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - Central control for all my home devices. (CENTRAL INTERFACE)
    - Easy-to-use and intuitive features (USER-FRIENDLY INTERFACE)
    - By design, it should provide maximum privacy and security (DESIGN)
    - *(Attention Check Question)* Select 'Somewhat agree' to let us know that you are paying attention.
21. *(Five-point Likert options from Strongly Disagree to Strongly Agree)* From the following, select your level of agreement with the options you want in smart home devices:
    - Setup password or other authentication such as fingerprint. (AUTHENTICATION)
    - Notify me when some one accesses my device or its data. (ACCESS DETECTION)
    - Data are protected by encryption or other data protection techniques. (ENCRYPTION)
    - Choose who is allowed access to my device and its data. (NETWORK CONTROL)
    - Generate secure passwords. (PASSWORDS)
22. *(Open-ended question)* Think about any additional privacy features that you want in a smart home device (or app). Type them below in the box below as much detail as

possible.

23. *(IUIPC Scale [176], Seven-point Likert options from Strongly Disagree to Strongly Agree)* Please rate your level of agreement with the following statements:

    - Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used and shared.
    - Consumer control of personal information lies at the heart of consumer privacy.
    - I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
    - Companies seeking information online should disclose the way the data are collected, processed, and used.
    - A good consumer online privacy policy should have a clear and conspicuous disclosure.
    - It is very important to me that I am aware and knowledgeable about how my personal information will be used.
    - It usually bothers me when online companies ask me for personal information.
    - When online companies ask me for personal information, I sometimes think twice before providing it.
    - It bothers me to give personal information to so many online companies.
    - I'm concerned that online companies are collecting too much personal information about me.

24. What is your gender?

    - Male

- Female
- Non-binary / third gender
- Prefer not to respond

25. What is your age? (Please specify)

26. Do you live in the US? [Yes/No]

27. How many hours do you spend using the Internet every week? [Slider: 0-168 hours per week]

28. *(Open-ended question)* What is your occupation?

29. What is the highest level of school you have completed or the highest degree you have received?

    - Less than high school degree
    - High school graduate (high school diploma or equivalent including GED)
    - Some college but not degree
    - Associate degree in college (2-year)
    - Bachelor's degree (4-year)
    - Master's degree
    - Doctoral degree
    - Professional degree (JD, MD)

30. Information about income is very important to understand. Please indicate the answer that includes your entire household income in (previous year) before taxes.

    - Less than $10,000

- $10,000 - $19,999
- $20,000 - $29,999
- $30,000 - $39,999
- $40,000 - $49,999
- $50,000 - $59,999
- $60,000 - $69,999
- $70,000 - $79,999
- $80,000 - $89,999
- $90,000 - $99,999
- $100,000 - $149,999
- More than $150,000

31. What is the size of your household?

- 1
- 2
- 3
- 4
- 5
- 6
- 7 or more

32. Are you now married, widowed, divorced, separated, or never married?

- Married

- Widowed
- Divorced
- Separated
- Never married

33. Do you have any comments or suggestions for this survey? Thanks

C.2 Prototype Evaluation Survey Questions

1. *(Consent)* In this survey, you will evaluate an app and provide your feedback. If you agree to do so, please proceed using the option below. You can leave the survey at any time. [Agree/Disagree]

2. Do you currently use a smart home device? [Yes/No]

3. How many smart home devices do you use? [1-5+]

4. Demographic Questions: Age, Gender, Employment, Marital Status, Location, Education, Income.

5. These questions ask for your feedback on MyCam app. Your answers will help us understand the strengths and weaknesses of our app. The app should open below. If not, click here to open the app in your browser.

   Imagine you have a MyCam indoor video camera installed in your house. The app below allows you to remotely operate the camera and manage privacy settings.

   Please use the app below and share your feedback. [Show app] *(Task questions were inspired by [206])*

- TASK1 Click Continue on the MyCam Home page to go the privacy settings page. Did this work for you?
- BROWSEAPP The privacy settings page gives you options to manage your data privacy. We will now ask you to perform the following tasks in the app.
- TASK2 This apps allows you to control data collected about you. Assume you want to allow data collection. Turn on Opt In to Data Collection. Did this work for you?
- TASK3 Think about what data you would allow the MyCam to collect about you. Pick from name, email and other options you are given. Did this work for you?
- TASK4 Assume that you are not comfortable sending your data to cloud. Turn off Allow sending of data to the cloud. Did this work for you?
- TASK5 MyCam app may share your data with business partners and other entities if you turn on sharing. Assume you are comfortable with allowing sharing of your data and turn on Allow sharing of data. Did this work for you?
- TASK6 Choose who you would allow the company to share the data with (advertisers, government, or business partners). Did this work for you?
- TASK7 Think about whether you would allow or disallow MyCam to sell your data. Turn on (or off) Allow selling of data. Did this work for you?
- TASK8 Click View and Manage Data to go to the data dashboard. Select the fist audio file 2022-03-01-1001.mp3. Delete this file. Did this work for you?
- TASK9 Go to the MyCam Home page. Did this work for you?
- IMPROVE Feel free to browse through the app. How can we improve the app?

6. *(Open-ended question)* What were your **challenges** in using the app ?

7. *(Open-ended question)* How can we **improve** the app to meet your smart home privacy needs?

8. *(User Experience Questionnaire [211], 7 point scale, -3 to +3)* For the assessment of the product, please fill out the following questionnaire. The questionnaire consists of pairs of contrasting attributes that may apply to the product. The circles between the attributes represent gradations between the opposites. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

   Please decide spontaneously. Don't think too long about your decision to make sure that you convey your original impression. It is your personal opinion that counts. Please remember: there is no wrong or right answer! [Present scale items here.]

9. *(System Usability Scale Questions [212], Likert Options: Strongly Disagree (1) to Strongly Agree (5))*

   - I think that I would like to use this system frequently
   - I found the system unnecessarily complex
   - I thought the system was easy to use
   - I think that I would need the support of a technical person to be able to use this system
   - I found the various functions in this system were well integrated
   - I thought there was too much inconsistency in this system
   - I would imagine that most people would learn to use this system very quickly
   - I found the system very cumbersome to use
   - I felt very confident using the system

- I needed to learn a lot of things before I could get going with this system

10. *(Attention Check Questions)*

    - AT1 How likely are you to purchase this app? Please select neither for this question.
    - ATT2 Do you agree that this app is named well? Please select agree for this question.

    (Perceived Information Control[214], Likert Scale 1-7)

11. How much control do you feel you have over the amount of your personal information collected by MyCam?

12. How much control do you feel you have over who can get access to your personal information?

13. How much control do you feel you have over your personal information that has been released to MyCam?

14. How much control do you feel you have over how your personal information is being used by MyCam?

15. Overall, how much in control do you feel you have over your personal information provided to MyCam?

    (User Satisfaction [213] Likert Scale 1-7)

    Please rate your overall satisfaction with MyCam.

