Enhancing the Design of Data-Related Privacy Controls for Smart Home Devices

Journal:	*Information and Computer Security*
Manuscript ID	ICS-11-2022-0173
Manuscript Type:	Original Article
Keywords:	Usability, Privacy, Internet of Things, Smart home, Privacy Controls, User interfaces

Enhancing the design of data-related privacy controls for smart home devices

First author
(email)

Second author
(email)

November 5, 2022

Abstract

Purpose: Past research shows that users of smart home devices have privacy concerns. These concerns have been validated from technical research that shows smart home devices introduce a lot of privacy risks. However, there is limited research in addressing these concerns and risks.

Design/methodology/approach: In this paper, we follow a user-centered design approach to design data-related privacy controls from design requirements backed by literature. We test the design for usability and perceived information control using psychometrically validated scales.

For this purpose, we created two variations of the prototype (MyCam1 with a listing of data-related privacy controls and MyCam2 with three privacy presets) and tested them in a between-subjects experimental setting. Study participants (n=207) were recruited via Mechanical Turk and asked to use the prototype app. An online survey was distributed to the participants to measure some usability and privacy-related constructs.

Findings: Findings show that the presented prototype design were usable and met the privacy control needs of users. The prototype design with privacy presets was found to be significantly more usable than the list of privacy controls.

Originality: The findings of this article are original and build on the findings presented in our HAISA paper. This paper contributes better and usable designs of privacy controls for smart home applications.

1 Introduction

As the Internet of Things (IoT) grows to tens of billions of connected devices, the portion those IoT devices is also increasing (Taylor, Baron & Schmidt 2015). In this article, we refer to these home IoT devices as smart home devices (SHD). Although SHDs are primarily used for convenience and home automation reasons, they introduce risks to the users.

Prior research shows that SHDs vulnerabilities can be exploited resulting in the violation of users' privacy (Chhetri & Motti 2020). Various incidents that have received media attention, such as baby monitor hacks and botnet attacks, have demonstrated such possibilities. Such incidents endanger people's lives and hinder the peace and harmony of the home. Hence, the design of privacy preserving smart home devices is crucial.

Researchers have studied privacy concerns of users, non-users and bystanders. They have made design recommendations to address those concerns and prevent privacy violations incidents (Feng, Yao & Sadeh 2021). Chhetri & Motti (2022*d*) presented a privacy design framework for smart home devices. The framework consisted of seven design factors: data-related controls, transparency-related controls, centralized interface, device controls, multi-user controls, user support, and security controls.

However, fewer recommendations have been translated into designs. For the users to benefit from the recommendations, designs need to be created and implemented in smart home applications. We aim to fill this gap by creating and evaluating privacy designs to meet the privacy needs of SHD users.

Among the seven design-factors stated earlier, data-related privacy controls were the most desired by users. Thus, Chhetri & Motti (2022*b*) presented a design of data-related privacy controls and evaluated the prototype design to elicit users' feedback and made design recommendations. They implemented the privacy settings as a list of privacy controls for smart home data control. They identified weaknesses in the proposed design and made recommendations to improve the usability and user experience (UX) of the app design.

In the work discussed in this article, we advance the work on the design of data-related privacy controls forward by creating an improved design of the app. We implemented a newer version of the prototype app in which the privacy settings are designed as privacy presets. To this end, we created two prototype app designs (list condition and presets condition). We called the app with privacy controls list MyCam1 and the app with privacy presets MyCam2. We then conducted survey studies involving smart home users to evaluate the usability, user experience, perceived information control, user satisfaction, and intention to use both versions. We analyzed whether there was statistical significance in the user perceptions on both of these apps. Our hypothesis was that the improved design (presets condition) will be more usable or provide better usability than the earlier design (list condition).

The survey results proved our hypothesis to be true. The newer design (presets condition) scored significantly higher on the usability than the older design (list condition or MyCam1). We will further discuss the methods, results, and their implications in this paper.

Thus, this paper contributes to the smart home privacy domain by informing how to better design more usable privacy controls for the smart home. We have made the prototype designs available for smart home designers to build upon. The interactive prototypes can also serve as design patterns for the hundreds of types of smart home devices in the domain and for IoT devices at large.

2 Related Work

In this section, we will discuss prior work on users' privacy concerns, users' privacy control needs, and designs of privacy controls to meet those needs.

2.1 SHD Users' Privacy Concerns

Researchers have studied various stakeholders to understand and characterize their concerns (Emami-Naeini 2021, Haney, Furman & Acar 2020, Yang, Lee &

Lee 2018). Users are one of the stakeholders. SHD users are people who own and use SHDs and are primarily responsible to manage their SHDs. Another group of stakeholders is bystanders, such as visitors and guests, who are subject to the data collected by SHDs but do not have any control over the management of those SHDs (Yao, Basdeo, Kaushik & Wang 2019*a*). Lastly, non-users are people who do not use SHDs for a variety of reasons, such as privacy concerns, lack of interest, and cost (Chhetri & Motti 2022*a*).

Both users and non-users can become bystanders to SHDs owned and managed by other people. Thus, the concerns among these three stakeholders are overlapping and not mutually exclusive. It is essential to create designs that address concerns of all stakeholders (Chhetri 2019).

