# “It did not give me an option to decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products

George Chalhoub
Department of Computer Science
University of Oxford
george.chalhoub@cs.ox.ac.uk

Martin J. Kraemer
Department of Computer Science
University of Oxford
martin.kraemer@cs.ox.ac.uk

Norbert Nthala
Department of Media and Information
Michigan State University
nthalano@msu.edu

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

**Figure 1: Smart products deployed in household four. Images from left to right: (a) Arlo Pro security camera at the front entry door, (b) Arlo Pro security camera in the bedroom, (c) Philips Hue light bulb in the bedroom, (d) Amazon Echo smart speaker in the bedroom, (e) Google Home smart speaker in the bedroom and (f) Amazon Echo Show smart display in the bathroom.**

## ABSTRACT

Smart home products aren’t living up to their promise. They claim to transform the way we live, providing convenience, energy efficiency, and safety. However, the reality is significantly less profound and often frustrating. This is particularly apparent in security and privacy experiences: powerlessness, confusion, and annoyance have all been reported.

In order to reduce frustration and help fulfill the promise of smart homes, we need to explore the experience of security and privacy in situ. We analyze an ethnographic study observing six UK households over six months to present a longitudinal view of security and privacy user experiences in smart products. We find inconsistencies in managing security and privacy, e.g., contrasting the ease of granting and difficulty of withholding consent. We identify security and privacy issues in repurposing smart home devices – using devices outside of their initial intended purposes. We conclude with recommendations for design in smart home devices.

## CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; *Empirical studies in ubiquitous and mobile computing*; • **Security and privacy** → Usability in security and privacy.

## KEYWORDS

user experience; security; privacy; smart home; longitudinal study; qualitative study

**ACM Reference Format:**
George Chalhoub, Martin J. Kraemer, Norbert Nthala, and Ivan Flechais. 2021. “It did not give me an option to decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *CHI Conference on Human Factors in Computing Systems (CHI ’21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3411764.3445691


*CHI ’21, May 8–13, 2021, Yokohama, Japan*

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445691

# 1 INTRODUCTION

Smart homes are routinely marketed as the future: making life easier, better, faster and cheaper. They promise to provide convenience and give users control over items and events in their homes – whether at home or not – as well as providing comfort and energy efficiency (e.g., sensing temperature and automating air conditioning or heating) [47]. However, commercial smart home platforms are also seen as having a more pernicious side, which conjures up images of surveillance cameras and smart speakers that are constantly tracking, watching, listening, and monitoring.

Previous studies have emphasized the need for research to improve the User eXperience (UX) of smart home products. The international standard of human-system interaction (ISO 9241-210) defines UX [29] as "*a person's perceptions and responses that result from the use or anticipated use of a product, system or service.*" The UX of smart home products extends beyond the use of day-to-day services into the experience of security and privacy. Research has uncovered a number of negative security and privacy experiences: powerlessness, confusion, frustration, disappointment and annoyance [93]. Shortfalls have also been identified in UX design of security and privacy in smart cameras [13].

Prior research on the UX of smart home technology has been conducted in laboratories [46, 51], or with prototypes in experimental settings [40, 55]. Smart home security and privacy interactions have been studied using surveys (e.g., [62]), in-situ design evaluation (e.g., [93]), focus groups and interviews (e.g., [20, 92]). Despite calls from researchers to provide insights into the lived experience of smart home security and privacy (e.g., [48, 61]); to our knowledge, *no in-depth and longitudinal studies* have been conducted on the *user experience of security and privacy in smart homes.*

Our research aims to study the longitudinal aspects of security and privacy user experiences among households in the context of real, deployed smart homes. Our overarching research question is **RQ:** How can security and privacy experiences in smart homes be understood and well supported? We break this down into two further questions: (i) **RQ1:** What is the security and privacy user experience over time in smart homes? Based on this, (ii) **RQ2:** How can designers and developers improve security and privacy User eXperience design in smart home products?

In order to answer these questions, we analyzed an extensive body of data that was collected as part of a separate ethnographic study into the communal use of smart technology in the home. This body of data provided a detailed, ethnographic observation of the experience of 22 participants in six households installing and using smart devices (e.g., cameras, doorbells, voice assistants, lights and heating) over a period of six months. The data consisted of a combination of unstructured interviews, fieldnotes, photographs, and diaries. We conduct a systematic thematic analysis of this data to identify factors pertaining to security and privacy user experiences. We summarize our key findings below:

- Both privacy and security concerns arose from mass media and online sources (e.g., hearing about breaches); however, privacy concerns also arose from device use and features (e.g., feeling that a camera is intrusive).
- Protecting personal data consisted of a mix of workarounds (e.g., covering camera lens with a sticker) and using designed controls; however, security involved only designed controls use (e.g., password, account management).
- Usability issues in privacy and security designed controls were observed: consenting to data collection and use was easy, but difficult to withhold or revoke; and access management was poorly suited to the needs of the household, which resulted in account sharing rather than permission delegation.
- Some participants repurposed (i.e., adapted for use in a different purpose) smart home devices for parenting and entertainment, resulting in several security and privacy implications arising from these new applications.

The rest of the paper is organized as follows: we discuss related work in Section 2; we describe the methodology followed in this study in Section 3; in Section 4, we present the findings of our study; we discuss the findings in Section 5; we conclude the paper and present our design recommendations in Section 6.

# 2 RELATED WORK

"Smart homes" refer to homes which contain connected devices providing users with automated context-aware services such as home automation, remote home control or ambient intelligence (e.g., smart speakers and cameras) [2]. Smart homes are part of Internet of Things (IoT) devices, which encompass interrelated communicating devices and sensors.

## 2.1 User Experience in smart homes

Several studies [11, 37, 88, 89] have investigated smart homes, interviewing households to provide directions for future research and to improve UX. More research [17, 38, 39, 68, 72, 78] has explored how users configure, manage, or live with their home networks, and also how they manage access control for sharing data and devices [52, 58]. Zeng et al. [92] interviewed smart home users and found that their understanding depends on the sophistication of their mental models, motivating continued research into user experiences. Chetty et al. [17] studied networked homes to understand the relationships between households, their inhabitants, and networks. In other work, Yang and Newman [90] investigated experiences of thermostats, highlighting the importance of understanding user values and behaviors.

Previous research on smart homes has been conducted in laboratories [46, 51], or with prototypes in experimental settings [40, 55]. Randall et al. [69], researched users living in smart homes and found that control is a social-technical matter. Jakobi et al. [47] studied the issues faced by users adopting smart homes in a living lab. Jakobi et al. [48] also reported a design case study with 12 households and found that users' accountability needs changed over time. Brush et al. [11] found that manageability and unreliable behavior were

major concerns for smart home users. Mennicken and Huang [61] explored smart home interactions through an "*in the wild*" qualitative study. They report on the need for more research exploring the use and adoption of technology-equipped smart homes in the context of everyday life.