16. How adequately do you feel the MyCam **meets** your privacy needs ?

17. How **efficient** is MyCam?

18. How **effective** is MyCam?

19. Overall, how **satisfied** are you with MyCam?

    (Behavioral Intention to Use), Likert 1-7, Adapted and modified from [215]

20. How likely are you to use MyCam's privacy settings if available to you?

21. How likely are you to recommend others to use MyCam's privacy settings?

22. How likely are you to use privacy settings of other apps in the future?

Appendix D: Coding Manuals

D.1 Privacy Controls Categories, Sub-categories, and Codes

Design Factors	Sub-factors	Codes	n=215	%
Data-Related Controls			**85**	**39.53%**
	Choice		**24**	**11.16%**
		choose what data to use	1	0.47%
		choose what is (not) shared	2	0.93%
		choose what is in your profile	1	0.47%
		choose what is shared between devices	1	0.47%
		choose what is transmitted	4	1.86%
		choose when to delete	2	0.93%
		choose when to record	3	1.40%
		choose who has access to data	6	2.79%
		choose who to send data to	1	0.47%
		disallow information to public	1	0.47%
		do not store payment information	1	0.47%
		don't allow company to access data	1	0.47%
	Monitor		**16**	**7.44%**
		audit data	3	1.40%
		monitor data	4	1.86%
		replay audio files	1	0.47%
		view activity	1	0.47%
		view audio logs	1	0.47%
		view collected data	5	2.33%
		view who has access to data	1	0.47%
	Deletion		**14**	**6.51%**
		delete data	7	3.26%
		delete data (after use termination)	1	0.47%
		delete data (all, onebyone)	1	0.47%
		delete data (audio, logs)	1	0.47%
		delete data (logs)	1	0.47%
		delete data after specified period	1	0.47%
		delete data automatically	1	0.47%
		delete personal information	1	0.47%
	Do not share		**8**	**3.72%**
		do not share	3	1.40%
		do not share (default/option to share)	2	0.93%
		do not share personal information	1	0.47%
		do not share usage statistics	1	0.47%
		no default social media sharing	1	0.47%
	Consent		**6**	**2.79%**
		consent (data collection)	1	0.47%
		consent (data usage)	2	0.93%
		consent (share information)	1	0.47%
		consent (transfer information)	1	0.47%
		consent (update)	1	0.47%
	Opt out		**5**	**2.33%**

		opt out	5	2.33%
	Complete control		**4**	**1.86%**
		complete data control	4	1.86%
	Opt in		**3**	**1.40%**
		opt out (default)	3	1.40%
	Limit		**3**	**1.40%**
		limit data collection	2	0.93%
		turn off sharing (health data)	1	0.47%
	Local storage		**2**	**0.93%**
		manage data	1	0.47%
		option to store data locally	1	0.47%
Transparency			**42**	**19.5%**
	Easy-to-Read explanation		**24**	**11.2%**
		clear terms and privacy policies	2	0.9%
		clear terms of service/privacy policies	1	0.5%
		disclaimer (what data are collected)	1	0.5%
		easy to read explanation: consent	2	0.9%
		easy to read explanation: data purpose	1	0.5%
		easy to read explanation: retention period	1	0.5%
		easy to read explanation: type of data collected	1	0.5%
		easy to read terms	3	1.4%
		information on device capabilities	1	0.5%
		information on how data will be protected	1	0.47%
		easy to read explanation: how data will be used	4	1.86%
		easy to read explanation: what data will be collected	3	1.40%
		easy to read explanation: how will data be used	1	0.47%
		easy to read explanation: what data will be stored	1	0.47%
		information on benefits and drawbacks of sharing data	1	0.47%
	Indicators		**10**	**4.7%**
		indicator (audio)	1	0.5%
		indicator (listening)	2	0.9%
		indicator (on)	1	0.5%
		indicator (recording)	2	0.9%
		indicator (video)	1	0.5%
		Indicators	1	0.5%
		indicators (alarms)	1	0.5%
		indicators (LED, device status)	1	0.47%
	Transparency		**5**	**2.3%**
		transparency	5	2.3%
	Notification		**3**	**1.4%**
		notification; option to keep/erase	1	0.47%
		notification/awareness when data are used	1	0.5%
		status notification (audio/video)	1	0.5%

Centralized Interface			**35**	**16.3%**
	User-friendly Interface		**18**	**8.4%**
		ADA friendly interfaces (for children and elderly)	1	0.5%
		child friendly interface	1	0.5%
		easy access	2	0.9%
		easy basic and advanced controls	1	0.5%
		easy interface	6	2.8%
		intuitive controls	1	0.5%
		mobile interface	1	0.5%
		quick controls	1	0.5%
		reduce user burden	1	0.5%
		user friendly app	1	0.5%
		voice activation	1	0.5%
		do-it-yourself interface	1	0.47%
	Central interface		**15**	**7.0%**
		app displaying all devices and data	2	0.9%
		automation	1	0.5%
		central control for all devices	1	0.5%
		centralized control interface	3	1.4%
		centralized privacy interface	1	0.5%
		interface showing how the data is used	1	0.5%
		interface showing what data is collected	1	0.5%
		open source friendly	1	0.5%
		privacy-centric design	1	0.5%
		report of collected data	1	0.5%
		standard privacy control system	1	0.5%
		visualize data	1	0.5%
	Design		**2**	**0.9%**
		privacy-centric design	1	0.5%
		safety-focused design	1	0.5%
Device Controls			**28**	**13.0%**
	Turn off		**15**	**7.0%**
		turn all devices off	4	1.9%
		turn all devices off (for specified period)	1	0.5%
		turn off recording /listening	4	1.9%
		turn specific device off	6	2.8%
	Disconnect		**7**	**3.3%**
		disconnect from Internet	4	1.9%
		hardware disconnect	1	0.5%
		permission to connect	1	0.5%
		separate home network	1	0.5%
	Mute		**3**	**1.4%**
		mute	3	1.4%
	Sleep mode		**3**	**1.4%**
		sleep mode	3	1.4%

Multi-user Controls		**11**	**5.1%**
	User-level settings	**4**	**1.9%**
	add/remove users	1	0.5%
	do not share (with other users)	1	0.5%
	option to give permission to family members	1	0.5%
	user-level data display	1	0.5%
	User-level privacy	**3**	**1.4%**
	anonymize	1	0.5%
	customizing privacy settings	1	0.5%
	scheduled operation	1	0.5%
	Multi-user privacy settings	**3**	**1.4%**
	multi-user privacy settings	3	1.4%
	Privacy By Default	**1**	**0.5%**
	default privacy optimized	1	0.5%
Security Controls		**7**	**3.3%**
	Password control	**3**	**1.4%**
	generate secure passwords	1	0.5%
	password	2	0.9%
	Access Detection	**1**	**0.5%**
	option to detect unauthorized access	1	0.5%
	Authentication	**1**	**0.5%**
	fingerprint/password authentication	1	0.5%
	Network control	**1**	**0.5%**
	choose who is allowed to network	1	0.5%
	Encryption	**1**	**0.5%**
	encrypt data	1	0.5%
User Support		**7**	**3.3%**
	Legislation	**5**	**2.33%**
	better data rights	1	0.47%
	legislation on companies	1	0.47%
	mandatory deletion	1	0.47%
	neutral Law	1	0.47%
	right to delete	1	0.47%
	Awareness	**1**	**0.47%**
	user training	1	0.47%
	Independent review	**1**	**0.47%**
	display 'certified privacy' status	1	0.47%

Appendix E: Additional Results

E.1 Stacked Bar Chart Showing Frequencies of Sub-Factors

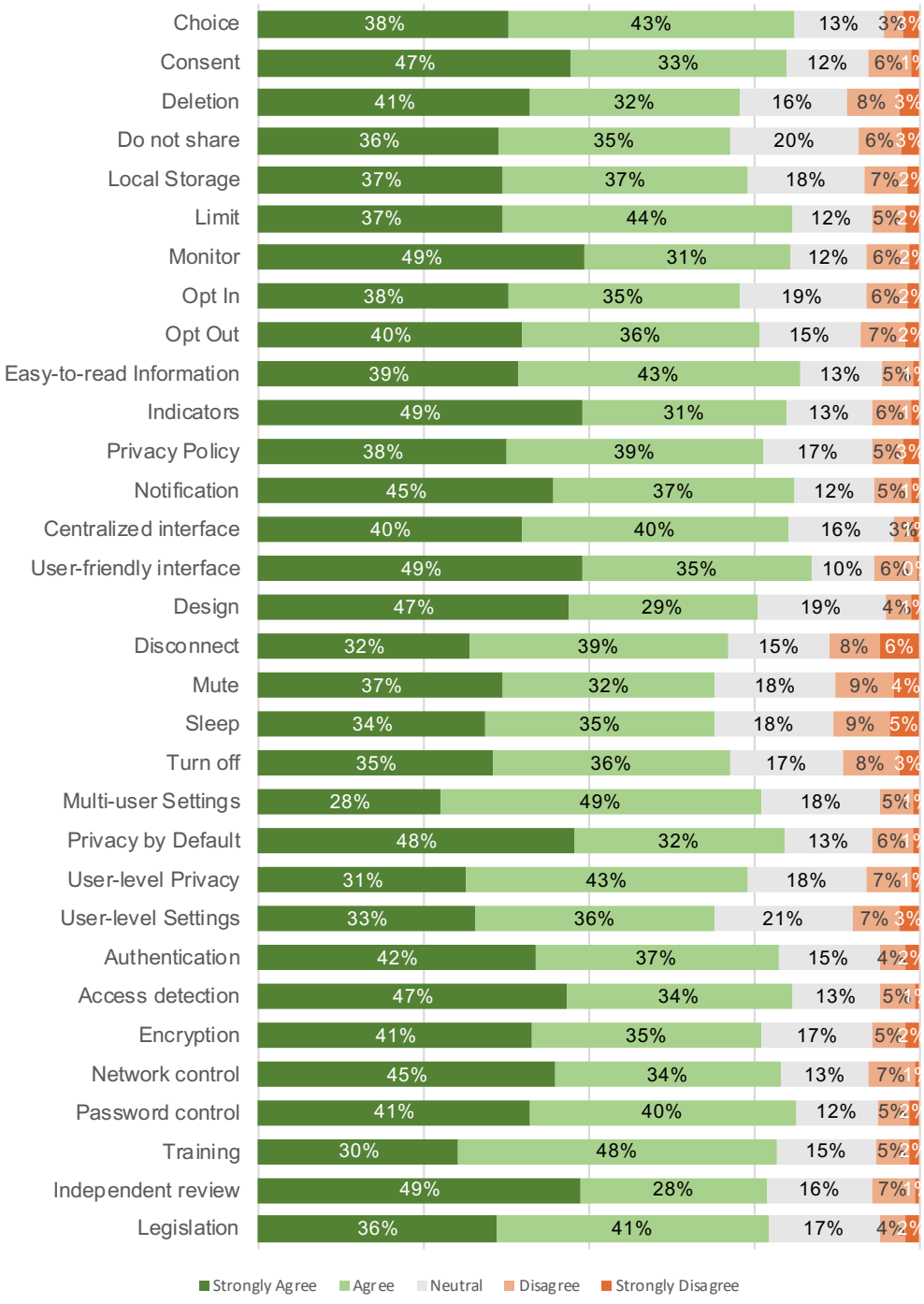


Figure E.1: Frequency breakdown of survey responses for the 32 sub-factors.

Bibliography

[1] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[2] K. Ashton, "That 'internet of things' thing," *RFiD journal*, vol. 22, no. 7, pp. 97–114, 2009.

[3] "Research & Advisory, Gartner," https://www.gartner.com/technology/research.jsp, [Accessed 12-Nov-2021].

[4] "Insider Intelligence — BI intelligence," http://www.businessinsider.com/research, [Accessed 12-Nov-2021].

[5] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, pp. 1–20, 2018.

[6] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in *2016 IEEE Symposium on Security and Privacy (SP)*. California: IEEE, 2016, pp. 636–654. [Online]. Available: http://ieeexplore.ieee.org/document/7546527/

[7] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security Analysis of Internet-of-Things: A Case Study of August Smart Lock," in *MobiSec 2017: Security, Privacy, and Digital Forensics of Mobile Systems and Networks*, Georgia, 2017, pp. 499–504. [Online]. Available: https://courses.csail.mit.edu/6.857/2017/project/3.pdf

[8] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[9] N. Bowles, "Thermostats, locks and lights: Digital tools of domestic abuse," Jul 2018. [Online]. Available: https://www.sfgate.com/business/article/Thermostats-locks-and-lights-digital-tools-of-13040641.php

[10] C. Chhetri and V. G. Motti, "User centric privacy controls for smart homes," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, Nov 2022. [Online]. Available: https://doi.org/10.1145/3555769

[11] ——, "Eliciting privacy concerns for smart home devices from a user centered perspective," in *Information in Contemporary Society. iConference 2019. Lecture Notes in Computer Science, vol 11420*, N. G. Taylor, C. Christian-Lamb, M. H. Martin, and B. Nardi, Eds. Cham: Springer, 2019, pp. 91–101.

[12] C. Chhetri and V. Motti, "Identifying older adults' expectations of privacy-preserving controls for smart home devices," in *CSCW Workshop on Networked Privacy, "Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms"*, Nov 2019.

[13] C. Chhetri, "Towards a smart home usable privacy framework," in *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*, ser. CSCW '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 43–46. [Online]. Available: https://doi.org/10.1145/3311957.3361849

[14] C. Chhetri and V. Motti, "Identifying vulnerabilities in security and privacy of smart home devices," in *National Cyber Summit*. Springer, 2020, pp. 211–231.