Prior work has found that SHD users are concerned about information collection, information processing, information sharing, and information protection (Chhetri & Motti 2022*c*). Similarly, literature shows that similar concerns exist among bystanders or accidental users (Yao, Basdeo, Mcdonough & Wang 2019). In addition, prior work has shown that there exist non-users with similar concerns, although they may be more concerned more about information collection than users who are more concerned about information protection (Chhetri & Motti 2022*a*).

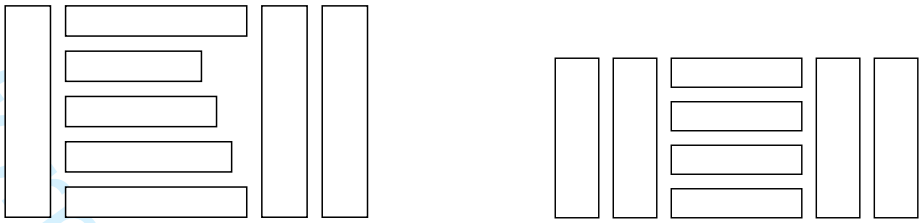
Prior work shows that bystanders share similar concerns but those concerns vary by context, such as their relationship with the SHD owner and the length of their stay. For instance, their degree of concern at a trusted friend's home may be lesser than their concern at a vacation rental (Yao, Basdeo, Mcdonough & Wang 2019).

2.2 SHD Users' Privacy Control Needs

Prior work has identified privacy control needs of users. One of the notable works that this paper builds on is the privacy control framework (PCF), which was derived from empirical user studies to identify what privacy control needs the users of smart home devices have (Chhetri & Motti 2022*d*).

The privacy control framework (PCF) consists of seven design factors of smart home privacy control design which contains 32 sub-factors and 215 user interface controls for privacy. The seven design factors of the PCF are data-related controls, transparency-related controls, centralized interface, device controls, multi-user controls, user support, and security controls (Chhetri & Motti 2022*d*). Figure 1a summarizes the design factors visually. In the figure, the vertical bars represent constructs that affect the factors in horizontal bars (Chhetri & Motti 2022*b*).

Data-related controls are the mostly desired controls regarding data collection, transmission, processing, and storage. Transparency-related controls provide information, policy, disclaimer, indicators, and notifications. Centralized interface provides a central way to manage smart home device controls. Device controls are hardware and software features that control the operation of the device or its capabilities, such as powering a device on or off. Multi-user controls allowing owners to manage multiple users of SHD, their preferences, and their data. User support controls provide training and do-it-yourself solutions to users. Security controls are controls regarding device security and preventing unauthorized access to the device (Chhetri & Motti 2022*d*).



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

Figure 1: Privacy Controls from Chhetri & Motti (2022*b*)

2.3 SHD Privacy Designs

A large body of research exists in the area of transparency-related controls. One popular approach that has received wide research attention is the idea of privacy labels. The concept of privacy labels can be useful to smart home apps. Examples of such work include research on online privacy labels (Kelley, Bresee, Cranor & Reeder 2009, Emami-Naeini, Agarwal, Cranor & Hibshi 2020), which has even recently been adopted by Apple[1] and Google[2] in their app stores. Other examples of work on privacy labels include privacy nutrition label (Kelley et al. 2009), GDPR-based privacy label for IoT devices OnLITE (Railean & Reinhardt 2020), and security and privacy label with device factors (Shen & Vervier 2019). Another approach that has been investigated regarding transparency-related controls is the design of user notifications and nudges (Murmann & Karegar 2021).

Furthermore, prior work has explored the design of *multi-user* controls. Zeng & Roesner (2019) developed and evaluated multi-user settings for a smart home app. In another paper, Feng et al. (2021) proposed a design space for privacy choices and use-case design of a privacy choice platform app, IOTAssistant.

Chhetri & Motti (2022*b*) translated the user requirements of smart home privacy controls into a prototype app that implemented the data-related privacy controls. They further evaluated the design with smart home users to find that the design met the user expectations of privacy controls but needed improvement in usability and user experience. The data-related privacy controls were based on user requirements and drawn from Chhetri & Motti (2022*d*): Opt-in (or out), Consent, Data collection, Storage, Usage, Sharing or selling, Monitor or view, and Delete. Figure 1b illustrates the data-related privacy controls.

3 Methods

We designed two prototype apps to implement the user requirements of data-related privacy controls. Then, we conducted user studies to evaluate the prototypes and gain insights into design improvements. For the evaluation of the apps, we used validated measures of usability, perceived information control, user satisfaction, and user intention to use. Fig. 2 visualizes our research approach.

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

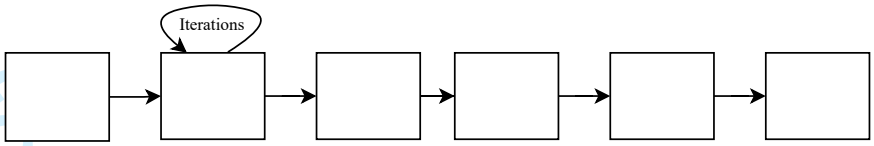


Figure 2: Research Approach

3.1 Prototype Design

We used Mockplus[3] to design interactive prototypes to implement the data-related privacy controls requirements of the PCF (See section 2.2). We followed iterative design process. We conducted a brainstorming session and a feedback session with multiple researchers and designers in our lab. The initial designs were reviewed and updated until final versions were reached to be used in evaluation studies.

