Designing and Evaluating a Prototype for Data-related Privacy Controls in a Smart Home*

Chola Chhetri and Vivian Motti

George Mason University, Fairfax VA 22030, USA
{cchhetri,vmotti}@gmu.edu

Abstract. The privacy concerns of home Internet of Things (IoT) device users and experts have been widely studied, but the designs of privacy controls addressing those concerns are sparse. Literature shows a significant body of research uncovering design factors for privacy controls in smart home devices, but fewer studies have translated those design recommendations into design and evaluated the designs. To fill this gap, we designed a prototype user interface implementing the design recommendations of data-related privacy controls based on prior work and evaluated the prototype for user experience, usability, perceived information control, user satisfaction, and intention to use. The results of interviews (n=10) critique the proposed design and the survey results (n=105) show that the prototype design provides positive evaluation for perceived information control, user satisfaction and intention to use. Based on findings, we discuss design recommendations for further improvements. Thus, this paper contributes to the design of data-related privacy controls for user interfaces of home IoT devices and applications.

Keywords: Prototype · Smart home devices · Privacy · Interface.

1 Introduction

Researchers and security experts have identified vulnerabilities and concerns in smart home devices (SHDs) or home Internet of Things (IoT) devices [3, 8]. Although users are known to have inadequate and inaccurate mental models of smart device risks [25], they have expressed concerns [6]. Privacy has been identified as one of the primary reasons for non-use of SHDs [25, 4].

Researchers have further identified privacy concerns of users and made design recommendations for the development of privacy controls [22–24]. However, few studies have translated those design recommendations and needs into user interface designs that can address the privacy concerns.

To fill this gap, we designed a prototype of a user interface implementing the design factors elicited from prior literature. For the prototype design, we

Published by Springer Nature Switzerland AG 2022
N. Clarke and S. Furnell (Eds.): HAISA 2022, IFIP AICT 658, pp. 1–11, 2022.
https://doi.org/10.1007/978-3-031-12172-2_19

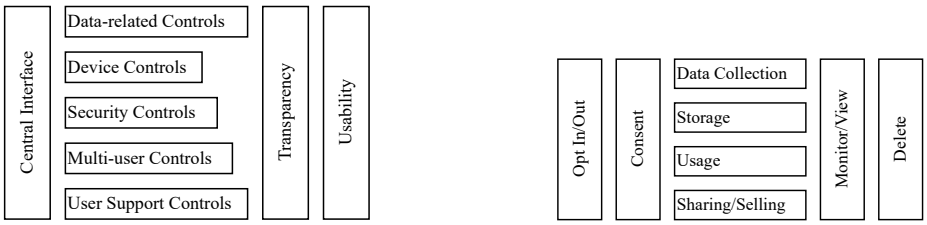
followed an iterative approach. We evaluated the prototype for user experience, usability, perceived information control, user satisfaction and intention to use. Evaluation user studies included interviews (n=10) and survey (n=105). For the purpose of this study, we framed the prototype as an app for camera. However, the proposed design may serve as a design pattern for other home IoT systems.

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

2 Background

2.1 Privacy Control Design Factors and Sub-factors

Researchers have identified privacy concerns and provided design recommendations for smart home designers and developers [7, 10, 21–23]. In [5], researchers empirically identified seven design factors for implementing privacy controls in smart home designs: data-related controls, device controls, transparency, multi-user, central interface, support and security controls. We summarize the design factors in the form of a graphic in Fig. 1a. The vertical bars represent constructs that affect all factors in horizontal bars.



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

Fig. 1: Privacy Controls from Literature and our Research Approach

2.2 Translating Privacy Control Design Factors into Design

Transparency with regard to online privacy has been widely investigated with one popular approach being privacy labels. There has been research about online privacy labels [11, 8], which has even recently been adopted by Apple[1] and Google[2] in their app stores. Examples of privacy label work include privacy nutrition label [11], GDPR-based privacy label for IoT devices OnLITE [14], and security and privacy label with device factors [17]. Similarly, prior work has investigated the designs of user notifications to enhance transparency [13].

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

Prior work has explored the design of *multi-user* controls. In [24], researchers developed and evaluated multi-user settings for a smart home app. In [9], authors proposed a design space for privacy choices and use-case design of a privacy choice platform app IOTAssistant.