## 2.2 Security and Privacy in smart homes

We refer to user privacy as "*control over personal information*" [74] and this has been a focus in the design of smart homes [8, 43, 44, 67]. Several studies have explored users' needs, perceptions, and concerns in relation to smart home surveillance (e.g., data collection, use, and sharing) [18, 19, 85–87] and security and privacy [1, 4, 36, 64, 92–94].

*2.2.1 Conflicts and tensions within households.* Personal data monitoring raised concerns among households prior to the introduction of contemporary smart home devices [16]. Unlike earlier home devices, smart homes often do not have screens and have more constrained visualizations [47, 50]. Smart homes have been a source of conflict and tensions among households, due to misuse (e.g., abuse) and conflicts. Conflicts can arise due to differences in opinion on thermostat settings [36, 92], tensions between parents and teens over entryway surveillance [82], or due to the use of recorded evidence in household disputes [19]. For example, Choe et al. [19] explored what affects people's perceptions of smart homes, and found tensions among households in managing recordings. Choe et al. [18] also looked into house activity that people would not want recorded. Zeng et al. [92] found that users felt a loss of privacy because others could view their activity through logs. Tensions about parents and children with respect to monitoring and privacy have been explored [24, 82]; prior work has also researched concerns of older generations [28, 79].

The different levels of skills and ability among households have been a common issue in prior work [12, 36, 61]. Bell et al. called for research exploring how smart homes reproduce existing power concentrations in relationships [7]. Mennicken et al. [61] and Zeng et al. [92] found that there is a need to assist passive smart home users. Geeng and Roesner [36] found that tech-savvy active users have more access and agency over device functionality. We aim to expand on these findings by including experiences of all household members, including passive users.

*2.2.2 Security and privacy concerns towards external parties.* Earlier work has researched smart home security and privacy from external parties such as manufacturers, advertisers, and law enforcement [5, 35, 62, 66, 92, 94]. According to Cranor et al. [21], smart home data can be exploited and used for purposes such as legal proceedings, insurance decisions, unwanted advertising, and crime. Apthorpe et al. [5] surveyed smart home users to measure the acceptability of third-party data sharing, and provided insights into existing privacy norms. Malkin et al. [56] found that smart speaker users were protective of the audio command history of children and guests, and strongly opposed third-party tracking. Hoyle et al. explored how people manage privacy in the context of lifelogging cameras [44]. Egelman et al. [34] used crowdsourcing to study privacy camera icons, with the aim of helping users make privacy decisions. Abdi et al. [1] interviewed smart assistant users and found that they had limited understanding of data storage and sharing. Emami-Naeini et al. [62] investigated smart home privacy preferences, and found that users were more likely to consent to providing data for uses they perceived as beneficial. Wash and Rader [84] argue that measuring security and privacy behavior with qualitative and quantitative tools is challenging because security decisions depend on the contextual factors [31] and self-reported behavior has limitations such as social desirability bias [70] and imperfect recall [3]. We attempt to address this shortcoming by analyzing an ethnographic dataset which includes participant observation in addition to interviews and diaries.

*2.2.3 Smart home access controls.* Earlier research in access control in homes initially looked at file storage (e.g., mobile phones) [58, 59] before considering access control for smart home users [81]. Mazurek et al .[58] studied access control for home data sharing, providing guidelines for usable access-control systems. He et al. [41] researched smart home access control preferences and found that users would prefer access control per-feature rather than per-device. Mare et al. found that adoption of access control policies is uneven and limited [57]. He et al. [41] and Ur et al. [81] both reported different access control and authentication policies among devices (i.e., smart locks had access controls but smart thermostats had none). In more recent work, Zeng and Roesner [93] evaluated multi-user smart home access control designs in seven households and provided design guidelines. We expand on their findings by exploring access control experiences resulting from various devices, including more invasive devices (e.g., smart cameras).

## 2.3 Summary

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

# 3 METHODS

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

(1) planning workshops with participants where they selected smart home products for their home.
(2) procuring and providing the chosen smart home products to participants.

(3) observing the deployment, installation and use.
We carried out a secondary analysis of data collected between August 2019 and May 2020 which consisted of fieldnotes, photographs, unstructured interviews, and diaries. We chose to perform a secondary analysis of this data as (i) it is highly relevant to our research question, it contains very detailed information pertaining to both (ii) an elusive research population (parents and children), and (iii) to a sensitive topic (security and privacy), and finally (iv) two of the authors were directly involved in the primary study and thus already familiar with the data.

## 3.1 Secondary Analysis

Secondary analysis is a systematic method with procedural and evaluative steps for using existing data to address research questions different from ones used in original research [22, 42]. The secondary analysis we conducted followed the approach described by Johnston [49] which consists of forming the research questions, and identifying, evaluating, and then analyzing appropriate datasets.

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

*3.1.2 Identifying the Dataset.* To identify a suitable dataset to answer our research question, we reviewed both past and currently available research in the field of usable security and privacy in smart homes. We selected the 'Informing the Future of Data Protection by Design and by Default' dataset on the basis of its suitability and familiarity. From a suitability perspective, our research question fits very well with the purpose of the original study since both studies focused on smart home product use. We found the ethnographic dataset suitable for carrying out multiple interpretations and investigating different phenomena. Moreover, ethnography's approach of observing people and cultural groups is highly suitable for researching UX [9]. On a more practical note, several investigators from the primary study were available to provide detailed insights and contribute to the secondary analysis, which has proven to be instrumental in ensuring the secondary analysis remains faithful to the data.

*3.1.3 Evaluating the Dataset.* We evaluated the data of the primary study to ensure its appropriateness and quality in advance of actual use. We were given access to and utilized all documentation on the collection of the data, and consulted and involved investigators from the primary ethnographic study in order to complete this evaluation. We used Stewart and Kamins' [76] reflective approach to evaluate the data in a "*stepwise fashion*". The approach consisted of evaluative steps (e.g., [22, 25, 30]) to ensure congruency, quality of the primary study and the resulting dataset. The steps taken were determining (a) the purpose of the study; (b) the entities responsible for data collection; (c) what, when and how the information was obtained; and (d) the consistency of the information obtained.

*3.1.4 Analyzing the Data.* The dataset consisted of diaries, fieldnotes and interviews which had been audio recorded and professionally transcribed. We coded this data using iterative open coding [83] in accordance with Braun and Clark's thematic analysis [10]. Authors 1 and 2 both coded the data: author 1 was not part of the data collection; however, author 2 was the investigator that collected the data in the original study. Throughout the coding process, author 1 was able to ask for clarifications and additional insights while author 2 annotated the study data to provide additional context. Both coded the data focusing on home practices and experiences and developed an initial codebook.

To verify the credibility of our codebook, author 3 cross-checked the codes against the interview transcripts. At the same time, author 4 reviewed the initial codes and supporting quotes. All researchers discussed any differences and generated a final codebook. We tested for inter-rater reliability. The average Cohen's kappa coefficient ($\kappa$) for all codes in our data was 0.84. Cohen's kappa values over 0.80 indicate almost perfect agreement [60]. Further, we explored the codes to focus on evolving security and privacy experiences over time, and clustered relevant codes into themes.