We called the prototype MyCam. MyCam app is an app that allows users to control an indoor camera system and provides privacy settings and data dashboard. We evaluated two versions of MyCam app. MyCam1 was evaluated and the feedback from user studies was used to inform the design of MyCam2. User studies were also conducted to evaluate MyCam2.

The final iterations of both versions that were used in user studies consisted of three pages: MyCam Home, Privacy Settings, and Data Dashboard. MyCam Home was the first page of the app, which provided brief information on the app, a placeholder to view the camera footage and a button to navigate to the privacy settings page. The privacy settings were designed to be different in the two versions of the app. MyCam1 provided a list of over a dozen data-related privacy choices whereas MyCam2 provided three-tiered privacy presets. The data dashboard page, which remained the same in both versions provided a listing of users' data files, such as audio and video activity files, and options to delete the data files individually and all at once.

3.1.1 MyCam1: List of Privacy Controls

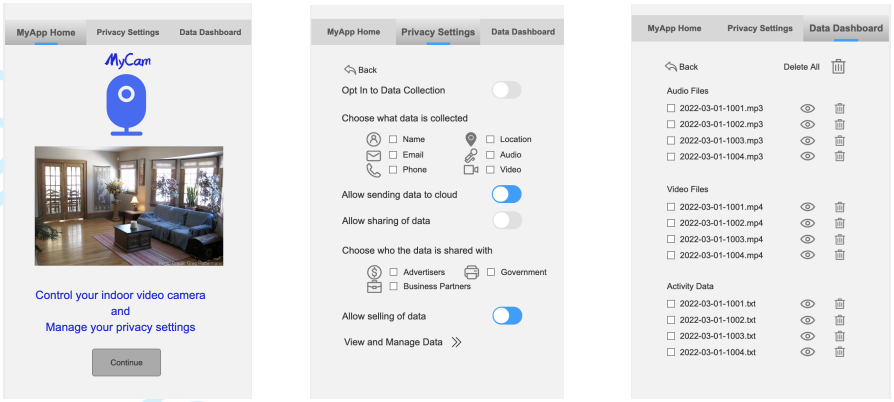
MyCam1 consisted of three pages: MyApp Home, Privacy Settings, and Data Dashboard. The privacy settings page consisted of data-related controls: opt-in to data collection, control what data type is collected, allow (or disallow) sending/sharing/selling of data, choose who data are shared with, and a link to data dashboard for viewing and managing data (See Fig. 3b). The data 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).

3.1.2 MyCam2: Tiered Preset Privacy Controls

The privacy settings page in MyCam2 was designed as tiered preset to allow less burden on users in managing their privacy. Three preset options were provided: High privacy, Medium privacy, and Low privacy.

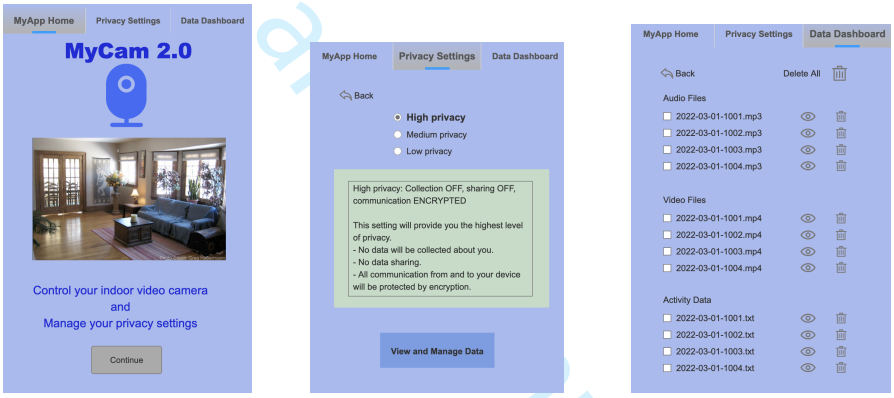
In the high privacy setting, no data will be collected about the user, no data will be shared, and all communication from and to the device will be protected

[3]www.mockplus.com



(a) Home page (b) Settings page (c) Data dashboard page

Figure 3: MyCam1 prototype app.



(a) Home page (b) Settings page (c) Data dashboard page

Figure 4: MyCam2 prototype app

by encryption. In the medium privacy setting, the device will collect user data (such as email address, location, and device name), but no data about user will be shared with anyone, and all communication from and to your device will be protected by encryption. Lastly, in the low privacy setting, the device will collect user data (such as email address, location, and device name), these data will be shared with third party (such as marketing partners, advertisers, and other parties), and no data will be protected by encryption.

The privacy settings page on the MyCam2 app was designed to display each of the preset configurations in details. A colored text box was displayed to provide the details as soon as the user made a selection of the presets. Lighter color choices were made for the text boxes. Red, yellow and green colors were used in the text boxes for low, medium, and high privacy settings respectively. Figure 5 shows the text boxes used in the prototype app.

(a) High privacy (b) Medium privacy (c) Low privacy

Figure 5: MyCam2 preset configurations explained to the users

3.2 Study Design

We evaluated MyCam1 through interviews (n=10) and a survey (n=105). We used the thematic analysis of the feedback of interviews to inform the design of MyCam2. The survey results were used to evaluate the usability, user experience, perceived information control, satisfaction, and intention to use. The preliminary findings from the survey and the findings of the interview which were used to inform the design of MyCam2 were published in Chhetri & Motti (2022*b*).