[15] ——, "Privacy concerns about smart home devices: A comparative analysis between non-users and users," in *Human Factors in Cybersecurity*, vol. 53, AHFE International. AHFE Open Access, 2022, pp. 102–110. [Online]. Available: https://doi.org/10.54941/ahfe1002207

[16] C. Chhetri and V. G. Motti, "Designing and evaluating a prototype for data-related privacy controls in a smart home," in *Human Aspects of Information Security and Assurance*, N. Clarke and S. Furnell, Eds. Cham: Springer International Publishing, 2022, pp. 240–250. [Online]. Available: https://doi.org/10.1007/978-3-031-12172-2_19

[17] N. Fruchter and I. Liccardi, "Consumer attitudes towards privacy and security in home assistants," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–6.

[18] E. Zeng and F. 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.

[19] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, pp. 1–31, 2018.

[20] R. E. Freeman, *Strategic management: A stakeholder approach*. Cambridge university press, 2010.

[21] M. Goulden, "'delete the family': platform families and the colonisation of the smart home," *Information, Communication & Society*, vol. 24, no. 7, pp. 903–920, 2021. [Online]. Available: https://doi.org/10.1080/1369118X.2019.1668454

[22] J. Cocco, "Smart home technology for the elderly and the need for regulation," *Pitt. J. Envtl. Pub. Health L.*, vol. 6, p. 85, 2011.

[23] J. O. Wobbrock and J. A. Kientz, "Research contributions in human-computer interaction," *Interactions*, vol. 23, no. 3, p. 38–44, Apr 2016. [Online]. Available: https://doi.org/10.1145/2907069

[24] M. Hung, *Leading the IoT*. Gartner, Inc., 2017. [Online]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook{_}digital.pdf

[25] E. Zeng, S. Mare, and F. Roesner, "End User Security & Privacy Concerns with Smart Homes," in *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[26] V. Chang, P. Chundury, and M. Chetty, ""Spiders in the Sky": User Perceptions of Drones, Privacy, and Security," *Chi'17*, 2017. [Online]. Available: https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017{_}CameraReady.pdf

[27] M. Antonakakis, T. April, M. Bailey, E. Bursztein, J. Cochran, Z. Durumeric, J. Alex Halderman, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[28] K. Hill, "How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old." *Forbes.com*, 2013.

[29] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, Are You Listening? Privacy Perceptions , Concerns and Privacy-seeking Behaviors with Smart Speakers," in *Proceedings of ACM Human-Computer Interaction*, vol. 2, no. CSCW, 2018, pp. 102:1–31.

[30] R. Hoenkamp, G. B. Huitema, and A. J. C. D. M. V. Vugt, "The Neglected Consumer: The Case of the Smart Meter Rollout in the Netherlands," *Renewable Energy Law and Policy*, vol. 4, no. November 2011, pp. 269–282, 2014.

[31] M. N. Anwar, M. Nazir, and K. Mustafa, "Security threats taxonomy: Smart-home perspective," in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, 2017, pp. 1–4.

[32] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[33] A. K. Das, S. Zeadally, and M. Wazid, "Lightweight authentication protocols for wearable devices," *Computers & Electrical Engineering*, vol. 0, pp. 1–13, 2017. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0045790617305347

[34] X. Ma, N. Goonawardene, and H. P. Tan, "Identifying elderly with poor sleep quality using unobtrusive in-home sensors for early intervention," in *Proceedings of the 4th EAI International Conference on Smart Objects and Technologies for Social Good*, ser. Goodtechs '18. New York, NY, USA: ACM, 2018, pp. 94–99. [Online]. Available: http://doi.acm.org/10.1145/3284869.3284894

[35] K. T. Mahadewa, K. Wang, G. Bai, L. Shi, J. S. Dong, and Z. Liang, "Homescan: Scrutinizing implementations of smart home integrations," in *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, Dec 2018, pp. 21–30.

[36] M. Moody and A. Hunter, "Exploiting known vulnerabilities of a smart thermostat," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 50–53.

[37] W. Hsieh and J. Leu, "A dynamic identity user authentication scheme in wireless sensor networks," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2013, pp. 1132–1137.

[38] J. Bugeja, D. Jönsson, and A. Jacobsson, "An investigation of vulnerabilities in smart connected cameras," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2018, pp. 537–542.

[39] M. Saleh, N. B. Al Barghuthi, K. Alawadhi, F. Sallal, and A. Ferrah, "Streamlining x201c;smart grid end point devices x201d; vulnerability testing using single board computer," in *2018 Advances in Science and Engineering Technology International Conferences (ASET)*, Feb 2018, pp. 1–6.

[40] R. Alharbi and D. Aspinall, "An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, March 2018, pp. 1–10.

[41] E. McMahon, M. Patton, S. Samtani, and H. Chen, "Benchmarking vulnerability assessment tools for enhanced cyber-physical system (cps) resiliency," in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Nov 2018, pp. 100–105.

[42] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899–1909, Dec 2017.

[43] A. Sivanathan, F. Loi, H. H. Gharakheili, and V. Sivaraman, "Experimental evaluation of cybersecurity threats to the smart-home," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec 2017, pp. 1–6.

[44] X. Lei, G. Tu, A. X. Liu, C. Li, and T. Xie, "The insecurity of home digital voice assistants - vulnerabilities, attacks and countermeasures," in *2018 IEEE Conference on Communications and Network Security (CNS)*, May 2018, pp. 1–9.

[45] A. Sun, W. Gong, R. Shea, and J. Liu, "A castle of glass: Leaky IoT appliances in modern smart homes," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 32–37, December 2018.

[46] R. Johnson, M. Elsabagh, A. Stavrou, and J. Offutt, "Dazed droids: A longitudinal study of android inter-app vulnerabilities," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: ACM, 2018, pp. 777–791. [Online]. Available: http://doi.acm.org/10.1145/3196494.3196549

[47] A. Tekeoglu and A. Tosun, "Blackbox security evaluation of chromecast network communications," in *2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC)*, Dec 2014, pp. 1–2.

[48] ——, "A closer look into privacy and security of chromecast multimedia cloud communications," in *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2015, pp. 121–126.

[49] X. Jia, X. Li, and Y. Gao, "A novel semi-automatic vulnerability detection system for smart home," in *Proceedings of the International Conference on Big Data and Internet of Thing*, ser. BDIOT2017. New York, NY, USA: ACM, 2017, pp. 195–199. [Online]. Available: http://doi.acm.org/10.1145/3175684.3175718

[50] J. Cipriani, "What you need to know about encryption on your phone," 2016. [Online]. Available: https://www.cnet.com/news/iphone-android-encryption-fbi/

[51] M. Zhang, Y. Liu, J. Wang, and Y. Hu, "A new approach to security analysis of wireless sensor networks for smart home systems," in *2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Sep. 2016, pp. 318–323.

[52] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," in *Data and Algorithmic Transparency Workshop (DAT)*, New York, 2016. [Online]. Available: http://datworkshop.org/papers/dat16-final37.pdf

[53] "Cost of Data Breach Study," 2018. [Online]. Available: www.ibm.com/security/data-breach

[54] Y. Liu, S. Hu, J. Wu, Y. Shi, Y. Jin, Y. Hu, and X. Li, "Impact assessment of net metering on smart home cyberattack detection," in *Proceedings of the 52Nd Annual Design Automation Conference*, ser. DAC '15. New York, NY, USA: ACM, 2015, pp. 97:1–97:6. [Online]. Available: http://doi.acm.org/10.1145/2744769.2747930

[55] A. Alanwar, B. Balaji, Y. Tian, S. Yang, and M. Srivastava, "Echosafe: Sonar-based verifiable interaction with intelligent digital agents," in *Proceedings of the 1st ACM Workshop on the Internet of Safe Things*, ser. SafeThings'17. New York, NY, USA: ACM, 2017, pp. 38–43. [Online]. Available: http://doi.acm.org/10.1145/3137003.3137014

[56] M. Braga, "People Are Complaining That Amazon Echo Is Responding to Ads on TV," 2015.

[57] Y. Meng, Z. Wang, W. Zhang, P. Wu, H. Zhu, X. Liang, and Y. Liu, "Wivo: Enhancing the security of voice control system via wireless signal in IoT environment," in *Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. Mobihoc '18. New York, NY, USA: ACM, 2018, pp. 81–90. [Online]. Available: http://doi.acm.org/10.1145/3209582.3209591

[58] K. M. Malik, H. Malik, and R. Baumann, "Towards vulnerability analysis of voice-driven interfaces and countermeasures for replay attacks," in *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, March 2019, pp. 523–528.

[59] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," *arXiv Preprint*, 2017. [Online]. Available: http://arxiv.org/abs/1708.05044

[60] S. M. Beyer, B. E. Mullins, S. R. Graham, and J. M. Bindewald, "Pattern-of-life modeling in smart homes," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5317–5325, Dec 2018.

[61] S. Gong and H. Li, "Anybody home? keeping user presence privacy for advanced metering in future smart grid," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, Dec 2011, pp. 1211–1215.

[62] H. Li, S. Gong, L. Lai, Z. Han, R. C. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1540–1551, Sep. 2012.

[63] C. Lee, L. Zappaterra, Kwanghee Choi, and Hyeong-Ah Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *2014 IEEE Conference on Communications and Network Security*, Oct 2014, pp. 67–72.

[64] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based home area network for metering in smart grids," *IEEE Systems Journal*, vol. 8, no. 2, pp. 509–520, June 2014.

[65] L. N. Whitehurst, T. R. Andel, and J. T. McDonald, "Exploring Security in ZigBee Networks," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, ser. CISR '14. New York, NY, USA: ACM, 2014, pp. 25–28. [Online]. Available: http://doi.acm.org/10.1145/2602087.2602090

[66] X. Feng, M. Ye, V. Swaminathan, and S. Wei, "Towards the security of motion detection-based video surveillance on IoT devices," in *Proceedings of the on Thematic Workshops of ACM Multimedia 2017*, ser. Thematic Workshops '17. New York, NY, USA: ACM, 2017, pp. 228–235. [Online]. Available: http://doi.acm.org/10.1145/3126686.3126713

[67] Y. Jia, Y. Xiao, J. Yu, X. Cheng, Z. Liang, and Z. Wan, "A novel graph-based mechanism for identifying traffic vulnerabilities in smart home IoT," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, April 2018, pp. 1493–1501.

[68] J. Wurm, K. Hoang, O. Arias, A. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jan 2016, pp. 519–524.

[69] M. M. Fouda, Z. M. Fadlullah, and N. Kato, "Assessing attack threat against zigbee-based home area network for smart grid communications," in *The 2010 International Conference on Computer Engineering Systems*, Nov 2010, pp. 245–250.

[70] D. M. Menon and N. Radhika, "Anomaly detection in smart grid traffic data for home area network," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, March 2016, pp. 1–4.

[71] T. Shen and M. Ma, "Security enhancements on home area networks in smart grids," in *2016 IEEE Region 10 Conference (TENCON)*, Nov 2016, pp. 2444–2447.

[72] R. Trimananda, A. Younis, B. Wang, B. Xu, B. Demsky, and G. Xu, "Vigilia: Securing smart home edge computing," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, Oct 2018, pp. 74–89.

[73] N. Gyory and M. Chuah, "IoTOne: Integrated platform for heterogeneous IoT devices," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, Jan 2017, pp. 783–787.

[74] J. D. Fuller and B. W. Ramsey, "Rogue z-wave controllers: A persistent attack channel," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, Oct 2015, pp. 734–741.

[75] I. Aouini, L. Ben Azzouz, M. Jebali, and L. A. Saidane, "Improvements to the smart energy profile security," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, June 2017, pp. 1356–1361.

[76] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '16. New York, NY, USA: ACM, 2016, pp. 195–200. [Online]. Available: http://doi.acm.org/10.1145/2939918.2939925

[77] W. Ahmad, J. Sunshine, C. Kaestner, and A. Wynne, "Enforcing fine-grained security and privacy policies in an ecosystem within an ecosystem," in *Proceedings of the 3rd International Workshop on Mobile Development Lifecycle*, ser. MobileDeLi 2015. New York, NY, USA: ACM, 2015, pp. 28–34. [Online]. Available: http://doi.acm.org/10.1145/2846661.2846664

[78] I. Sanchez, R. Satta, I. N. Fovino, G. Baldini, G. Steri, D. Shaw, and A. Ciardulli, "Privacy leakages in smart home wireless technologies," in *2014 International Carnahan Conference on Security Technology (ICCST)*, Oct 2014, pp. 1–6.

[79] A. U. Gawade and N. M. Shekokar, "Lightweight secure rpl: A need in IoT," in *2017 International Conference on Information Technology (ICIT)*, Dec 2017, pp. 214–219.

[80] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "Split: A secure and scalable rpl routing protocol for internet of things," in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2018, pp. 1–8.

[81] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in IoT," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[82] R. d. J. Martins, V. G. Schaurich, L. A. D. Knob, J. A. Wickboldt, A. S. Filho, L. Z. Granville, and M. Pias, "Performance analysis of 6lowpan and coap for secure

communications in smart homes," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, March 2016, pp. 1027–1034.

[83] H. Liu, C. Li, X. Jin, J. Li, Y. Zhang, and D. Gu, "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, ser. IoTS&P '17. New York, NY, USA: ACM, 2017, pp. 13–18. [Online]. Available: http://doi.acm.org/10.1145/3139937.3139948

[84] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 636–654.