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

## 3.2 Data Source

We describe in more detail the data provided by the 'Informing the Future of Data Protection by Design and by Default' project. The study researched communal use of smart technology in the home and used an ethnographic approach to observe six households setting up and using smart home devices over time. Materials from the study can be found at https://osf.io/9ztk2/.

*3.2.1 Description.* The data was collected in four different phases (see Figure 2): planning (week 0-4), deployment (week 4-12), problem solving (week 12-20) and reflection (week 20-26). We describe three phases below.

*Planning:* Participants were visited by author 2 who learned about their practices and conducted a planning workshop for selecting products. They were asked to sketch their floor plan and were provided with a budget and a card deck designed for the study which contained descriptions of different products (e.g., cost, compatibility and functionalities). Participants placed cards into their drawing based on available budget, household need and perceived benefits.

*Deployment:* Based on their choices in the planning phase, smart home products were then provided to households who installed, explored, and started to form routines. During the setup and installation phase, households negotiated occupant needs, device placement, configuration and usage. The researcher did not interfere in the setup phase except when asked to help. Households were

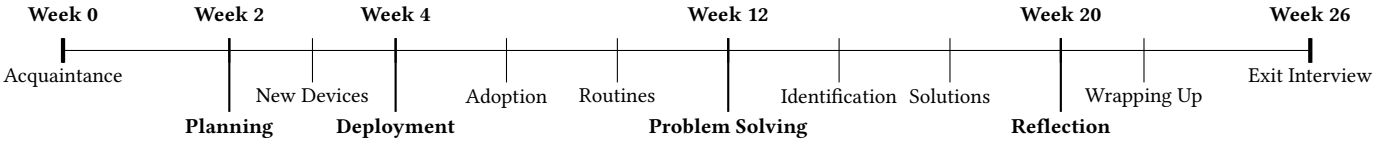


**Figure 2: Timeline of different phases of data collection**

then visited every two to four weeks over then next four months where informal and unstructured interviews were conducted.

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

*3.2.2 Recruitment.* To recruit participants, the study was advertised on social media and online platforms. Interested participants were asked to complete an online screening questionnaire. The study aimed to recruit demographically-diverse dual-income families that are in favor of technology adoption [27]. Hence, demographic questions about gender, age, educational level, employment status and household income were included. Additionally, participants were asked to specify the smart products they own and use, or intend to purchase. They were also asked to describe their existing knowledge of smart products, and their interest behind wanting to participate.

Different levels of technical competence were defined (Novice, Competent, Expert) using a simplified Dreyfus model of skill acquisition [32]. Dreyfus' model has been widely used to define levels for assessing one's competence. Participants were asked to report their own and their household members' skill level using the recruitment questionnaire. Our recruitment questionnaire form can be found at https://osf.io/9ztk2/.

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

*Unstructured group interviews:* Observing households in real-life settings is difficult [77]. Instead, unstructured group interviews were conducted during all visits. Such interviews enable conversational groups within households which allows observation of open and unfettered discussions [77]. Interviews depended on the availability of household members and took place in communal living spaces. Interview prompts were based on information from diaries and previous visits. They focused on eliciting information about experiences and practices. Interviews conducted after March 2020 were moved online due to the COVID-19 lockdown.

*Researcher fieldnotes:* To gain insight into cultural practices and phenomena, descriptive and reflective field notes [53] were collected in line with Yin's best practices for recording qualitative field notes [91]. Descriptive field notes consisted of time and date, present family members, their conduct, remarkable interactions, and a general reflection on the home visit. Reflective information consisted of the researcher's reflections about the observation being conducted and included ideas, questions, concerns, and related thoughts.

*Participant diaries:* To gain longer and regular insight into lived experiences, diaries were provided to participants who were encouraged to report their experiences regularly. A diary study template was used that listed an example entry, the project aims, list of questions and minimum entry expectations (e.g., at least two entries per week). Questions asked about instances of shared use, comments on interactions with new devices, likes/dislikes, and positive/negative experiences. Diary options offered were both paper-based and digital. Diaries used can be found at https://osf.io/9ztk2/.

## 3.3 Participant Demographics

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

## 3.4 Research Ethics

The University of Oxford Central University Research Ethics Committee (CUREC) reviewed and approved our study who determined that the secondary analysis was consistent with the consent given by participants in the original study (R59140/RE001) and did not require additional consent. Participants in the original study read an information sheet that explained the high-level purpose of the research and outlined data-protection practices. They were asked to sign a consent form that presented all the information required in Article 14 of the EU General Data Protection Regulation (GDPR). Households had the option to withdraw from the study without providing an explanation. They kept the smart home products provided to them; and no data was accessed from these products. Each household was compensated with £200.

## 3.5 Limitations

First, a major limitation inherent in the nature of secondary data analysis is that the data used was not collected to address our research questions [30, 76]. To address this limitation, we followed a process of careful reflective examination and critical evaluation

**Table 1: Participant Demographics**

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

of the data to ensure a match between our research questions and the existing data.

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

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

## 4 RESULTS

In this section, we present our findings. We discuss our key themes: the experience of privacy (Section 4.1), the experience of security (Section 4.2) and technology repurposing (Section 4.3);

### 4.1 The Experience of Privacy

We use the term '*experience of privacy*' to refer to a person's privacy-related perceptions and responses that result from the use or anticipated use of a product, system or service. Participants' privacy experiences consisted of *feelings of intrusiveness* (Section 4.1.1), *tracking concerns* (Section 4.1.2), and *privacy management* (Section 4.1.3).

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

**Cameras:** Participants (n=10) expressed concerns over security cameras (e.g., Arlo Pro) and smart display cameras (e.g., Echo Show 5). In H1, Jaco H1b and Iria H1c were concerned after discovering a camera in an Echo Show 5; but they were reassured by Rosa H1a who said that the camera can be muted anytime. In H4, Carla H4a and Aaron H4b installed smart displays in different rooms in the house to increase utility and connectivity. However, they were worried about the ones placed in sensitive locations (e.g., bedroom, bathroom). Aaron H4b stated it was '*unethical*' to add cameras in children's bedrooms. He explained: "*You realize that some people literally have one of those in their children's bedrooms watching their children sleep, you know. [...] That is really creepy.*" However, Aaron H4b placed an Arlo Pro security camera at the front entrance door because he did not consider it to be a private space (see Figure 1a).

**Microphones:** Participants (n=3) expressed privacy concerns over microphones found in smart speakers (e.g., Amazon Echo, Google Home) and displays (e.g., Echo Show 5) due to their *always-listening* capabilities. In H1, Iria H1c explained that she mutes her Echo Show during sleep: "*I put it on the 'do not disturb' one so when you press it, the red light comes on. And I do not know, it could still be listening.*" In H3, Carrie H3a was worried the device would listen to her conversations. She wrote in her diary: "*I also wondered how much of what I was saying was being captured and passed on,*

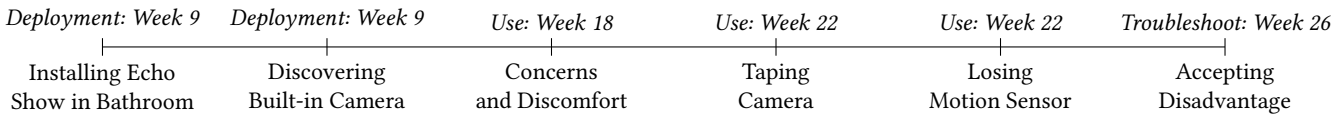


**Figure 3: Timeline illustrating H4's privacy experiences with the Echo Show 5 over time**

*including things I wasn't saying to the Google Home.*" In H2, Adam H2b was initially '*scared*' of using Google Home speakers but later '*felt comfortable*' because he '*had the control to stop it*' through the physical-mute button.