We evaluated MyCam2 through a survey (n=102). We compared the results to gain quantitative insights on how MyCam2 was evaluated over MyCam1 by survey participants.

The survey design for both MyCam1 and MyCam2 was consistent. The studies were approved by the Institutional Review Board of our host institution. The survey questionnaire was designed using Qualtrics[4] and deployed using Mechanical Turk[5], which is widely used by researchers to conduct security and privacy studies. We advertised the study as a survey that collects opinions about an app.

The survey initially presented the informed consent and a choice to agree to participate in the survey. If the participants agreed to participate, they received some screening questions. If they continued past the screening, they received information about one app condition (MyCam1 or MyCam2). Each participant was assigned to only one condition. They were then asked to perform a set of tasks in the app and report completion status. Following the app tasks, they received questions related to the measures of usability (SUS), user experience (UEQ), perceived information control, user satisfaction, and intention to use. They also received open-ended questions to report challenges, problems, and suggestions for improvement followed by demographic questions. Finally, we debriefed and thanked the participants.

3.3 Participants

We conducted a priori power analysis using G*Power 3.1 (Faul, Erdfelder, Lang & Buchner 2007) to determine the minimum sample size to compare the means of two independent groups. Results indicated a total sample size of 176 (88 per group) was required to achieve a power of 0.95 with $\alpha = 0.05$ and a medium effect size of $d = 0.5$.

[4]qualtrics.com
[5]mturk.com

Table 1: Participant Demographics (n=207)

		n	%
Gender:	Male	128	61.8%
	Female	79	38.2%
Age:	18-24 years	12	5.8%
	25-34 years	116	56%
	35-44 years	51	24.6%
	45-54 years	18	8.7%
	55+ years	10	4.8%
Employment	Full-time	194	93.7%
	Part-time	6	2.9%
	Other	7	3.4%
Education:	High school or less	24	11.6%
	Some college	9	4.3%
	Associate degree	8	3.9%
	Bachelor's degree	120	58.0%
	Masters or above	46	22.2%

We recruited 240 participants using the crowdwork platform Amazon Mechanital Turk (AMT). We used the following screening criteria: (a) Participants lived in the US (b) Participants completed at least 100 tasks in AMT (c) Participants had at least 95% approval ratings in prior AMT tasks, and (d) Participants reported using at least one smart home device. In the survey, participants performed given tasks in the app and provided their perceptions about the app. Participants were compensated with USD 1.50 for the survey, which had an average completion time of 7 minutes.

Among the responses collected, 33 were excluded from the analysis due to participants not answering attention check questions correctly, completing the survey in extremely low duration, and providing copy-paste or lined up answers.

Thus, 207 participants' survey responses were included in the analysis. Among them, 105 participants evaluated MyCam1 and 102 participants evaluated MyCam2. Table 1 shows the demographic breakdown of the participants.

The survey participants varied in age, gender, employment status, and education. The participants were mostly male (male 62%, female 38%), mostly young (18-24 years 6%, 25-34 years 56%, 35-44 years 24%, 45-54 years 9%, and 55+ years 5%), mostly educated (high school 12%, some college 4%, associate degree 4%, bachelor's degree 58%, and master's degree 22%), and mostly employed full-time (94%).

3.4 Measures and Data Analysis

All survey statements were taken from previously validated scales from literature. We measured user experience through the 26-item User Experience Questionnaire (UEQ) scale (Schrepp, Hinderks & Thomaschewski 2017). We measured usability using the 10-item System Usability Scale (SUS) scale (5-point Likert) (Brooke 1996). We measured user satisfaction using a 4-item scale adapted from Seddon & Kiew (1996). We adapted perceived information con-

Table 2: Descriptive statistics for system usability (SUS), perceived information control (PCTL), user satisfaction (SAT), and behavioral intention to use (BI).

	App	N	Mean	SE	SD	Minimum	Maximum
SUS	MyCam1	105	62.50	1.376	14.10	37.50	100.00
	MyCam2	102	72.08	1.124	11.36	50.00	100.00
PCTL	MyCam1	105	4.37	0.125	1.28	1.00	6.60
	MyCam2	102	4.36	0.115	1.16	1.60	6.60
SAT	MyCam1	105	5.14	0.143	1.46	1.25	7.00
	MyCam2	102	5.22	0.117	1.18	2.00	7.00
BI	MyCam1	105	5.40	0.125	1.28	1.67	7.00
	MyCam2	102	5.55	0.111	1.12	1.67	7.00

trol scale (5 items) from Xu (2007) and intention-to-use scale (3 items) from Venkatesh, Morris, Davis & Davis (2003). Unless otherwise noted, we designed all items as 7-point Likert items.

We performed qualitative thematic analysis on interview data and quantitative analyses on survey data. We used descriptive statistics, t-tests, ANOVA, and correlation to gain insights about MyCam1 and MyCam2. As descibed above in Section 3.4, only 207 responses were included in the dataset.

4 Results

In this section, we present the results of our data analysis.