[85] A. Armando, R. Carbone, E. G. Chekole, and S. Ranise, "Attribute based access control for apis in spring security," in *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 85–88. [Online]. Available: https://doi.org/10.1145/2613087.2613109

[86] M. A. Crossman and Hong Liu, "Study of authentication with IoT testbed," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, April 2015, pp. 1–7.

[87] S. A. Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Aug 2016, pp. 382–388.

[88] Y. Liu, S. Hu, and T.-Y. Ho, "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks," in *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, ser. ICCAD '14. Piscataway, NJ, USA: IEEE Press, 2014, pp. 183–190. [Online]. Available: http://dl.acm.org/citation.cfm?id=2691365.2691404

[89] Y. Liu, S. Hu, and T. Ho, "Leveraging strategic detection techniques for smart home pricing cyberattacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 220–235, March 2016.

[90] J. Roux, Alata, G. Auriol, M. Kaâniche, V. Nicomette, and R. Cayre, "RadIoT: Radio communications intrusion detection for IoT - a protocol independent approach," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, Nov 2018, pp. 1–8.

[91] J. Roux, Alata, G. Auriol, V. Nicomette, and M. Kâaniche, "Toward an intrusion detection approach for IoT based on radio communications profiling," in *2017 13th European Dependable Computing Conference (EDCC)*, Sep. 2017, pp. 147–150.

[92] B. Chatfield and R. J. Haddad, "Rssi-based spoofing detection in smart grid ieee 802.11 home area networks," in *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, April 2017, pp. 1–5.

[93] F. M. Tabrizi and K. Pattabiraman, "Intrusion detection system for embedded systems," in *Proceedings of the Doctoral Symposium of the 16th International Middleware Conference*, ser. Middleware Doct Symposium '15. New York, NY, USA: ACM, 2015, pp. 9:1–9:4. [Online]. Available: http://doi.acm.org/10.1145/2843966.2843975

[94] M. Lei, Y. Yang, N. Ma, H. Sun, C. Zhou, and M. Ma, "Dynamically enabled defense effectiveness evaluation of a home internet based on vulnerability analysis and attack layer measurement," *Personal Ubiquitous Comput.*, vol. 22, no. 1, pp. 153–162, Feb. 2018. [Online]. Available: https://doi.org/10.1007/s00779-017-1084-3

[95] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[96] "Smart Home Ecosystem: IoT and Consumers," Parks Associates and Consumer Electronics Assoiciation USA, Tech. Rep. Understanding the transformation from connected to smart home products, 2014.

[97] A. Arabo, I. Brown, and F. El-Moussa, "Privacy in the age of mobility and smart devices in smart homes," in *ASE/IEEE International Conference on Privacy, Security, Risk and Trust, and ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT*. IEEE, 2012, pp. 819–826.

[98] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, Are You Listening?" in *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, no. CSCW, 2018, pp. 1–31. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3290265.3274371

[99] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[100] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, and K. Kritikos, "Privacy attitudes and data valuation among fitness tracker users," in *International Conference on Information*. Springer, 2018, pp. 229–239.

[101] H. Nissenbaum, "A contextual approach to privacy online," *Daedalus*, vol. 140, no. 4, pp. 32–48, 2011.

[102] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *thirteenth symposium on usable privacy and security ({SOUPS} 2017)*, 2017, pp. 65–80.

[103] L. Kugler, "The war over the value of personal data," *Communications of the ACM*, vol. 61, no. 2, pp. 17–19, 2018.

[104] "Echo Dot (2nd Generation)," https://www.amazon.com/dp/B01DFKC2SO, [Accessed 12-Nov-2021].

[105] "Google Home," https://store.google.com/us/product/google_home, [Accessed 12-Nov-2021].

[106] "Wink Hub 2," https://www.wink.com/products/wink-hub-2, [Accessed 12-Nov-2021].

[107] "Insteon Hub," https://www.insteon.com/insteon-hub, [Accessed 12-Nov-2021].

[108] "The Best Smart Home Devices for 2021," https://www.pcmag.com/article2/0,2817,2410889,00.asp, [Accessed 12-Nov-2021].

[109] "Best smart home devices to buy in 2021," https://www.cnet.com/home/smart-home/best-smart-home-devices/, [Accessed 12-Nov-2021].

[110] "SmartThings hub," https://www.smartthings.com/products/smartthings-hub., [Accessed 12-Nov-2021].

[111] V. G. Motti and K. Caine, "Users' privacy concerns about wearables," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 231–244.

[112] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2017, pp. 1292–1297.

[113] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic," in *Data and Algorithmic Transparency Workshop (DAT)*, New York, 2016. [Online]. Available: http://datworkshop.org/papers/dat16-final37.pdf

[114] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 727–732.

[115] B. Fisher and S. Umarji, "Identity and access management for smart home devices," *National Cybersecurity Center of Excellence*, 2016. [Online]. Available: https://nccoe.nist.gov/sites/default/files/library/conceptpapers/idam-smart-home-concept-draft.pdf

[116] D. Gibson and A. Igonor, *Managing risk in information systems*. Jones & Bartlett Learning, 2020.

[117] N. Malkin, J. Bernd, M. Johnson, and S. Egelman, ""what can't data be used for?" privacy expectations about Smart TVs in the US," in *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK*, 2018.

[118] D. van der Linden, M. Edwards, I. Hadar, and A. Zamansky, "Pets without pets: on pet owners' under-estimation of privacy concerns in pet wearables," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, pp. 143–164, 2020.

[119] J. Bugeja, P. Davidsson, and A. Jacobsson, "Functional classification and quantitative analysis of smart connected home devices," in *2018 Global Internet of Things Summit (GIoTS)*, 2018, pp. 1–6.

[120] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang, "Privacy Perceptions and Designs of Bystanders in Smart Homes," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, nov 2019. [Online]. Available: https://doi.org/10.1145/3359161

[121] R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker you wear - a security analysis of wearable health trackers," *SAC '16 Proceedings of the 31st Annual ACM Symposium on Applied Computing*, pp. 131–136, 2016.

[122] V. G. Motti and K. Caine, "Towards a visual vocabulary for privacy concepts," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60, no. 1, pp. 1078–1082, 2016. [Online]. Available: https://doi.org/10.1177/1541931213601249

[123] X. Page, P. Bahirat, M. I. Safi, B. P. Knijnenburg, and P. Wisniewski, "The internet of what? understanding differences in perceptions and adoption for the internet of things," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–22, 2018.

[124] Y. Liao, J. Vitak, P. Kumar, M. Zimmer, and K. Kritikos, "Understanding the role of privacy and trust in intelligent personal assistant adoption," vol. 11420 LNCS, 2019, pp. 102–113.

[125] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending my castle: A co-design study of privacy mechanisms for smart homes," ser. CHI '19. New York, NY, USA: ACM, 2019, pp. 198:1—198:12.

[126] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, 11 2019.

[127] S. M. Wyatt, "Non-users also matter: The construction of users and non-users of the internet," *Now users matter: The co-construction of users and technology*, pp. 67–79, 2003.