While designs towards *transparency*, *multi-user settings*, d*evice controls*, and notice and choice have been explored, designs of *data-related controls* are sparse. So, this paper focuses on the design of data-related privacy controls using the design factors from section 2.1 as a foundation. For this purpose, we drew from literature [5] the following data-related privacy control *requirements* : Opt-in (or out), Consent, Data collection, Storage, Usage, Sharing or selling, Monitor or view, and Delete [9, 10, 21–25]. We illustrate these requirements in Fig. 1b.

3 Method

We designed a prototype to implement the user requirements of data-related privacy controls. Then, we conducted user studies to evaluate the prototype and gain insights into design improvements. Fig. 2 visualizes our research approach.

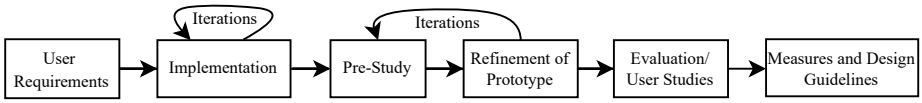


Fig. 2: Research Approach

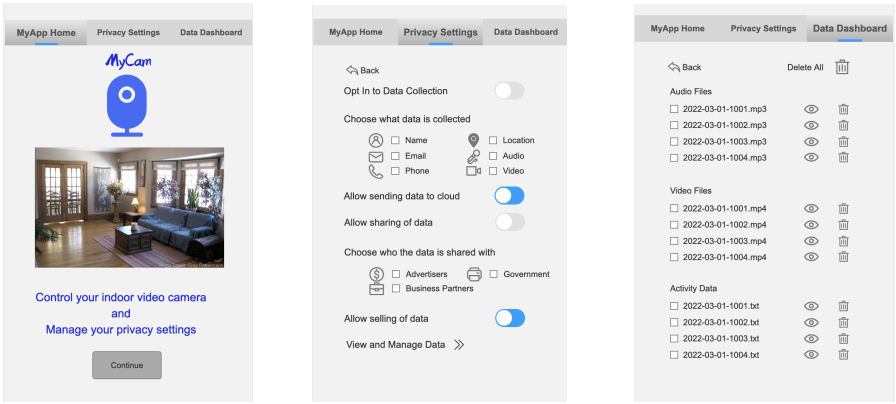
3.1 Stimulus (Prototype App)

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

The prototype app, called MyCam, consisted of three pages: MyCam Home, Privacy Settings, and Data Dashboard. The home page contained the app logo, a view of the camera footage, a brief explanation that user can control the camera and manage privacy settings, and a continue button to navigate to the privacy settings page (See Fig. 3a). The privacy settings page consisted of data-related controls: opt-in to data collection, control what data type is collected, allow (or disallow) sending/sharing/selling of data, choose who data are shared with, and a link to data dashboard for viewing and managing data (See Fig. 3b). The data

[3] mockplus.com

dashboard page displayed all audio, video and other activity files with options to view and delete the data individually or all-at-once (See Fig. 3c). In addition, each page contained a horizontal navigation bar with three buttons at the top.



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

Fig. 3: Home, Settings, and Dashboard pages of the MyCam prototype app.

3.2 Pre-Study

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

3.3 Interview Study

We conducted semi-structured interviews with 10 participants recruited via twitter. Interview protocol was reviewed by George Mason University's institutional review board (IRB). Interview protocol included demographics and prototype evaluation questions. We have shared the entire study in [2].

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

We qualitatively analyzed the interviews. We did not perform quantitative analysis on interview data due to the small sample size. Interviews allowed us

to probe deeper into the perceptions of participants and understand the problems that participants experienced while using the prototype. We analyzed the interview transcripts for recurring patterns or themes.

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

3.4 Survey Study

To reach a large and diverse sample of participants, we designed a survey in which we embedded the app and requested participants' opinions and feedback on the app. We designed the evaluation questions from standard instruments or psychometrically validated Likert scales.