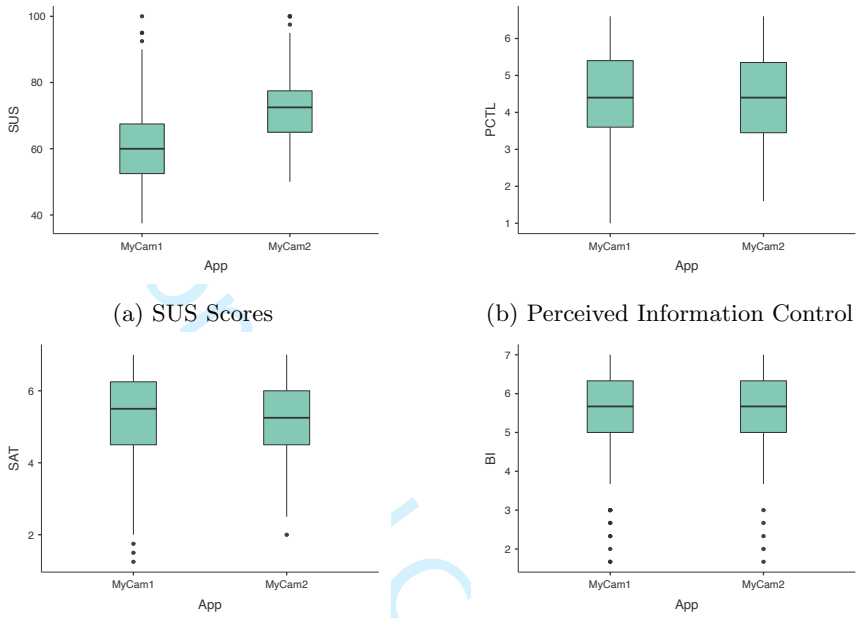
4.1 Usability: SUS Scores

MyCam1 received an aggregate SUS score of 62.50 (Min=37.5, Max=100). However, MyCam2 received a better SUS aggregate score of 72.08 (Min=50, Max=100). Table 2 lists the descriptive statistics for SUS scores. Figure 6a shows the box plots of aggregate SUS scores for both MyCam1 and MyCam2. Although MyCam2 clearly has a higher SUS score, we tested whether the difference is statistically significant through independent samples t-test and analyses of variance (ANOVA).

As shown in Table 3, Student's t-test showed statistical significance in the difference of SUS scores between MyCam1 and MyCam2 ($t(205) = -5.38, p < .001$). Similarly, an ANOVA test showed that there was significant difference in the SUS scores between the two versions ($F(1, 205) = 28.9, p < .001, \eta^2 = 0.12$). These tests confirmed that MyCam2 was perceived by the survey participants as significantly more usable than MyCam1.

4.2 User Experience

The UEQ scale consists of 26 items that measure six dimensions of user experience: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty (Schrepp et al. 2017). Mean score below -0.8 is considered negative, between -0.8 and 0.8 is neutral, and above 0.8 is considered positive evaluation.



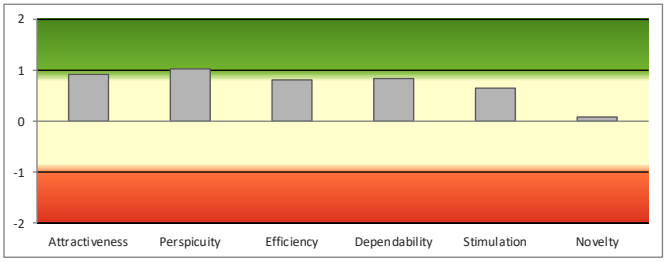
(a) SUS Scores (b) Perceived Information Control

(c) Satisfaction (d) Intention to Use

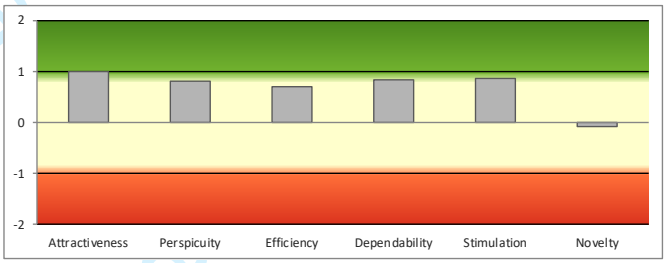
Figure 6: Box plots showing the scores of SUS, PCTL, SAT, and BI

Table 3: Independent samples t-test results

	Statistic	**df**	**p**
SUS	-5.3753	205	<.001*
PCTL	0.0175	205	0.507
SAT	-0.4590	205	0.323
BI	-0.8927	205	0.187



(a) UEQ scores for MyCam1



(b) UEQ scores for MyCam2

Figure 7: Results showing scores for the six dimensions of the UEQ scale.

MyCam1 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. 7a). Similarly, MyCam2 was evaluated *positive* for attractiveness (Mean μ =0.99 and Variance σ^2=1.21), perspicuity (μ=0.81, σ^2=1.48), dependability (μ=0.83, σ^2=1.40), and stimulation (μ=0.85, σ^2=1.36). It was evaluated *neutral* for efficiency (μ=0.70, σ^2=1.14) and novelty (μ=0.07, σ^2=0.73) (see Fig. 7b).

The independent samples t-test showed no significant difference between the scores of the six user experience dimensions in MyCam1 and MyCam2.

4.3 Perceived Information Control

Survey participants found MyCam's perceived information control to be above average in both conditions: MyCam1 (μ=4.37, σ=1.28) and MyCam2 (μ=4.36, σ=1.16). The results of the independent samples t-test showed no significant difference between the perceived information control of MyCam1 and MyCam2. Cronbach's alpha showed that the scale demonstrated good internal consistency (α=0.88) (See Table 3).