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

*4.1.3 Management of Privacy.* We describe how privacy experiences were managed below:

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

**Awareness:** Awareness refers to a user's attention and cognition in relation to the control, use, and disclosure of personal data. Participants (n=9) developed privacy awareness through learning (i) how their personal data is processed and used, and (ii) which personal information is received by companies (e.g., home presence, activities). In H4, Aaron H4b enabled the '*Follow-Up Mode*' feature on Amazon Alexa which allows for successive requests without repeating the wake word; but he was worried about recordings of his private conversations (see Figure 1d). He said: "*The issue with this is that more of our private conversations have the potential to be recorded.*" In H2, Adam H2b was concerned that his Google Home data would be '*mined*' and '*exploited*' for the provision of free services (e.g., Google Assistant).

**Decision making:** Decision making refers to a user's process of making privacy-related decisions. Participants (n=8) made decisions based on weighing risks and benefits. In H4, Carla H4a and Aaron H4b believed that providing personal data (e.g., home footage) to the Arlo Pro security camera was required to receive useful and personalized services (see Figure 1b). Carla H4a said: "*If you want to give people good services and personalization, you need their data.*" In H3, Carrie H3a was prompted to provide her home address to the Google Home during setup to be able to query for local places, weather, and time. Unwilling to provide her home address, Carrie H3a provided the address of a nearby street instead; which protected her address without hindering the ability to query for local information.

**Action:** Action refers to the privacy behavior and attitude of users. Participants' (n=12) action consisted of (i) using physical privacy controls and (ii) managing personal information. Physical privacy controls strongly alleviated concerns of monitoring, listening and tracking. In H4, the camera of an Amazon Echo Show 5 placed in the bathroom created privacy concerns (see Figure 1f). Aaron H4b enabled the built-in camera shutter which provided assurance. He explained: "*It physically puts something in front of it, so actually it is perfectly safe to have it in a bathroom*" (see Figure 3). In H3, Carrie H3a covered the camera of the Google Hub Max with a sticker. Moreover, personal data (e.g., audio logs, video footage) collected by smart products were reviewed and often deleted. In H4, Aaron H4b reviewed the audio history stored by Alexa's mobile application and configured his audio history to be periodically deleted.

*4.1.3.2 Management of Consent.* Privacy concerns were managed through consent preferences (e.g., privacy permissions). Consent management was inconsistent: *granting consent* (e.g., H1) was straightforward, but *withholding consent* (e.g., H3, H4) caused detriment and prompted reconfiguration of consent preferences (see Figure 4).

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

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

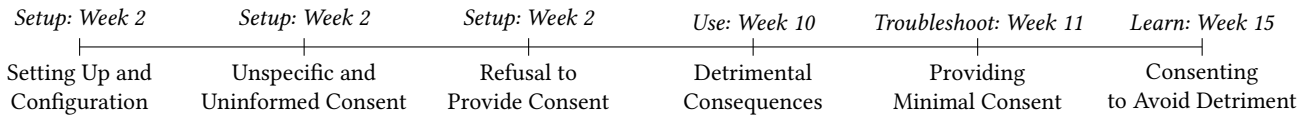


**Figure 4: Timeline illustrating H3's consent experiences with the Google Home over time**

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

**Detriment from withholding consent:** Participants (n=2) faced problems from withholding consent. Some were unable to set up products or use certain features. In H3, Carrie H3a was unable to set up her Google Home because it required '*location services*' on her Android phone to be enabled; a location tracking feature that Carrie H3a refused to activate. She said: "*I do not really want somebody following me around where I am going all the time.*' Moreover, Carrie H3a refused to enable '*Web & Activity*' tracking when setting up a Google Nest Mini. As a result, she was unable to play music on the device as streaming required '*Web & Activity*' tracking to be activated [33]. In H4, Aaron H4b obscured the camera of the Echo Show (see Figure 3) using a built-in physical shutter. However, Aaron H4b lost access to the device's motion detector, which used the camera to function to wake up the device when someone was in range.

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

## 4.2 The Experience of Security

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

*4.2.1 Security Experiences.* We report observed security experiences below:

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

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

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

**Security threats:** Security threats refer to potential violations of security vulnerabilities that result in unwanted impact, such as harm or theft of sensitive data. Participants (n=6) learned about security threats from external sources (e.g., forums, news). In H2, Adam H2b learned from a forum about potential security threats associated with Arlo security cameras. He also discovered ways

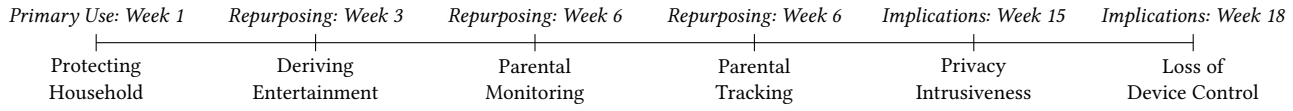


**Figure 5: Timeline illustrating H1's repurposed use of the Arlo Pro security camera over time**

that landlords had exploited smart controls associated with smart heating systems. In H6, Tobias H6a read online about news articles describing Ring security cameras as vulnerable and discussed his concerns: '*I don't know if you saw on the news that these things were all hackable?*' In H2, Rosa H1a learned from mumsnet, a forum website, that cyber criminals could turn an Amazon Echo into an eavesdropping microphone.

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

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

**Password creation:** Participants were prompted to create passwords during the registration process (see Section 4.2.1). Participants (n=2) found some password policies to be complicated and confusing. In H3, Felicity H3c was confused with password instructions prompting her to create a "*strong*" password without offering password complexity guidance and recommendations. Felicity H3c said: "*I wonder what a strong password is. [...] How do you make a strong password?*" Further, in H4, Carla H4a was confused when prompted to create a new password when setting up an Amazon Echo device. She was unsure whether her existing password from her Amazon account would work.

**Password storage:** Participants (n=3) used password managers and physical notebooks to store a large number of distinct and complex passwords. Different password managers were incompatible among products and caused inconsistent password synchronization. For instance, in H6, smart home products produced by different manufacturers (Amazon and Apple) prompted Tobias T6a to use two password managers: 1Password and Apple's Keychain Access. However, the password managers were incompatible causing frustration when Tobias T6a tried to authenticate to a Ring device. Tobias H6a explained: "*I think it [1Password] conflicts with the in-built password manager, so even though having a password manager, signing up to something like Philips, or whatever it may be [...], it is trumped by Apple's own one. So you have to hit 'No', and then every time you use 1Password to auto-fill it asks whether you want to update the in-built one.*" In H1, Rosa H1a and Jaco H1b stored their passwords on a physical notebook. Rosa H1a did not trust the security of password managers while Jaco H1b found the approach handy when passwords could not be remembered.

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

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

## 4.3 The Experience of Technology Repurposing

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

*4.3.1 Repurposing Uses.* We report the repurposing uses for parenting and entertainment (see Figure 5 and Table 2).

**Parenting:** Some products brought for entertainment and home security were repurposed for parenting. Participants (n=6) used smart home products to monitor and track minors' online and offline activities. In H1, Jaco H1b and Rosa H1a used the footage recorded by security cameras to monitor their children's activities. Jaco H1b told Iria H1c that he is constantly worried about her safety. In H4, Carla H4a used smart lights to track her children.

She wrote in her diary: "*[The lamp] seems to be up and working again. I'm definitely relying on it to track the kids.*" In H4, Aaron H4b changed the wake word from '*Alexa*' to '*Computer*' to control Malte H4c's use of the Echo device. In H3, Carrie H3a expressed concerns over Felicity H3c's access to the Google Home after the device told her: '*Your friendship keeps me warm*'. Carrie found Google Home's response to her daughter Felicity H3c inappropriate. As a result, she was concerned about her daughter's safety.

**Entertainment:** Participants (n=4) used smart cameras to derive entertainment from recorded footage. In H4, households used smart cameras as a means of '*nature spotting*'. Aaron H4b pointed his Arlo Pro camera at a birdhouse to record baby birds (see Figure 1b). In H1, households regularly reviewed camera footage to watch and share memorable moments and family activities. Rosa H1a shared interesting moments with other household members while Jaco H1b monitored the footage for entertainment. He said: "*I was excited to see what's going on and who's going to come [...] And I was seeing some cars and catching some cars, and then I just started inside the house, and they [children] just leave home to go school. I really cheer for that. It's really good stuff.*"

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

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

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

# 5 DISCUSSION

## 5.1 Privacy Design

*5.1.1 Intrusiveness and tracking:* Our findings on user concerns with intrusiveness and tracking confirm previous research by Nguyen et al. [63] who found that smart home users feel *too watched* (for camera-enabled devices) or *too listened to* (for voice-enabled devices). While most of the experiences from our participants revolve around data directly collected by the devices, data inferred from those collected by the devices can be even more intrusive [65]. For instance, continuous recording and retention of data can be used to infer physical information about the user's home (e.g., location data), and behavioral patterns in the home (e.g., when people wake up, take a shower, leave for work, return from work, go to bed, receive visitors, who the visitors were, and many more). Companies are not mandated to reveal what inferences they make from the data and for what purposes. Without such details, it is hard for users to know the kinds of inferences that will or can be made and to negotiate allowable use. Users are left to speculate about this (e.g., Carrie H3a speculated that Bluetooth can be used by manufacturers to locate her, hence she turned it off).

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

*5.1.2 Consent management:* Our results also highlight the importance of improving the design of consent management. They reveal that the life cycle of consent can change over time (see Figure 4): users can withhold - grant - revoke - amend consent as they see fit at different times of product use and for different reasons and purposes (e.g., Carrie H3a temporarily granted access to her location). User needs are usually not static and final; an unwanted service today can become critical tomorrow. The dimension of time should be explicitly designed for privacy consent management and allow users to revisit granted permissions (e.g., breach notifications can invite users to revisit their privacy settings).

Withholding consent can be an unpleasant experience, particularly in cases where users are given options to either grant consent wholesale or be denied services; or be allowed to withhold consent,

**Table 2: Examples of repurposed uses and implications for each household**

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

but have broken features in a device/service. For example, Carrie H3a could not play music on her Google Home because she withheld consent to '*Web & Activity*' tracking: a feature that collects queries and device activity across Google apps and services. As such, Carrie H3a perceived the option to consent to '*Web & Activity*' tracking as a false choice. Consent options should give users genuine choice and control; data protection regulation asserts that consent should not be bundled up as a condition of service unless it is necessary [45]. Google Home users have reported that '*Web & Activity*' tracking must be enabled to stream music on the device [73]. It was not clear to Carrie H3a why tracking was necessary for streaming, and moreover this was neither explained upfront in the consent interface nor was the failure to stream music clearly explained as consequence of withholding consent in the Google Home.

Finally, consent management is perceived to be highly unforgiving and not a safe space in which to make mistakes. In H6, Tobias H6a synced his contacts with his Echo device; but regretted his decision. He believed his action could not be undone since Amazon had already received all his contact details, and that this was irrevocable. This is fundamentally tied to the question of what happens to data that was collected when users agreed by mistake, and whether there are options for deleting this retrospectively. While the right to erasure is covered by data protection regulation [80], the process is typically cumbersome and detached from the consent management process. One recommendation would be to offer a time-limited window following consent being granted during which data that has been collected by mistake is automatically erased should the consent be revoked or amended. This approach would help to provide more forgiveness in the case of mistakenly granting consent to data use.

## 5.2 Security Design

*5.2.1 Password fatigue:* Our results confirm the continued existence of a well-known problem: password fatigue (e.g., Rosa H1a writing her passwords on a notebook). This results in poorly chosen and excessive reuse of passwords, thereby weakening the security of the protected services [26]. Given the current proliferation of smart home devices (e.g., each requiring a username and password), there are higher chances that passwords will be reused on devices and services on the home network; hence compromising one account exposes other accounts. Password fatigue may also encourage users to use insecure passwords that can be cracked.

*5.2.2 Authorization:* We also show that authorization mechanisms (e.g., family sharing features) were not user-friendly and often not used. Some households (e.g., H3) were not aware of multi-user features (e.g., family sharing); while other households (e.g., H1) tried them but found them unsuitable. In H1, Rosa H1a and Iria H1c found that using two Amazon accounts on an Echo was inconvenient (e.g., Amazon Music did not work and required another subscription). Households that used multi-user features found difficulties in configuring them (e.g., H2 and H4 struggled to set up sharing on Amazon Household and Arlo Video Doorbell). Prior work has also shown that sharing smart home products with others can be troublesome [15]. A team from CNET Smart Home that performed extensive testing on smart home devices described the process of setting up multiple devices and users as '*anything but simple*' and '*smart home from hell*' [23].

More work needs to be done to streamline the setup and management processes of authorization methods to fit the context, communal implications, and competence levels available in the home. One specific area of concern is that product manufacturers (e.g., Apple, Amazon, Google) have different rules and procedures for multi-user features which can cause confusion. For instance, Apple's HomeKit does not permit owners to selectively share devices with family members whereas Amazon Household does [14].

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

## 5.3 Designing for Technology Repurposing and Misuse

*5.3.1 Technology repurposing:* Our results indicate that smart home products were repurposed in five households. Smart home cameras that were originally intended to protect the household from

burglary and vandalism were repurposed for parenting and entertainment. Conversely, smart lights that were originally intended for lighting control were used as a deterrent against burglary (e.g., making the house appear to be occupied while inhabitants were away).