Measurements We used the User Experience Questionnaire (UEQ) scale (26 items) to measure user experience [15]. To measure usability, we used the System Usability Scale (SUS) scale (10 items, 5-point Likert) [1]. We measured user satisfaction using a 4-item scale adapted from [16]. We adapted perceived information control scale (5 items) from [20] and intention-to-use scale (3 items) from [19]. Unless otherwise noted, we designed all items as 7-point Likert items.

Procedure We advertised the study as an evaluation of a prototype app. The study was approved by our university's Institutional Review Board (IRB) prior to the survey. We recruited participants using the crowd-sourcing platform Mechanical Turk (MTurk), which is widely used by researchers to conduct security and privacy studies. We screened out participants to ensure good quality responses. Participants were adults living in the United States, had an approval rating of 95%, completed 100 MTurk tasks, and used at least one SHD. Research shows that MTurk sample is diverse and its perception is US representative [18].

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

Interface Interaction/Task Selection We asked the participants to perform the following tasks in the prototype app and report completion status:

- TASK1 Click Continue on MyCam Home page to go to privacy settings page.
- TASK2 Turn on Opt In to Data Collection.
- TASK3 Select the data you would allow MyCam to collect about you.
- TASK4 Turn off Allow sending of data to the cloud.

- TASK5 Turn on Allow sharing of data.
- TASK6 Choose who you would allow the company to share the data with.
- TASK7 Turn on (or off) Allow selling of data.
- TASK8 Delete the fist audio file 2022-03-01-1001.mp3.
- TASK9 Go to the MyCam Home page.

Participants A total of 120 participants completed the survey and were compensated US$1.50 for completing the survey. With an average completion time of 7 minutes, the rate averaged about $12.85 an hour. We excluded 16 responses that (a) did not pass the attention check questions, (b) contained copy-paste answers for an open-ended question, (c) had patterned or lined-up answers, or (d) had extremely low survey completion time resulting in low quality responses. We included the remaining 105 responses in the analysis.

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

4 Results

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

4.1 Task Accuracy

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

Table 1: Task accuracy (n=105).

Task#	TASK1	TASK2	TASK3	TASK4	TASK5	TASK6	TASK7	TASK8	TASK9
Accuracy	0.981	0.952	0.971	0.962	0.943	0.971	0.933	0.733	0.524

4.2 User Experience

The UEQ instrument measures six dimensions of user experience: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. Mean score below -0.8 is negative, between -0.8 and 0.8 is neutral, and above 0.8 is positive evaluation. Our prototype was evaluated *positive* for attractiveness (Mean μ =0.91 and

Variance σ^2=1.44), perspicuity (μ=1.02, σ^2=1.58), efficiency (μ=0.82, σ^2=1.42), and dependability (μ=0.83, σ^2=1.08). It was evaluated *neutral* for stimulation (μ=0.65, σ^2=1.38) and novelty (μ=0.07, σ^2=0.95) (see Fig. 4).

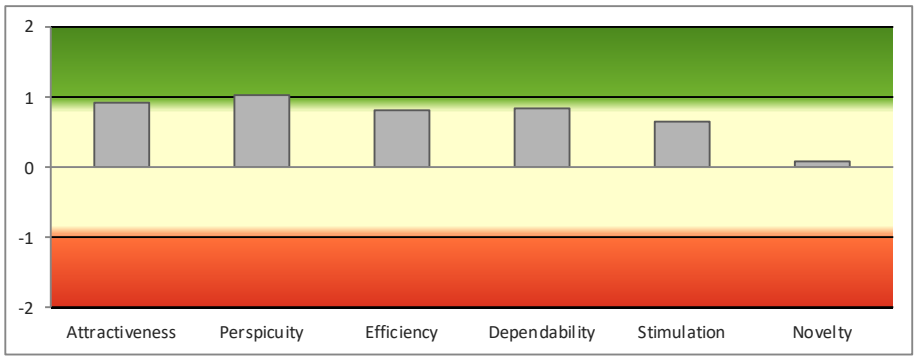


Fig. 4: Results showing scores for the six dimensions of the UEQ scale.

4.3 Usability

We used the SUS scale to measure the usability of the prototype. The average overall SUS score from survey participants (n=105) was 62.5 (Min=37.5, Max=100) which is about average [12]. The benchmark average SUS score for a website is 68; we were unable to find a benchmark for home IoT apps. The SUS scores of MyCam show that MyCam has room for improvement in usability.