[128] E. P. S. Baumer, J. Burrell, M. G. Ames, J. R. Brubaker, and P. Dourish, "On the importance and implications of studying technology non-use," *Interactions*, vol. 22, no. 2, p. 52–56, 2 2015.

[129] A.-M. Oostveen, "Non-use of automated border control systems: identifying reasons and solutions," in *Proceedings of the 28th International BCS Human Computer Interaction Conference (HCI 2014) 28*, 2014, pp. 228–233.

[130] C. Satchell and P. Dourish, "Beyond the user: Use and non-use in hci," in *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7*, ser. OZCHI '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 9–16. [Online]. Available: https://doi.org/10.1145/1738826.1738829

[131] C. Chhetri, "Questionnaire for non-user privacy concerns survey," Jun 2022. [Online]. Available: osf.io/tnr2z

[132] K. Baxter, C. Courage, and K. Caine, *Understanding Your Users: A Practical Guide to User Research Methods*, 2nd ed. Morgan Kaufmann, 2015.

[133] A. Mathur, N. Malkin, M. Harbach, E. Peer, and S. Egelman, "Quantifying users' beliefs about software updates," *arXiv preprint arXiv:1805.04594*, 2018.

[134] M. Williams, J. R. Nurse, and S. 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. 181–18 109.

[135] K. Olmstead, "Nearly half of americans use digital voice assistants, mostly on their smartphones," *Pew Research Center*, 2017. [Online]. Available: http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/

[136] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[137] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, 2017.

[138] Policy, R. Group *et al.*, "The internet of things: An introduction to privacy issues with a focus on the retail and home environments," *Office of the Privacy Commissioner of Canada, Feb*, 2016.

[139] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technological Forecasting and Social Change*, vol. 138, pp. 139–154, 2019.

[140] I. Worldwide, "Quarterly smart home device tracker, 29 march 2019."

[141] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[142] M. J. Kraemer and I. Flechais, "Researching privacy in smart homes: A roadmap of future directions and research methods," 2018.

[143] J. Bugeja, A. Jacobsson, and P. Davidsson, "On privacy and security challenges in smart connected homes," in *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2016, pp. 172–175.

[144] V. Nathan, S. Paul, T. Prioleau, L. Niu, B. J. Mortazavi, S. A. Cambone, A. Veeraraghavan, A. Sabharwal, and R. Jafari, "A survey on smart homes for aging in place: Toward solutions to the specific needs of the elderly," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 111–119, 2018.

[145] J. M. Batalla, A. Vasilakos, and M. Gajewski, "Secure smart homes: Opportunities and challenges," *ACM Computing Surveys (CSUR)*, vol. 50, no. 5, pp. 1–32, 2017.

[146] M. J. Kim, M. E. Cho, and H. J. Jun, "Developing design solutions for smart homes through user-centered scenarios," *Frontiers in Psychology*, vol. 11, p. 335, 2020.

[147] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy expectations and preferences in an IoT world," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 399–412.

[148] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "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*, ser. CHI '19. New York, NY, USA: ACM, 2019, pp. 198:1—-198:12. [Online]. Available: http://doi.acm.org/10.1145/3290605.3300428

[149] K. Marky, S. Prange, F. Krell, M. Mühlhäuser, and F. Alt, ""you just can't know about everything": Privacy perceptions of smart home visitors," in *19th International Conference on Mobile and Ubiquitous Multimedia*, 2020, pp. 83–95.

[150] B. K. Sovacool and D. D. F. Del Rio, "Smart home technologies in europe: A critical review of concepts, benefits, risks and policies," *Renewable and Sustainable Energy Reviews*, vol. 120, p. 109663, 2020.

[151] V. Zimmermann, P. Gerber, K. Marky, L. Böck, and F. Kirchbuchner, "Assessing users' privacy and security concerns of smart home technologies," *i-com*, vol. 18, no. 3, pp. 197–216, 2019.

[152] L. Rainie and M. Duggan, "Privacy and information sharing. pew research center (2016)."

[153] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Securing the smart home: A real case study," *Internet Technology Letters*, vol. 1, no. 3, p. e22, 2018.

[154] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments. information, 7 (3), 44," 2016.

[155] J. Chen, L. Edwards, L. Urquhart, and D. McAuley, "Who is responsible for data processing in smart homes? reconsidering joint controllership and the household exemption," *Reconsidering Joint Controllership and the Household Exemption (November 18, 2019)*, 2019.

[156] G. Birchley, R. Huxtable, M. Murtagh, R. Ter Meulen, P. Flach, and R. Gooberman-Hill, "Smart homes, private homes? an empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies," *BMC medical ethics*, vol. 18, no. 1, pp. 1–13, 2017.

[157] S. Cannizzaro, R. Procter, S. Ma, and C. Maple, "Trust in the smart home: Findings from a nationally representative survey in the UK," *Plos one*, vol. 15, no. 5, p. e0231615, 2020. [Online]. Available: https://doi.org/10.1371/journal.pone.0231615

[158] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[159] A. A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5g internet of things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, 2020.

[160] C. Fung and Y. Pillai, "A privacy-aware collaborative ddos defence network," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2020, pp. 1–5.

[161] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," *SN Applied Sciences*, vol. 2, no. 2, p. 247, 2020.

[162] C. Mao, "Privacy issues in IoT: Privacy concerns in smart home," 2019.

[163] H. Yang, W. Lee, and H. Lee, "IoT smart home adoption: the importance of proper level automation," *Journal of Sensors*, vol. 2018, pp. 1–11, 2018.

[164] E. Cho, S. S. Sundar, S. Abdullah, and N. Motalebi, "Will deleting history make alexa more trustworthy? effects of privacy and content customization on user experience of smart speakers," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–13.

[165] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, vol. 42, no. 2, pp. 60–67, 1999.

[166] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences," in *Proceedings of the 1st ACM conference on Electronic commerce*, 1999, pp. 1–8.

[167] D. J. Solove, *Understanding Privacy.* Harvard University Press, May 2008.

[168] H. Nissenbaum, *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press, 2009.

[169] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation.* Springer, 2008, pp. 1–19.

[170] S. Egelman, A. P. Felt, and D. Wagner, "Choice architecture and smartphone privacy: There'sa price for that," in *The economics of information security and privacy.* Springer, 2013, pp. 211–236.

[171] A. Frik and A. Gaudeul, "A measure of the implicit value of privacy under risk," *Journal of Consumer Marketing*, 2020.

[172] F. Bélanger and R. E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," *MIS quarterly*, pp. 1017–1041, 2011.

[173] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, pp. 477–564, 2006.

[174] G. Bleaney, M. Kuzyk, J. Man, H. Mayanloo, and H. R. Tizhoosh, "Auto-detection of safety issues in baby products," in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems.* Springer, 2018, pp. 505–516.