4.4 User Satisfaction

The satisfaction scale scores of survey participants for MyCam were good in both conditions: MyCam1 (μ=5.14, σ=1.46) and MyCam2 (μ=5.22, σ=1.18). Although the mean of MyCam2 is higher than that of MyCam1, the results of the independent samples t-test showed no significant difference between the user satisfaction scores of MyCam1 and MyCam2. Cronbach's alpha showed that the scale demonstrated good internal consistency (α=0.91).

Table 4: Correlation matrix for system usability (SUS), perceived information control (PCTL), user satisfaction (SAT), and behavioral intention to use (BI). Asterisks (***) represent statistical significance, $p < .001$.

		SUS		SAT		PCTL		BI
SUS	Pearson's r	—						
	p-value	—						
SAT	Pearson's r	0.228	***	—				
	p-value	<.001		—				
PCTL	Pearson's r	-0.018		0.441	***	—		
	p-value	0.802		<.001		—		
BI	Pearson's r	0.353	***	0.669	***	0.285	***	—
	p-value	<.001		<.001		<.001		—

4.5 Intention to Use

Survey participants reported a high intention to use a privacy control system similar to MyCam. The 3-item intention-to-use scale was rated very good for both conditions: MyCam1 (μ=5.40, σ=1.28) and MyCam2 (μ=5.55, σ=1.12). Although the mean of MyCam2 is higher than that of MyCam1, the results of the independent samples t-test showed no significant difference between the user satisfaction scores of MyCam1 and MyCam2. Cronbach's alpha showed that the scale demonstrated good internal consistency (α=0.91).

4.6 Correlation Among the Measures

The Pearson's correlation coefficient (r) showed that the intention to use was correlated positively with perceived information control ($r = 0.29$), user satisfaction ($r = 0.67$), and usability ($r = 0.35$) at the significance level of $p < .001$. Similarly, perceived information control ($r = 0.44$) and usability ($r = 0.22$) were positively correlated with satisfaction at the same significance level ($p < .001$). Table 4 shows the correlation matrix for all four measures.

5 Discussion

The findings of our between-subjects prototype evaluation of the list condition and the presets condition showed that the presets condition was perceived to be more usable. However, there was no evidence that either condition was perceived to provide more control, satisfaction, or intention to use.

Based on the findings, we discuss the following implications to privacy controls design.

5.1 Users desire usable controls to manage their privacy

Privacy controls are a widely studied technique to provide users options to manage their privacy. However, the privacy controls need to be easy for users to find, understand, and use. Usability is a theme that has emerged in the literature

on user-centric privacy controls (Yao, Basdeo, Kaushik & Wang 2019*b*, Chhetri & Motti 2022*d*).

In our experiments, the user intention to use correlated positively with usability ($Pearson\ r = 0.35,\ p < .001$) and user satisfaction ($Pearson\ r = 0.67,\ p < .001$). User satisfaction correlated positively with usability ($Pearson\ r = 0.23,\ p < .001$). This means that users are more likely to use the privacy settings when they are more usable.

5.2 Presets or tiered settings can reduce burden and are perceived by users to be more usable

In the list condition, users have the burden of picking all the settings by themselves. In contrast, privacy presets allow the users to switch between pre-configured privacy settings (Jin, Guo, Roychoudhury, Yao, Kumar, Agarwal & Hong 2022). Privacy presets reduce the burden on users making the management of privacy less overwhelming by allowing users to pick a range of privacy controls through one click or slider bar (Chhetri 2022). In Chhetri & Motti (2022*b*), the authors made a recommendation of privacy presets, which were implemented in MyCam2. The user evaluation showed that users perceived the usability of the privacy presets significantly higher than the list condition. Thus, privacy presets are the more usable option that can be provided to users in smart home apps to manage privacy with ease.

While implementing the privacy presets, each pre-configured privacy setting needs to be explained clearly to the users so that the users understand what privacy controls are set with each preset configuration. For example, in the presets condition used in our experiment, we explained briefly and then in detail about data collection, sharing, and protection by encryption for each preset. This allowed the users to understand what data will be collected, who the data will be shared with, and whether the data will be encrypted.

5.3 Presets should not replace but complement detailed controls

While most users in our experiment preferred the privacy presets, some users mentioned they need fine grained controls as opposed to presets. For example, survey participant, P112, noted *"I need more controls."* While most users may seek the convenience of managing privacy provided by presents, others may seek and benefit from the fine-grained, detailed list of privacy controls.

Designing the presets along with options for detailed privacy controls (for those users who prefer) will allow all users to get what they desire, regardless of whether they prefer presets or list. Presets could be presented first due to their higher usability and then the list could be presented next through a click or an expand button.

5.4 Limitations and Future Work

Online studies can present some limitations. The common pitfalls of online studies are the lack of control of participants or the experiment environment, lack of the researcher presence to assist participants in the event of technical failures, and external distractions that can hinder participant motivation to

complete the experiment with quality responses (Gagné & Franzen 2021). Thus, it is necessary to use some quality controls in online studies.