Smart lights have been previously susceptible to numerous attacks. For instance, an attack was able to remotely leak data from smart lights from a distance of 100 meters using cheap and readily available equipment [71]. In contrast, the intrusive nature of smart cameras can make them susceptible to misuse and even abuse. Researchers have argued that smart home cameras can be exploited and facilitate domestic abuse by controlling and monitoring victims [54, 93]. In response to these on-going threats, smart home manufacturers (e.g., Google) have introduced large counter-abuse teams. Those teams are often reactive, relying largely on users to report misbehavior [75]. Given the diversity, immaturity, complexity of smart homes and the inconsistencies surrounding security and privacy experiences, we argue that a more proactive approach is also needed.

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

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

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

A summary of the major contributions of this paper and how they relate to existing work can be found in the appendix in Table 3.

## 6 CONCLUSION

Despite growing at double-digit rates across the globe, smart home devices still routinely suffer from consumer privacy and security problems. In this paper, we have presented a longitudinal view of smart home security and privacy experiences from the secondary analysis of a six-month ethnographic study of six UK households. We found the experience of managing security and privacy to be inconsistent. We also found that repurposed smart home products introduced negative security and privacy effects (e.g., intrusiveness). Based on our findings, we conclude with design recommendations:

**Improve the experience of consent processes:** The design of data use consent needs to consider the experience of changes over time (e.g., granting, revoking and amending consent), the experience of withholding consent, and how the experience of making mistakes can be made more forgiving.

**Forecast and plan for the consequences of technology repurposing:** Technology repurposing can bring benefits, but can also introduce new security and privacy threats. Designers should develop knowledge of the risks and threats of repurposing and improve the transparency of sensitive features (e.g., cameras). Users should be able to easily find accessible usage logs and should be reminded (e.g., notifications, visual indicators) when sensitive features are enabled.

**Where available, tangible controls can improve the privacy experience:** The ability to give users full control over their personal information is crucial to providing assurance. Tangible privacy controls (e.g., physically taping a camera) provided more assurance than other more abstract controls (e.g., data use policies). Visual cues have historically provided privacy assurance to web users [6], however more research is needed to understand whether this is applicable, and more fundamentally how effectiveness of privacy controls is perceived in smart products.

## ACKNOWLEDGMENTS

This research was supported by the 2018-2019 Information Commissioner's Office's (ICO) Grants Programme. George Chalhoub is funded by Fondation Sesam. The authors would like to thank Elie Tom, Ruba Abu-Salma, and the anonymous CHI reviewers for their valuable input. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ICO, or any sponsor.

## REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[2] Muhammad Raisul Alam, Mamun Bin Ibne Reaz, and Mohd Alauddin Mohd Ali. 2012. A Review of Smart Homes—Past, Present, and Future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42, 6 (Nov. 2012), 1190–1203. https://doi.org/10.1109/TSMCC.2012.2189204

[3] Alaa Althubaiti. 2016. Information bias in health research: definition, pitfalls, and adjustment methods. *Journal of Multidisciplinary Healthcare* 9 (May 2016), 211–217. https://doi.org/10.2147/JMDH.S104807

[4] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).

[5] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 59.

[6] Gaurav Bansal, Fatemeh 'Mariam' Zahedi, and David Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems* 24, 6 (2015), 624–644.

[7] Genevieve Bell and Paul Dourish. 2007. Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal and Ubiquitous Computing* 11, 2 (Feb. 2007), 133–143. https://doi.org/10.1007/s00779-006-0071-x

[8] Victoria Bellotti and Abigail Sellen. 1993. Design for privacy in ubiquitous computing environments. In *Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work (ECSCW'93)*. Kluwer Academic Publishers, Milan, Italy, 77–92.

[9] Asa Blomquist and Mattias Arvola. 2002. Personas in action: ethnography in an interaction design team. In *Proceedings of the second Nordic conference on Human-computer interaction*. 197–200.

[10] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological*. American Psychological Association, Washington, DC, US, 57–71. https://doi.org/10.1037/13620-004

[11] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, Vancouver, BC, Canada, 2115–2124. https://doi.org/10.1145/1978942.1979249

[12] Marta Cecchinato and Daniel Harrison. 2017. Degrees of Agency in Owners and Users of Home IoT Devices. In *CHI'17 workshop: Making Home: Asserting Agency in the Age of IoT*. Association for Computing Machinery (ACM).

[13] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In *Sixteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2020)*. 185–204.

[14] Bradley Chambers. 2020. HomeKit Weekly: Apple should allow selective access to HomeKit devices for Family Sharing. https://9to5mac.com/2020/01/24/homekit-family-sharing/

[15] Charlton, Alistair. 2018. Sharing your smart home with others is a minefield of inconvenience. https://www.gearbrain.com/sharing-smart-home-devices-2608366363.html

[16] Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. 2010. Who's hogging the bandwidth: the consequences of revealing the invisible in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, Atlanta, Georgia, USA, 659–668. https://doi.org/10.1145/1753326.1753423

[17] Marshini Chetty, Ja-Young Sung, and Rebecca E. Grinter. 2007. How Smart Homes Learn: The Evolution of the Networked Home and Household. In *UbiComp 2007: Ubiquitous Computing (Lecture Notes in Computer Science)*, John Krumm, Gregory D. Abowd, Aruna Seneviratne, and Thomas Strang (Eds.). Springer, Berlin, Heidelberg, 127–144. https://doi.org/10.1007/978-3-540-74853-3_8

[18] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a glass house: a survey of private moments in the home. In *Proceedings of the 13th international conference on Ubiquitous computing (UbiComp '11)*. Association for Computing Machinery, Beijing, China, 41–44. https://doi.org/10.1145/2030112.2030118

[19] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. Association for Computing Machinery, Pittsburgh, Pennsylvania, 61–70. https://doi.org/10.1145/2370216.2370226

[20] K. L. Courtney. 2008. Privacy and Senior Willingness to Adopt Smart Home Information Technology in Residential Care Facilities. *Methods of Information in Medicine* 47, 1 (2008), 76–81. https://doi.org/10.3414/ME9104 Publisher: Schattauer GmbH.

[21] L. Cranor, T. Rabin, V. Shmatikov, S. Vadhan, and D. Weitzner. 2015. Towards a Privacy Research Roadmap for the Computing Community: A white paper prepared for the computing community consortium committee of the computing research association. (2015).

[22] John W. Creswell and J. David Creswell. 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

[23] Ry Crist. 2015. Multiple users, multiple systems, multiple devices: Is this the smart home from hell? https://www.cnet.com/news/multiple-users-multiple-systems-multiple-devices-is-this-the-smart-home-from-hell/

[24] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. 2010. Parenting from the pocket: value tensions and technical directions for secure and private parent-teen mobile safety. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. Association for Computing Machinery, Redmond, Washington, USA, 1–15. https://doi.org/10.1145/1837110.1837130

[25] Angela Dale, Sara Arber, and Michael Procter. 1988. *Doing secondary analysis*. Unwin Hyman.

[26] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse.. In *NDSS*, Vol. 14. 23–26.

[27] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. 2006. Principles of Smart Home Control. In *UbiComp 2006: Ubiquitous Computing (Lecture Notes in Computer Science)*, Paul Dourish and Adrian Friday (Eds.). Springer, Berlin, Heidelberg, 19–34. https://doi.org/10.1007/11853565_2

[28] George Demiris and Brian K. Hensel. 2008. Technologies for an aging society: a systematic review of "smart home" applications. *Yearb Med Inform* 3 (2008), 33–40.

[29] ISO DIS. 2010. 9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems (formerly known as 13407). *International Standardization Organization (ISO). Switzerland* (2010).

[30] Daniel M. Doolan and Erika S. Froelicher. 2009. Using an existing data set to answer new research questions: a methodological review. *Research and Theory for Nursing Practice* 23, 3 (2009), 203–215. https://doi.org/10.1891/1541-6577.23.3.203

[31] Paul Dourish, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[32] Stuart E. Dreyfus and Hubert L. Dreyfus. 1980. *A five-stage model of the mental activities involved in directed skill acquisition*. Technical Report. California Univ Berkeley Operations Research Center.

[33] Chris Duckett. 2018. Google needs to break up its all-or-nothing approach to permissions. https://www.zdnet.com/article/google-needs-to-break-up-its-all-or-nothing-approach-to-permissions/

[34] Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On? Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, Seoul, Republic of Korea, 1669–1678. https://doi.org/10.1145/2702123.2702251

[35] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[36] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 268.

[37] Esther Goernemann and Sarah Spiekermann. 2020. Moments of Truth with Conversational Agents: An Exploratory Quest for the Relevant Experiences of Alexa Users. *ECIS 2020 Research Papers* (June 2020). https://aisel.aisnet.org/ecis2020_rp/169

[38] Rebecca E. Grinter, W. Keith Edwards, Marshini Chetty, Erika S. Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, and Chris Greenhalgh. 2009. The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Transactions on Computer-Human Interaction (TOCHI)* 16, 2 (2009), 8.

[39] Rebecca E. Grinter, W. Keith Edwards, Mark W. Newman, and Nicolas Ducheneaut. 2005. The Work to Make a Home Network Work. In *ECSCW 2005*, Hans Gellersen, Kjeld Schmidt, Michel Beaudouin-Lafon, and Wendy Mackay (Eds.). Springer Netherlands, Dordrecht, 469–488. https://doi.org/10.1007/1-4020-4023-7_24

[40] Manu Gupta, Stephen S. Intille, and Kent Larson. 2009. Adding GPS-Control to Traditional Thermostats: An Exploration of Potential Energy Savings and Design Challenges. In *Pervasive Computing (Lecture Notes in Computer Science)*, Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe (Eds.). Springer, Berlin, Heidelberg, 95–114. https://doi.org/10.1007/978-3-642-01516-8_8

[41] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT). In *27th ${$USENIX$}$ Security Symposium (${$USENIX$}$ Security 18)*. 255–272.

[42] Pamela S. Hinds, Ralph J. Vogel, and Laura Clarke-Steffen. 2016. The Possibilities and Pitfalls of Doing a Secondary Analysis of a Qualitative Data Set:. *Qualitative Health Research* (July 2016). https://doi.org/10.1177/104973239700700306 Publisher: Sage PublicationsSage CA: Thousand Oaks, CA.

[43] Jason I. Hong and James A. Landay. 2004. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services (MobiSys '04)*. Association for Computing

Machinery, Boston, MA, USA, 177–189. https://doi.org/10.1145/990064.990087
[44] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. Association for Computing Machinery, Seattle, Washington, 571–582. https://doi.org/10.1145/2632048.2632079
[45] Information Commissioner's Office. 2020. When is consent appropriate? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/
[46] S.S. Intille. 2002. Designing a home of the future. *IEEE Pervasive Computing* 1, 2 (April 2002), 76–82. https://doi.org/10.1109/MPRV.2002.1012340
[47] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, Denver, Colorado, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799
[48] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (Dec. 2018), 171:1–171:28. https://doi.org/10.1145/3287049
[49] Melissa P. Johnston. 2017. Secondary data analysis: A method of which the time has come. *Qualitative and quantitative methods in libraries* 3, 3 (2017), 619–626.
[50] Meg Leta Jones. 2015. *Privacy Without Screens & the Internet of Other People's Things*. SSRN Scholarly Paper ID 2614066. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=2614066
[51] Cory D. Kidd, Robert Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner, and Wendy Newstetter. 1999. The Aware Home: A Living Laboratory for Ubiquitous Computing Research. In *Cooperative Buildings. Integrating Information, Organizations, and Architecture (Lecture Notes in Computer Science)*, Norbert A. Streitz, Jane Siegel, Volker Hartkopf, and Shin'ichi Konomi (Eds.). Springer, Berlin, Heidelberg, 191–198. https://doi.org/10.1007/10705432_17
[52] Tiiu Koskela and Kaisa Väänänen-Vainio-Mattila. 2004. Evolution towards smart home environments: empirical evaluation of three user interfaces. *Personal and Ubiquitous Computing* 8, 3 (July 2004), 234–240. https://doi.org/10.1007/s00779-004-0283-x
[53] Robert V. Labaree. 2009. Research Guides: Organizing Your Social Sciences Research Paper: 5. The Literature Review. (2009).
[54] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. Association for Computing Machinery, New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366
[55] Brian Y. Lim, Anind K. Dey, and Daniel Avrahami. 2009. *Why and why not* explanations improve the intelligibility of context-aware intelligent systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. Association for Computing Machinery, Boston, MA, USA, 2119–2128. https://doi.org/10.1145/1518701.1519023
[56] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271.
[57] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications (HotMobile '19)*. Association for Computing Machinery, Santa Cruz, CA, USA, 117–122. https://doi.org/10.1145/3301293.3302371
[58] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, Atlanta, Georgia, USA, 645–654. https://doi.org/10.1145/1753326.1753421
[59] Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. 2011. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, Vancouver, BC, Canada, 2085–2094. https://doi.org/10.1145/1978942.1979245
[60] Mary L. McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica: Biochemia medica* 22, 3 (2012), 276–282. Publisher: Medicinska naklada.
[61] Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them. In *Pervasive Computing (Lecture Notes in Computer Science)*, Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger (Eds.). Springer, Berlin, Heidelberg, 143–160. https://doi.org/10.1007/978-3-642-31205-2_10
[62] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2017)*. 399–412.
[63] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An empirical investigation of concerns of everyday tracking and recording technologies. In *Proceedings of the 10th international conference on Ubiquitous computing*. Association for Computing Machinery, New York, NY, USA, 182–191. https://doi.org/10.1145/1409635.1409661
[64] Norbert Nthala and Ivan Flechais. 2018. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 63–82.
[65] Norbert Nthala and Emilee Rader. 2020. Towards a Conceptual Model for Provoking Privacy Speculation. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3382815
[66] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. Association for Computing Machinery, Pittsburgh, Pennsylvania, 41–50. https://doi.org/10.1145/2370216.2370224
[67] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. Association for Computing Machinery, Ft. Lauderdale, Florida, USA, 129–136. https://doi.org/10.1145/642611.642635
[68] Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems (DIS '08)*. Association for Computing Machinery, Cape Town, South Africa, 455–464. https://doi.org/10.1145/1394445.1394494
[69] Dave Randall. 2003. Living Inside a Smart Home: A Case Study. In *Inside the Smart Home*, Richard Harper (Ed.). Springer, London, 227–246. https://doi.org/10.1007/1-85233-854-7_12
[70] John P. Robinson, Phillip R. Shaver, and Lawrence S. Wrightsman. 2013. *Measures of personality and social psychological attitudes: Measures of social psychological attitudes*. Vol. 1. Academic Press.
[71] Eyal Ronen and Adi Shamir. 2016. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In *2016 IEEE European Symposium on Security and Privacy (EuroS P)*. 3–12. https://doi.org/10.1109/EuroSP.2016.13
[72] Erika Shehan and W. Keith Edwards. 2007. Home networking and HCI: what hath god wrought?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. Association for Computing Machinery, San Jose, California, USA, 547–556. https://doi.org/10.1145/1240624.1240712
[73] Dale Smith. 2020. Fix 3 common Google Home music glitches before they happen. https://www.cnet.com/how-to/fix-3-common-google-home-music-glitches-before-they-happen/
[74] Daniel J. Solove. 2008. Understanding privacy. (2008).
[75] Ashkan Soltani. 2019. Abusability testing: Considering the ways your technology might be used for harm. In *Enigma 2019 (Enigma 2019)*.
[76] David W. Stewart, David W. Stewart, and Michael A. Kamins. 1993. *Secondary research: Information sources and methods*. Vol. 4. Sage.
[77] Elizabeth A. Suter. 2000. Focus groups in ethnography of communication: Expanding topics of inquiry beyond participant observation. *The Qualitative Report* 5, 1 (2000), 1–14.
[78] Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2007. Making the home network at home: Digital housekeeping. In *ECSCW 2007*, Liam J. Bannon, Ina Wagner, Carl Gutwin, Richard H. R. Harper, and Kjeld Schmidt (Eds.). Springer, London, 331–350. https://doi.org/10.1007/978-1-84800-031-5_18
[79] Daphne Townsend, Frank Knoefel, and Rafik Goubran. 2011. Privacy versus autonomy: A tradeoff model for smart home monitoring technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 4749–4752. https://doi.org/10.1109/IEMBS.2011.6091176 ISSN: 1558-4615.
[80] Alexander Tsesis. 2014. The right to erasure: Privacy, data brokers, and the indefinite retention of data. *Wake Forest L. Rev.* 49 (2014), 433. Publisher: HeinOnline.
[81] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2014, 209–218.
[82] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 129–139.
[83] Mojtaba Vaismoradi, Hannele Turunen, and Terese Bondas. 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences* 15, 3 (2013), 398–405. https://doi.org/10.1111/nhs.12048 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/nhs.12048.
[84] Rick Wash and Emilee Rader. 2015. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (${$SOUPS$}$ 2015)*. 309–325.
[85] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2017. 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, 181–18109.

[86] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2 (2015), 463–476.

[87] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and risks of smart home technologies. *Energy Policy* 103 (2017), 72–83.

[88] Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourself-style smart homes. In *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing*. ACM, 779–790.

[89] Allison Woodruff, Sally Augustin, and Brooke Foucault. 2007. Sabbath day home automation: "it's like mixing technology and religion". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. Association for Computing Machinery, San Jose, California, USA, 527–536. https://doi.org/10.1145/1240624.1240710

[90] Rayoung Yang and Mark W. Newman. 2013. Learning from a learning thermostat: lessons for intelligent systems for the home. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing (UbiComp '13)*. Association for Computing Machinery, Zurich, Switzerland, 93–102. https://doi.org/10.1145/2493432.2493489

[91] Robert K. Yin. 2015. *Qualitative research from start to finish*. Guilford publications.

[92] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 65–80.

[93] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *28th USENIX Security Symposium (USENIX Security 19)*. 159–176.

[94] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 200.

# APPENDIX

In the table below, we align the major contributions of our paper with the related work described in Section 2.

**Table 3: Comparison of our major contribution with existing work**

| Finding | Comparison |
|---|---|
| The experience of consent management was uneven: consent to data collection was easy to grant, but difficult to withhold and revoke. | This is a novel finding and our research provides a rich ethnographic account of consent experiences. Other work [5, 44, 62] has explored, through surveys and a 1-week in-situ study (where participants wore a lifelogging device), the importance of consent and the modalities of consenting to data use in smart homes, however they have neither identified the disparity nor provided much information about the wider context of such consent experiences. |
| Smart home device use changed over time (for parenting and entertainment) which led to new security and privacy tensions from others both within and neighboring the home (e.g., intrusiveness, loss of control). | Prior work explores potential misuse [54, 75] of smart devices in the context of domestic abuse, more work [36, 61, 92] has identified that issues can arise from the imbalance between active and passive users (i.e., those that configure smart devices and those that do not). Our work provides examples and insights into how use changes over time and not just that it does. It aligns with the call for future work in Geeng and Roesner [36] to consider the concerns of children and passive users in smart homes, as well as how interactions change over longer periods of time. |
| Access control management was poorly suited to the needs of the households, and resulted in account sharing instead of permission delegation. | Smart home access control features have been reported to be poorly usable and inconsistent (e.g., [41, 57, 81, 93]). We corroborate earlier findings and provide additional detail pertaining to situations where access control does not fit the needs of the user (e.g., multiple accounts in smart speakers are too difficult to use). We also expand on this area by exploring access control experiences resulting from prolonged use of an ecosystem of more and less invasive commercial devices. |
| Participants exercised control over their private data through both designed controls and workarounds (e.g., physical taping a camera). However, security behavior involved only designed controls use. | Previous work has widely reported how smart home users control their personal information (e.g., [5, 34, 44, 56, 84]). Our research uses longitudinal data to study unsolicited security and privacy behaviors over time. We corroborate earlier findings and note that behavior observed over shorter periods of time is consistent with behaviors over longer periods of time. We also identify that home users commonly augment their use of designed controls with workarounds to protect their privacy (e.g., taping cameras, unplugging or moving devices), however they do not do this to protect their security and rely only on the designed controls. |
| Privacy and security concerns arose from media and online sources. While privacy concerns also arose from device use, security concerns did not. | Previous work widely reported smart home security and privacy concerns in smart homes (e.g., [1, 18, 19, 63, 82, 92, 94]). We corroborate earlier findings and expand them by providing a richer account of unsolicited privacy and security concerns and where they originate from. We confirm earlier findings that security and privacy concerns arise from online and media sources, however we make the novel observation that using devices led to new privacy concerns but not to security concerns. |