[175] M. Winkler, A. S. Abrahams, R. Gruss, and J. P. Ehsani, "Toy safety surveillance from online reviews," *Decision support systems*, vol. 90, pp. 23–32, 2016.

[176] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336–355, 2004.

[177] A. Jacobsson and P. Davidsson, "Towards a model of privacy and security for smart homes," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 727–732.

[178] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 5772–5781.

[179] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring How Privacy and Security Factor into IoT Device Purchase Behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: ACM, 2019, pp. 534:1—-534:12. [Online]. Available: http://doi.acm.org/10.1145/3290605.3300764

[180] S. S. Prettyman, S. Furman, M. Theofanos, and B. Stanton, "Privacy and security in the brave new world: The use of multiple mental models," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2015, pp. 260–270.

[181] J. M. Haney, S. M. Furman, and Y. Acar, "Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, A. Moallem, Ed., vol. 12210 LNCS. Cham: Springer International Publishing, 2020, pp. 393–411. [Online]. Available: https://tsapps.nist.gov/publication/get{_}pdf.cfm?pub{_}id=929479

[182] N. M. Barbosa, Z. Zhang, and Y. Wang, "Do privacy and security matter to everyone? quantifying and clustering user-centric considerations about smart home device adoption," in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Aug. 2020, pp. 417–435. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/barbosa

[183] D. Carbon and U. E. Carbon, "Ihre privacy box. mehr schutz im internet." Apr 2021. [Online]. Available: https://trutzbox.de/

[184] W. Seymour, M. J. Kraemer, R. Binns, and M. Van Kleek, "Informing the design of privacy-empowering tools for the connected home," ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–14. [Online]. Available: https://doi.org/10.1145/3313831.3376264

[185] D. Y. Huang, N. Apthorpe, F. Li, G. Acar, and N. Feamster, "IoT inspector: Crowdsourcing labeled network traffic from smart home devices at scale," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 4, no. 2, Jun. 2020. [Online]. Available: https://doi.org/10.1145/3397333

[186] M. D. Fetters, L. A. Curry, and J. W. Creswell, "Achieving integration in mixed methods designs—principles and practices," *Health services research*, vol. 48, no. 6pt2, pp. 2134–2156, 2013.

[187] B. J. Oates, *Researching information systems and computing.* Sage, 2005.

[188] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 77–101, 2006. [Online]. Available: https://www.researchgate.net/publication/235356393{_}Using{_}thematic{_}analysis{_}in{_}psychology

[189] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.

[190] G. Harboe and E. M. Huang, "Real-world affinity diagramming practices: Bridging the paper-digital gap," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 95–104.

[191] C. Chhetri and V. G. Motti, "'I mute my echo when I talk politics': Connecting smart home device users' concerns to privacy harms taxonomy," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 66, no. 1, pp. 2083–2087, 2022. [Online]. Available: https://doi.org/10.1177/1071181322661114

[192] ——, "Dataset: Privacy controls needs of smart home device users," Aug 2022. [Online]. Available: https://doi.org/10.17605/OSF.IO/8CXS4

[193] J. Tang, E. Birrell, and A. Lerner, "How well do my results generalize now? the external validity of online privacy and security surveys," *arXiv preprint arXiv:2202.14036*, 2022.

[194] B. Auxier, "5 things to know about americans and their smart speakers," *Pew Research Center. Retrieved from https://pewrsr.ch/2pDPSDX*, 2019.

[195] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951.

[196] J. A. Gliem and R. R. Gliem, "Calculating, interpreting, and reporting cronbach's alpha reliability coefficient for likert-type scales." Midwest Research-to-Practice Conference in Adult, Continuing, and Community ..., 2003.

[197] A. Cavoukian *et al.*, "Privacy by design: The 7 foundational principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, p. 12, 2009.

[198] J. Nielsen, "Ten usability heuristics," 2005.

[199] D. J. Solove, "Introduction: Privacy self-management and the consent dilemma," *Harvard Law Review*, vol. 126, p. 1880, 2012.

[200] E. A. Vogels, "Millennials stand out for their technology use, but older generations also embrace digital life," *Pew Research Center*, vol. 9, 2019.

[201] M. Blythe and A. Monk, "Notes towards an ethnography of domestic technology," in *Proceedings of the 4th conference on Designing interactive systems: processes, practices, methods, and techniques*, 2002, pp. 277–281.

[202] R. Kang, S. Brown, L. Dabbish, and S. Kiesler, "Privacy attitudes of mechanical turk workers and the us public," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 37–49.

[203] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[204] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?" in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 447–464.

[205] Y. Feng, Y. Yao, and N. Sadeh, "A design space for privacy choices: Towards meaningful privacy control in the internet of things," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445148

[206] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, ser. SOUPS '09. New York, NY, USA: Association for Computing Machinery, 2009. [Online]. Available: https://doi.org/10.1145/1572532.1572538

[207] A. Railean and D. Reinhardt, "Onlite: on-line label for IoT transparency enhancement," in *Nordic Conference on Secure IT Systems*. Springer, 2020, pp. 229–245.

[208] Y. Shen and P.-A. Vervier, "IoT security and privacy labels," in *Annual Privacy Forum*. Springer, 2019, pp. 136–147.

[209] P. Murmann and F. Karegar, "From design requirements to effective privacy notifications: empowering users of online services to make informed decisions," *International Journal of Human–Computer Interaction*, vol. 37, no. 19, pp. 1823–1848, 2021.

[210] C. Chhetri, "Study protocols for evaluation of MyCam app," Jun 2022. [Online]. Available: osf.io/zfvmx

[211] M. Schrepp, A. Hinderks, and J. Thomaschewski, "Design and evaluation of a short version of the user experience questionnaire (ueq-s)," *International Journal of Interactive Multimedia and Artificial Intelligence, 4 (6), 103-108.*, 2017.

[212] J. Brooke, "Sus: a "quick and dirty'usability," *Usability evaluation in industry*, vol. 189, no. 3, 1996.

[213] P. Seddon and M.-Y. Kiew, "A partial test and development of delone and mclean's model of is success," *Australasian Journal of Information Systems*, vol. 4, no. 1, pp. 90–109, 1996.

[214] H. Xu, "The effects of self-construal and perceived control on privacy concerns," 2007.

[215] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly*, vol. 27, no. 3, pp. 425–478, 2003.

[216] J. R. Lewis, "The system usability scale: past, present, and future," *International Journal of Human–Computer Interaction*, vol. 34, no. 7, pp. 577–590, 2018.

[217] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, pp. 166–170, 1968.

[218] Joint Task Force and Transformation Initiative, "Security and privacy controls for federal information systems and organizations," *NIST Special Publication*, vol. 800, no. 53, pp. 8–13, 2013.

Biography

Chola Chhetri graduated from New Horizons High School in 1996. He received his BA from Tribhuvan University in 2003. He received an MS in Computer Science from Sikkim Manipal University in 2005. He received another MS in Information Security and Assurance from George Mason University in 2011.