In our experiment, we used some quality controls to minimize the effects of these pitfalls. We used pre-screening criteria to screen out participants. We used the built-in qualification features of Mechanical Turk to recruit participants that were located only in the United States, had completed at least 100 tasks with Mechanical Turk, and had an approval rating of at least 95% in Mechanical Turk. In addition, we tried to keep the survey length as short as possible to reduce participant fatigue and loss of motivation.

To minimize the effects of the online studies' pitfalls, we also added two attention check questions in the survey. All responses with incorrect answers for one or both of the attention check questions were excluded from data analyses. Additionally, to ensure only quality responses were analyzed, we inspected the responses manually and excluded responses that appeared to be illegible, copy-paste, or lined-up responses. We also excluded survey responses that were completed in a very short time-span in which we felt the respondent might not have read the questions well.

Another limitation of study is that our sample is not US representative and includes more technology friendly, educated, and young participants. However, despite these limitations, our sample represents the current smart home user population and Mechanical Turk population's perceptions are US representative as shown by recent literature (Tang, Birrell & Lerner 2022). Future studies could target a US representative population.

In our experiment, we limited the participant location to the United States. Hence, the results may not be generalizable to non-US populations. Thus, future studies could investigate non-US participants.

For future work, another area that could be investigated is the presentation of the presets and list conditions based on participant preferences. For instance, a set of questions could be asked to determine whether a participant preferred the list or presents before the appropriate condition is presented. This could allow the designers to present the privacy settings design based on the users' preferences.

6 Conclusion

We proposed two designs of privacy settings for home IoT devices based on user requirements of data-related privacy controls from prior work. We found that the privacy presets were perceived to be more usable than than a list of controls. Hence, smart home designers should consider providing well-explained privacy presets for users to manage their privacy while using smart home devices. The designs presented in this article will be useful to smart home designers seeking to provide usable privacy settings to their users. By providing usable privacy settings to smart home users, smart home designers will address the privacy concerns of smart home users while allowing the benefits of home automation and the related convenience. The privacy designs presented in this paper will serve the privacy designs of not only smart home devices but IoT devices at large.

Acknowledgement

Removed for blind review

References

Brooke, J. (1996), 'SUS: A 'quick and dirty' usability scale', *Usability evaluation in industry* pp. 189–194.

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

Chhetri, C. (2022), Designing for Privacy in Smart Home Devices: Vulnerabilities, Concerns and User-Centric Privacy Controls, PhD dissertation, George Mason University.

Chhetri, C. & Motti, V. (2020), Identifying vulnerabilities in security and privacy of smart home devices, *in* 'National Cyber Summit', Springer, pp. 211–231.

Chhetri, C. & Motti, V. (2022*a*), Privacy concerns about smart home devices: A comparative analysis between non-users and users, *in* 'Human Factors in Cybersecurity', Vol. 53, AHFE International, AHFE Open Access, pp. 102–110.
URL: *https://doi.org/10.54941/ahfe1002207*

Chhetri, C. & Motti, V. G. (2022*b*), Designing and evaluating a prototype for data-related privacy controls in a smart home, *in* N. Clarke & S. Furnell, eds, 'Human Aspects of Information Security and Assurance', Springer International Publishing, Cham, pp. 240–250.
URL: *https://doi.org/10.1007/978-3-031-12172-2*$_1$9

Chhetri, C. & Motti, V. G. (2022*c*), '"I mute my echo when I talk politics": Connecting smart home device users' concerns to privacy harms taxonomy', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* **66**(1).

Chhetri, C. & Motti, V. G. (2022*d*), 'User centric privacy controls for smart homes', *Proceedings of the ACM on Human-Computer Interaction* **6**(CSCW2).
URL: *https://doi.org/10.1145/3555769*

Emami-Naeini, P. (2021), Privacy and security nutrition labels to inform IoT consumers, USENIX Association.

Emami-Naeini, P., Agarwal, Y., Cranor, L. F. & Hibshi, H. (2020), Ask the experts: What should be on an iot privacy and security label?, *in* '2020 IEEE Symposium on Security and Privacy (SP)', IEEE, pp. 447–464.

Faul, F., Erdfelder, E., Lang, A.-G. & Buchner, A. (2007), 'G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences', *Behavior research methods* **39**(2), 175–191.

Feng, Y., Yao, Y. & Sadeh, N. (2021), A design space for privacy choices: Towards meaningful privacy control in the internet of things, *in* 'Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems', pp. 1–16.

Gagné, N. & Franzen, L. (2021), 'How to run behavioural experiments online: best practice suggestions for cognitive psychology and neuroscience'.

Haney, J. M., Furman, S. M. & Acar, Y. (2020), Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges, *in* A. Moallem, ed., 'Lecture Notes in Computer Science', Vol. 12210 LNCS, Springer International Publishing, Cham, pp. 393–411.

Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y. & Hong, J. I. (2022), Exploring the needs of users for supporting privacy-protective behaviors in smart homes, *in* 'CHI Conference on Human Factors in Computing Systems', pp. 1–19.

Kelley, P. G., Bresee, J., Cranor, L. F. & Reeder, R. W. (2009), A "nutrition label" for privacy, *in* 'Proceedings of 5th Symposium on Usable Privacy and Security', pp. 1–12.

Murmann, P. & Karegar, F. (2021), 'From design requirements to effective privacy notifications: empowering users of online services to make informed decisions', *International Journal of Human–Computer Interaction* **37**(19), 1823–1848.

Railean, A. & Reinhardt, D. (2020), OnLITE: On-line label for IoT transparency enhancement, *in* 'Nordic Conference on Secure IT Systems', Springer, pp. 229–245.

Schrepp, M., Hinderks, A. & Thomaschewski, J. (2017), 'Design and evaluation of a short version of the user experience questionnaire (ueq-s)', *International Journal of Interactive Multimedia and Artificial Intelligence, 4 (6), 103-108.* .

Seddon, P. & Kiew, M.-Y. (1996), 'A partial test and development of delone and mclean's model of is success', *Australasian Journal of Information Systems* **4**(1).

Shen, Y. & Vervier, P.-A. (2019), Iot security and privacy labels, *in* 'Annual Privacy Forum', Springer, pp. 136–147.

Tang, J., Birrell, E. & Lerner, A. (2022), 'How well do my results generalize now? the external validity of online privacy and security surveys', *arXiv preprint arXiv:2202.14036* .

Taylor, R., Baron, D. & Schmidt, D. (2015), The world in 2025 - predictions for the next ten years, *in* '2015 10th International Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT)', pp. 192–195.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003), 'User acceptance of information technology: Toward a unified view', *MIS quarterly* pp. 425–478.

Xu, H. (2007), The effects of self-construal and perceived control on privacy concerns, *in* 'Twenty Eighth International Conference on Information Systems'.

Yang, H., Lee, W. & Lee, H. (2018), 'Iot smart home adoption: the importance of proper level automation', *Journal of Sensors* **2018**.

Yao, Y., Basdeo, J. R., Kaushik, S. & Wang, Y. (2019*a*), 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', CHI '19, ACM, New York, NY, USA, pp. 198:1–198:12.

Yao, Y., Basdeo, J. R., Kaushik, S. & Wang, Y. (2019*b*), 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. 1–12.

Yao, Y., Basdeo, J. R., Mcdonough, O. R. & Wang, Y. (2019), 'Privacy Perceptions and Designs of Bystanders in Smart Homes', *Proc. ACM Hum.-Comput. Interact.* **3**(CSCW).
URL: *https://doi.org/10.1145/3359161*

Zeng, E. & Roesner, F. (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)', pp. 159–176.

A Survey Questions

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

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

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

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

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

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

   Please use the app below and share your feedback. [Show app] *(Task questions were inspired by (Kelley et al. 2009))*

- TASK1 Click Continue on the MyCam Home page to go the privacy settings page. Did this work for you?
- BROWSEAPP The privacy settings page gives you options to manage your data privacy in three tiers: High privacy, Medium privacy, and Low privacy. For each setting you pick, you are provided with details of what is obtained from each setting. We will now ask you to perform the following tasks in the app.
- TASK2 Click on High privacy and read the description. Did this work for you?
- TASK3 Click on Medium privacy and read the description. Did this work for you?
- TASK4 Click on Low privacy and read the description. Did this work for you?
- TASK5 Now that you have read the descriptions of all three settings. If this were an actual smart camera in your living room, which privacy setting would you have picked? [Options: High privacy, Medium privacy, and Low privacy]
- TASK6 Go to the MyCam Home page. Did this work for you?
- IMPROVE Feel free to browse through the app. How can we improve the app?

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

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

8. *(User Experience Questionnaire (Schrepp et al. 2017), 7 point scale, -3 to +3)* For the assessment of the product, please fill out the following questionnaire. The questionnaire consists of pairs of contrasting attributes that may apply to the product. The circles between the attributes represent gradations between the opposites. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

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

9. *(System Usability Scale Questions (Brooke 1996), Likert Options: Strongly Disagree (1) to Strongly Agree (5))*

   - I think that I would like to use this system frequently
   - I found the system unnecessarily complex
   - I thought the system was easy to use
   - I think that I would need the support of a technical person to be able to use this system
   - I found the various functions in this system were well integrated

- I thought there was too much inconsistency in this system
- I would imagine that most people would learn to use this system very quickly
- I found the system very cumbersome to use
- I felt very confident using the system
- I needed to learn a lot of things before I could get going with this system

10. *(Attention Check Questions)*
    - ATT1 How likely are you to purchase this app? Please select neither for this question.
    - ATT2 Do you agree that this app is named well? Please select agree for this question.

    (Perceived Information Control(Xu 2007), Likert Scale 1-7)

11. How much control do you feel you have over the amount of your personal information collected by MyCam?
12. With MyCam, how much control do you feel you have over who can get access to your personal information ?
13. How much control do you feel you have over your personal information that has been released to MyCam?
14. How much control do you feel you have over how your personal information is being used by MyCam?
15. Overall, how much in control do you feel you have over your personal information provided to MyCam?

    (User Satisfaction (Seddon & Kiew 1996) Likert Scale 1-7)

    Please rate your overall satisfaction with MyCam.

16. How adequately do you feel the MyCam **meets** your privacy needs ?
17. How **efficient** is MyCam?
18. How **effective** is MyCam?
19. Overall, how **satisfied** are you with MyCam?

    (Behavioral Intention to Use), Likert 1-7, Adapted and modified from (Venkatesh et al. 2003)

20. How likely are you to use MyCam's privacy settings if available to you?
21. How likely are you to recommend others to use MyCam's privacy settings?
22. How likely are you to use privacy settings of other apps in the future?