4.4 Perceived Information Control

Survey participants found MyCam's perceived information control to be above average (μ=4.37, σ=1.28) and the scale demonstrated good internal consistency (α=0.88) (See Table 2).

Table 2: Scale statistics (n=105)

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

4.5 User Satisfaction

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

4.6 Behavioral Intention to Use

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

4.7 User Feedback

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

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

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

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

5 Discussion

Results of users studies show that our prototype was perceived by participants with good perceived information control, user satisfaction, and intention to use. The usability and user experience scores were satisfactory but there is room for improvement. Thus, based on the findings, we discuss some design recommendations for improvement to MyCam's usability and user experience.

5.1 Design Recommendations

Complement data-related controls with transparency features. In order to address the lack of transparency as stated in section 4.7, we suggest that transparency mechanisms be utilized in conjunction with data related controls. A combination of our design with notice and choice designs presented in [9] may be useful in this regard. Improvements can also include integration of labels [11] and notifications [13] with the data-related privacy designs.

Tiered Privacy Approach for Managing User Burden. The provision of large number of privacy controls may give users a sense of control but it lowers usability. In [25], authors call for reducing burden of privacy on users. Thus, we recommend a balanced approach to reduce the user burden while providing privacy control. In this regard, we suggest a tiered privacy settings approach involving three preset options: high privacy, medium privacy, and low privacy. Each of these privacy presets will achieve privacy that is equivalent to many user clicks. For example:

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

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

5.2 Limitations and Future Work

While a large body of privacy research utilizes MTurk, the representation has been debated. Recent literature shows that MTurk sample may not be US representative but its perceptions may be representative [18]. Thus, we utilized a mixed-methods approach to enhance the validity of findings. Another limitation is that the user studies' results may not be generalizable to non-US populations.

In our future work, we aim to improve the design of MyCam by implementing the above design guidelines and evaluate how they meet the user needs. We also aim to implement the data-related privacy controls designs in the context of other SHDs, such as voice speakers, baby monitors, thermostats, etc.

6 Conclusion

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

Acknowledgement

We thank our lab members for their input and anonymous reviewers for their comments. We are grateful to the interview and survey participants. This research was funded in part by 4-VA, a collaborative partnership for advancing the Commonwealth of Virginia, and Commonwealth Cyber Initiative (CCI). Any opinions expressed in this article are those of the authors and do not necessarily reflect the views of our research sponsors.

21. Yang, H., Lee, W., Lee, H.: Iot smart home adoption: the importance of proper level automation. Journal of Sensors **2018** (2018)
22. Yao, Y., Basdeo, J.R., Kaushik, S., Wang, Y.: Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 198:1–198:12. CHI '19, ACM, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300428
23. Yao, Y., Basdeo, J.R., Mcdonough, O.R., Wang, Y.: Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum.-Comput. Interact. **3**(CSCW) (nov 2019). https://doi.org/10.1145/3359161, https://doi.org/10.1145/3359161
24. Zeng, E., Roesner, F.: 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). pp. 159–176 (2019)
25. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home iot privacy. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–20 (2018)

A Interview Protocol

A.1 Screening Questions

1. Do you currently use a smart home device? [Yes/No]
2. How many smart home devices do you use? [1-5+]
3. What smart home devices do you use?

A.2 Interview Questions

[Informed Consent] [Permission to Record]

1. (Introduce the app) Many smart home device users like to manage privacy of their data. We have designed privacy settings of an app for possible use with a smart home device, such as a security camera.
   Imagine you have an indoor video camera and the app you are about to see provides privacy settings regarding your data collected by the camera, stored by the company and shared or sold by the company. We are calling this app MyCam. At this stage, we are in initial design phase. Your feedback will help improve the design of this app.
   Today, you will be evaluating the privacy settings of this MyCam app designed to provide privacy controls to the smart home device user. I will provide you a link to the app. (Give the link to the participant).
   Please take a few minutes to browse through the MyCam app and familiarize with it.
2. (When participant is done familiarizing with the MyCam app, ask them to share their screen, so the interviewer can see the participant's interaction with the MyCam app.) Please perform the following tasks in the MyCam app: