Users, Smart Homes, and Digital Assistants: Impact of Technology Experience and Adoption

Michael Shlega, Sana Maqsood, and Sonia Chiasson

Carleton University, Ottawa ON, Canada
michaelshlega@cmail.carleton.ca

Abstract. Smart Homes are becoming the norm, with manufacturers including connectivity within many home electronics and appliances by default; and these are often controllable through voice-activated digital assistants. Using an online survey of 212 participants, we explore how users' self-reported Technology Experience relates to their perceptions of the data protection done by Smart Home devices, their security and privacy concerns towards Smart Home digital assistants, and their likelihood of adopting mitigation techniques for digital assistants. We found no relation between self-reported Technology Experience and our dependent variables. We also compared adopters to non-adopters to explore differences between the two groups. We found that adopters of Smart Home technology had a higher level of perceived data protection and less overall concern towards the assistants.

Keywords: Usable security · Smart Homes · Digital assistants · Technology Adoption · User study · Survey

1 Introduction[1]

Recent statistics suggest that there are currently over 258 million "Smart Homes" worldwide [18]. According to estimates, 40% of US households have adopted Smart Home technology [19]. Even more popular, there are an estimated 4.2 billion voice digital assistants deployed worldwide [17]. Smart Home devices are now commonly combined with digital assistants to provide convenience and usability for consumers.

Despite these trends, some researchers project that the Smart Homes market is stalling, partly because of resistance in adoption due to perceived privacy and security risks [9]. Further research carried out by Barbossa et al. categorized factors that impact user adoption into blockers and motivators [3], with motivators promoting adoption and blockers impeding adoption. Of the blockers found, the more impactful ones can be grouped into user concerns and user perceptions.

Within this paper, we use the following definitions.

Smart Homes: Smart Homes are equipped with systems and appliances that can be operated remotely using a computer or mobile phone. Examples of Smart Homes are homes that include appliances/systems such as thermostats, fridges, locks, light switches, TVs, sound systems, or security cameras that can be controlled by the user through a computer or phone.

[1] Authors' copy. Published at HCI International (HCII) 2022

Digital Assistants: Digital assistants are digital AI, within Smart Home technology, meant to assist a user by carrying out voice commands. When this paper talks about digital assistants, it refers to devices such as the Amazon Alexa, Google Assistant, SmartThings, Siri, and other voice-controlled assistants. These assistants can perform tasks such as search the web, control other smart devices, play music, set timers, check the weather, make phone calls, or run other voice-controlled apps.

As discussed in Section 2, researchers have previously investigated end user perceptions of data protection of Smart Home devices, end user concerns, and the mitigation techniques users take to protect themselves from the risks facing them. Our paper extend this work by analyzing the differences between users who have more Technology Experience and those who do not. To our knowledge, this analysis has not been done before and may provide insight into why users differ on their perceptions, concerns, and mitigation methods. Thus, our first research question is:

RQ1: *What is the relationship between users' self-reported Technology Experience and users' perceived protection of data by Smart Home devices, their security and privacy concerns towards Smart Home digital assistants, and their mitigation technique implementation decisions?*

Prior research (e.g., [25, 8, 20, 1, 7, 2]) on users' perceptions and concerns towards Smart Homes has been primarily focused on users who have already adopted Smart Home devices. This leaves out a significant proportion of users: those who have chosen to avoid these types of devices. Investigating their perspective will enable a more complete understanding of the differences between adopters and non-adopters and the range of perceptions and concerns towards Smart Home digital assistants. Our second research question is:

RQ2: *What are the differences between adopters and non-adopters of Smart Homes in terms of users' Technology Experience, their perceived protection of data by Smart Home devices as well as their security and privacy concerns towards Smart Home digital assistants?*

To explore our research questions, we conducted an online survey with 212 participants. Our analysis revealed no relationship between the Technology Experience of respondents and (i) their perception of data protection with respect to Smart Home devices, (ii) the privacy and security concerns users harbor about Smart Home digital assistants, (iii) nor users' protection implementation strategies. When comparing adopters to non-adopters, we found that adopters had significantly more positive views on data protection in Smart Homes, had fewer privacy and security concerns about Smart Home digital assistants, and had higher level of Technology Experience. Furthermore, we found that adopters of Smart Homes rarely implemented proposed mitigation measures that would help protect their privacy or security.

2 Background

For context, we review recent research on Smart Homes and Smart Home digital assistants related to user perceptions, concerns, and mitigation strategies, organized by relevance to our two Research Questions.

2.1 Effect of Technology Experience

End User Perceived Protection of Data Based on recent research, users' perceptions on data protection by Smart Homes and Smart Home digital assistants vary considerably. Georgiev et al. [7] showed that users had differing beliefs about how well Smart Home devices protect users' private data. The authors specifically noted that participants had different levels of technology understanding, but this was not explicitly assessed as a factor. Other papers [22, 1, 11, 13, 23, 25] have similarly noted differences in technology understanding in their participant samples, however to our knowledge, none have explicitly tested its relationship to users' assessment of the perceived data protection offered by Smart Homes.

End User Concerns Users' concerns relating to Smart Home devices have also been investigated. A qualitative interview study with 15 adopters of Smart Homes found that participants exhibited a varied understanding of the Smart Home threat model and did not share a common set of concerns [24]. The authors noted that participants' described threat models often depended on the sophistication of their technical mental models. Moreover, the concerns held by users were said to be different from the concerns held by security experts [24]. Others have also noted a potential correlation between users' degree of technical understanding and concern levels [5, 11, 6, 23] though none explicitly tested for it. The literature on concerns has highlighted several common types of concern shared amongst users, with privacy and security being the most prominent categories [24, 5, 11, 6, 23]. It has been demonstrated that users who originally had few concerns showed increased concern immediately after being educated on the security and privacy issues arising from Smart Home devices, suggesting a potential connection between knowledge and the concerns of users [14]. Together, these studies indicate a potential link between the technical understanding of users and their concern level, however, no studies have directly investigated this relationship.

End User Mitigations Users tend to adopt a variety of mitigation strategies, with no clear pattern emerging [8, 11, 24, 20]. Mitigation strategies adopted by users have ranged from covering the microphone of a Smart Home digital assistant, to moving the Smart Home to a less sensitive room, to deleting Smart Home collected data. Zeng et al.'s interview study, mentioned above, found that users' understanding of the Smart Home threat model influenced their mitigation responses, however, it was not determined if a relationship exists between how advanced a users' mental model is and their likelihood of implementing a mitigation technique. Furthermore, Tabassum et al. [20] found that participants who had more advanced mental models showed more awareness about the mitigation strategies available for the Smart Home, yet it was unclear if this awareness led to higher likelihood of using mitigation strategies. Other academic work investigating mitigation strategies has suggested a link between *awareness* of mitigation strategies and users' overall understanding of Smart Homes, but has not determined whether this awareness leads users to adopt mitigation strategies [8, 11, 24, 20].

2.2 Comparison of Adopters and Non-Adopters

End User Perceived Protection of Data Previous research has primarily analyzed perceptions of Smart Home data protection from the perspective of current users of Smart Home devices, but few studies have explored the perceptions of non-adopters.

One notable exception is a recent survey conducted by Barbossa et al. [3] which investigated both adopters and non-adopters, looking at their decision-making process for adopting or not adopting Smart Home devices. They suggest that user perceptions can be categorized into 'motivators' and 'blockers' of adoption. Participants who had more blockers, or had more highly weighed blockers, such as privacy or security relating towards their personal data, were less likely to adopt Smart Home technologies.

Similarly, Lau et al. [11] analyzed both adopters and non-adopters in an interview study with 17 participants, where they found motivators for adoption such as perceived convenience, and non-motivators for adoption, such as perceived privacy and security concerns relating to their personal data.

Most other academic research in this area is primarily qualitative and has also mainly targeted adopters' of Smart Home technologies [24, 25, 8, 20, 5, 1, 12, 6, 7, 15].

End User Concerns End user concerns have also been primarily investigated from the adopters' point of view. A number of studies have examined the concerns held by adopters and demonstrated that adopters of Smart Home technology generally hold disparate concerns [24, 25, 8, 20, 5, 1, 6, 7]. Several studies have suggested that adopters' concerns about Smart Home devices may depend on the sophistication of their technical mental models of Smart Homes [24, 11]. Most often, research has demonstrated that adopters' are primarily worried about privacy and security; however, this has been shown to not necessarily be a result of their knowledge of the risks, but rather their awareness of media reports surrounding privacy breaches or other Smart Home security violations [6, 11, 26, 20]

2.3 Research Gap

While research has suggested a likely link between technical literacy and a user's perception and usage of Smart Home technology, this relationship has not been explicitly explored. Furthermore, most research has focused on adopters and this may underreport the prevalence of concerns relating to Smart Home technologies.

3 Methodology

Our study was reviewed and cleared by our institution's ethics review board. From November 2020 until April 2021, we conducted an online survey with participants to determine their: (1) Level of Technology Experience; (2) Concerns related to Smart Homes digital assistants; (3) Perceived protection of data by Smart Home devices; (4) Security and privacy behaviors relating to digital assistants within Smart Homes. We use this data to address our two research questions.

For this study, we define *Technology Experience* as an aggregate measure of users' understanding of various aspect of cybersecurity, their level of comfort and experience with using internet technology, their familiarity with privacy and security options online, and their education/work experience in the field.

3.1 Recruitment

Participation was open to anyone over 18 years of age who could complete a survey in English. Recruitment material was distributed through word of mouth, online research study groups, and the survey distribution site Survey Circle[2]. We also distributed our study through the online recruitment site Prolific [3], which is a crowd sourcing platform specifically meant for research studies. 250 participants (89 through Prolific, and 161 through other means) responded to the survey which took on average 10 minutes to complete. We excluded data from 38 participants because they did not press the final 'submit responses' button indicating their consent, had obvious patterns in their answers (e.g., {1,2,3,4,5} or {1,1,1,1,}). After cleaning the data, we had 212 valid responses. Participants who completed the survey on Prolific were paid £1.43. Participants who were recruited through other avenues were offered the chance to enter a raffle at the end of the survey for one of two $50 Amazon gift cards.

3.2 Participants

Participants' were between 18-70 years old; 43% identified as men, 55% women, 1% non-binary, and the remaining preferred not to say. With regards to education, 12% had completed up to high school, 5% had completed trade/poly-technical training, 28% had some undergrad (College/University), 27% finished undergrad, 14% some graduate school (e.g., Masters, PhD, Medical), and 14% completed graduate school. Geographically, 41% of participants resided in North America, 48% in Europe, 5% in Asia, and the rest were spread among the Middle East, Southern Africa, and Australia.

We asked participants whether they had adopted Smart Home technologies in their home: 49% (N=103) of participants were *adopters*, and 51% (N=109) were *non-adopters*. Of the adopters, 55 used Google devices, 43 used Amazon devices, and others used Apple (37), Samsung (17), and Microsoft (15) devices. A few (13) used brands not included on our list. Participants could select more than one option. With regards to security and privacy, 73 out of 103 adopters (74%) and 88 out of 109 non-adopters (81%) had previously encountered a privacy breach of their data.

3.3 Survey

We hosted the survey on the online survey platform Qualtrics[4]. The survey (available in Appendix A) consisted of 41 questions, including two definition confirmation questions. Prior to starting the survey questions, participants were informed that the term "digital assistant" refers to digital assistants that are specifically within Smart Homes. Participants were then provided definitions for 'Smart Homes' and 'Digital Assistants'

[2] https://www.surveycircle.com/en/
[3] https://www.prolific.co/
[4] https://www.qualtrics.com/

to ensure that all respondent had a uniform understanding. The terms were described as follows:

This survey applies to *digital assistants* within *Smart Homes*

Smart Homes: Smart Homes are equipped with systems and appliances that can be operated remotely using a computer or mobile phone. Examples of Smart Homes are homes that include appliances/systems such as thermostats, fridges, locks, light switches, TVs, sound systems, or security cameras that can be controlled by the user through a computer or phone.

Digital Assistants: Digital assistants are digital AI meant to assist a user by carrying out voice commands. When this survey talks about digital assistants, it refers to devices such as the Amazon Alexa, Google Assistant, SmartThings, Siri, and other voice-controlled assistants. These assistants can perform tasks such as search the web, control other smart devices, play music, set timers, check the weather, make phone calls, or run other voice-controlled apps.

Following these definitions, two attention questions were posed: one asked participants to identify Smart Home technologies from a given list, and the other asked participants to identify examples of digital assistants. Participants had to correctly answer these two questions to proceed to the remainder of the survey. Those who failed could re-read the definitions and re-attempt the attention check questions until correct.

The remaining 43 questions consisted of 22 five-point Likert scale questions with two extra options for not understanding the question, or not knowing the answer. The remaining questions consisted of yes/no questions, questions with matrix table rankings, and questions with multiple choice answers. Our survey asked questions within the following five categories:

Understanding Definitions (2 Questions): Questions to double check participants' understanding of the provided definitions.

Demographics (8 questions): We asked about participants' age, education, gender, geographic location, work experience in cyber security, and the adoption of Smart Homes technology in their homes.

Understanding of data collection (3 questions): We asked participants' perceptions of data collection practices on Smart Home devices.

Perceived protection of data by Smart Home devices (2 questions): Participants were asked their views on Smart Home data collection and their trust of companies holding user data.

Security and Privacy Concerns (10 questions): Participants ranked their level of concern for a set of privacy and security risks. The questions were modeled off claims used by Deursen et al. [21] which are based on truth statements ('Very true of me', 'Not at all true of me', 'Not very true of me', etc.). Deursen et al. showed that the wording of this scale led to objective responses from participants. We included additional options for not understanding the question and being unsure of an answer.

Experience with Technology (15 questions): We assessed participants' comfort and Experience with technology and cybersecurity. Four questions were based on the Internet Skills Scales test [21] which analyzed the five basic categories of internet skills: navigational, operational, social, creative, and mobile. Of these five skills, the operation and information navigation skills were most relevant to our study. The remaining 11 questions were devised by us to analyze Technology Experience by asking the participants to identify their knowledge level about various aspect of cybersecurity, familiarity with privacy and security options online, and their education/work experience in the field.

Security and Privacy Behaviors (3 questions): Participants who had adopted Smart Home technology were further prompted to identify whether they used certain mitigation techniques to minimize the risks associated with a Smart Home digital assistant. The techniques provided on the survey were based on multiple studies which had identified various common mitigation techniques that users took to defend themselves from risk [8, 24, 23]. We asked about the three most used strategies. These mitigation techniques were related to security and privacy as well as personal data management.

Table 1. Internal consistency across the various scales used.

Reliability Statistics

Scale Category	Chronbach's Alpha	Number of Items
Technology Experience	0.821	15
Privacy and Security Concerns	0.896	10
Perceived Protection of Data	0.708	2

We analyzed the inter-reliability of our scales (Table 1) to ensure the survey questions were assessing similar concepts in their respective categories, and found acceptable levels of agreement for all three categories.

Table 2. Statistical analysis of participants' perceived protection of data, protective strategies, and security and privacy concerns across two factors: Experience and adoption of Smart Home devices. Bold and * indicates statistically significant result at $p < .05$.

	Factor	
Measure	**Experience**	**Adoption**
Perceived Protection of Data	(r = -.006, p = .933)	**(t (205) = -3.63, p = .001)***
Protective strategies (only asked of adopters)	(r = -.182, p = .65)	—
Concerns	(F = 0.412, p = .522)	**(U = 7034, p = .00005)***
Experience	—	**(t (210) = 2.253, p = 0.025)***

4 Results

We provide an overview of participants' understanding of data collection practices on Smart Home devices, and then analyze the survey data to answer our two research questions:

RQ1: What is the relationship between users' self-reported Technology Experience and users' perceived protection of data by Smart Home devices, their security and privacy concerns towards Smart Home digital assistants, and their mitigation technique implementation decisions?

RQ2: What are the differences between adopters and non-adopters of Smart Homes in terms of users' Technology Experience, their perceived protection of data by Smart Home devices as well as their security and privacy concerns towards Smart Home digital assistants?

A summary of the inferential statistics results discussed in the following sections can be found in Table 2.

4.1 Understanding of data collection

We asked participants three questions (Q11-Q13) to assess their current understanding of data collection practices on digital assistants. Specifically, we asked them about the (i) types of data collected, (ii) manufacturer's purpose for collecting data, (iii) perceived likelihood of the manufacturer being able to identify the user.

Participants were asked to pick from a pre-defined list of data they believed was collected by digital assistants. Participants could select multiple options, including "Other" to provide free-form feedback. We found that most participants correctly identified that digital assistants commonly collect searches and commands (n=177), users' voice patterns (n=140), and everything users say (n=139).

A few participants incorrectly identified that digital assistants collect medical (n=46) and banking (n=48) information, suggesting that they may over-estimate the data collection practices in digital assistants and have mental models that reinforce (and possibly over-estimate) the surveillance or tracking capabilities of the technology. This was also reflected in the free-form feedback provided by a small number of participants (n=15). These participants explained that digital assistants collected specific types of data (e.g., hardware IDs, location) or collected "everything" once triggered by a command (e.g., "Ok, Google"). As one participant explained:

> "They will collect anything that they have sensors to collect. If it is in or connected to a smart watch it may collect blood oxygen level. If it is connected to something with GPS it will track where you have been.".

With regards to the purpose of data collection on digital devices, participants were asked to select from a pre-defined list of choices. They could pick multiple choices, including "Other" to provide free-form feedback. Most thought that the manufacturer's main objective of data collection was to build a digital profile of users for advertising

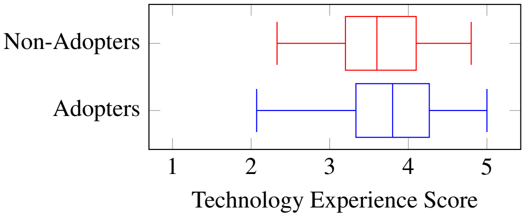

Fig. 1. Experience scores for adopters and non-adopters of Smart Home devices. Higher scores indicate higher Experience.

purposes (n=159), or to sell their data to third parties (n=106) . Approximately half (n=122) thought that it was for improving the quality of service.

On a 5-point Likert-scale (1 = not at all, 5 = very likely), we asked participants if they believed that companies could identify the current user of a digital assistant. A Mann-Whitney test found non-adopters (*M* = 4.14, *Md* = 4, *SD* = 1.00) were more likely to believe that companies could identify users of a digital assistant than adopters (*M* = 3.79, *Md* = 4, *SD* = 1.07), *(U = 3234, n1 = 92, n2 = 87, p = .020. two-tailed).*

4.2 Addressing RQ1: Effect of Experience

We computed participants' *Experience Score* by averaging their responses to the 15 *Experience with Technology* Likert-scale questions (Q19-Q33). Their *Experience Score* was out of 5 (M = 3.71, Md = 3.73, SD = 0.625), with 1 indicating the least Experience and 5 indicating the most Experience. Of the 3180 data points (212 participants * 15 questions), 36 responses were either 'I do not know' or 'I don't understand the question'; we coded these to align with the most negative Likert-scale response, since if one cannot understand the question or is unsure, this implies a lack of concept knowledge.

Experience and Perceived Protection of Data We asked participants two 5-point Likert-scale questions (Q14-Q15) to assess their views on Smart Home data protection. Specifically, we asked them whether they (i) trusted companies which held their digital assistant data; (ii) believed that Smart Home devices are well protected in terms of security and privacy. We averaged participants' responses to these questions to give them a perceived protection score out of 5 (*M* = 3.32, *Md* = 3.00, *SD* = 1.01). A higher score indicated a more positive perception, while a low score was indicative of negative perception. A Pearson product-moment correlation found no linear correlation between participants' Experience and their views on Smart Home device data protection (r = -.006, n = 211, p = .933), indicating no linear relationship between the two measures.

Experience and protective strategies Of the participants who had adopted Smart Home devices, we asked three 5-point Likert-scale questions (Q16-Q18) assessing their likelihood of using certain protective strategies on digital assistants. Specifically, we asked of their likelihood of: (i) covering the Smart Home digital assistants' microphone to prevent eavesdropping; (ii) regularly deleting data collected by the Smart Home digital assistant; (iii) covering the Smart Home digital assistants' camera to prevent unauthorized video recordings. As shown in Figure 5, we found that most adopters of Smart Home devices did not implement common strategies to protect their security and privacy in relation to the digital assistants.

We further explored whether there was a relationship between participants' Experience and their likelihood of using protective strategies on their Smart Home digital assistants. To do this, we averaged their scores on the three 5-point Likert-scale (1 = always implemented, 5 = never implemented) questions assessing their likelihood of using certain protective strategies. A Pearson product-moment correlation found no linear relationship between participants' Experience and their likelihood of using protective strategies on their Smart Home digital assistants (*r* = -.182, *n* = 103, *p* = .065).

Experience and security and privacy concerns Participants' security and privacy concerns about Smart Home digital assistants were measured using 10 Likert scale questions (Q34-Q43). We averaged their scores on these questions to compute a *Concern* score out of 5 (M = 3.43, Md = 3.60, SD = 1.00), where a higher score indicated higher security and privacy concerns about Smart Home digital assistants. To explore the existence of a relationship between participants' Experience and their security and privacy concerns, we computed a Pearson product-moment correlation, which found no correlation between the two (*r* = .065, *n* = 212, *p* = .348).

4.3 Addressing RQ2: Difference between adopters and non-adopters of Smart Home devices

As indicated by responses to Q7, 103 of the 212 survey respondents had adopted at least one type of Smart Home device. We explored the relationship between adoption and participants' Technology Experience, perceived protection of data by Smart Home devices as well as security and privacy concerns towards Smart Home digital assistants.

Adoption and Experience Figure 1 shows the Technology Experience of adopters and non-adopters. Using an independent samples t-test, we found that adopters (*M* = 3.80, *Md* = 3.80, *SD* = .614) of Smart Home devices had more Technology Experience compared to non-adopters (*M* = 3.61, *Md* = 3.63, *SD* = .626) *(t (210) = 2.253, p = 0.025)*. Normality and equal variance assumptions for the t-test were checked using the Shapiro-Wilk and Levene's tests respectively.

Adoption and Users' Perceived Protection of Data by Smart Home Devices We investigated whether adopters and non-adopters had different levels of perceived protection of data in Smart Home devices, using the same questions as in the previous section (Q14-Q15). We averaged participants' responses to these questions to give them a perceived protection of data score out of 5 (*M* = 3.32, *Md* = 3.00, *SD* = 1.01). Figure 2 shows the distribution of responses. An independent-samples t-test found that compared to non-adopters, adopters perceived protection of data Smart Home devices

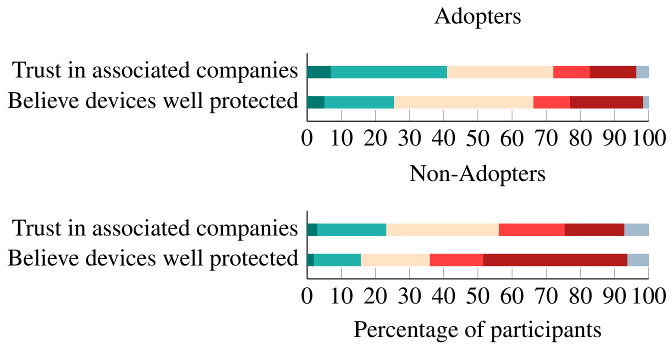

Fig. 2. 5-point Likert Scale responses to participants' perceived protection of data by Smart Home devices. 1 = 'True of me', represented in dark green; and 5 = 'Not true of me', represented in dark red. An answer of "Not Sure" or "I don't know" was represented in grey.

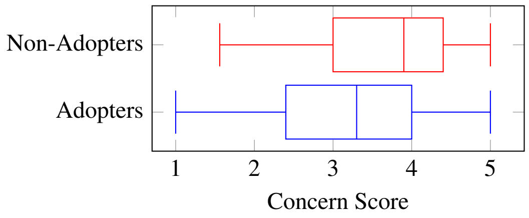

Fig. 3. Adopters and non-adopters' security and privacy concerns on Smart Home digital assistants; higher scores indicate a higher degree of concern.

more in terms of the companies which collected data on these devices, and believed that Smart Home devices are well protected in terms of their security and privacy *(t (205) = -3.63, p = .001)*. Normality and equal variance assumptions for the t-test were checked using the Shapiro-Wilk and Levene's tests respectively.

Adoption and Security and Privacy Concerns Towards Digital Assistants Participants' security and privacy concerns about Smart Home digital assistants were measured using 10 Likert scale questions (Q34-Q43). Figure 4 illustrates the distribution of responses for adopters and non-adopters. We see that non-adopters expressed high levels of concern for all privacy questions. Adopters were least concerned about image collection and voice data collection. We note smaller differences between the two groups on all security questions, although in each case non-adopters expressed more concern. We conducted an independent samples t-test to compare the concern score (comprised of the privacy and security questions) of adopters and non-adopters.

We found that adopters (*M* = 3.19, *Md* = 3.30 , *SD* = 1.02) are less concerned about Smart Home digital assistants than non-adopters (*M* = 3.65, *Md* = 3.90, *SD* = 0.94) , (*t (210)* = -3.483, *p* = 0.001). Normality and equal variance assumptions for the t-test were checked using the Shapiro-Wilk and Levene's tests respectively.

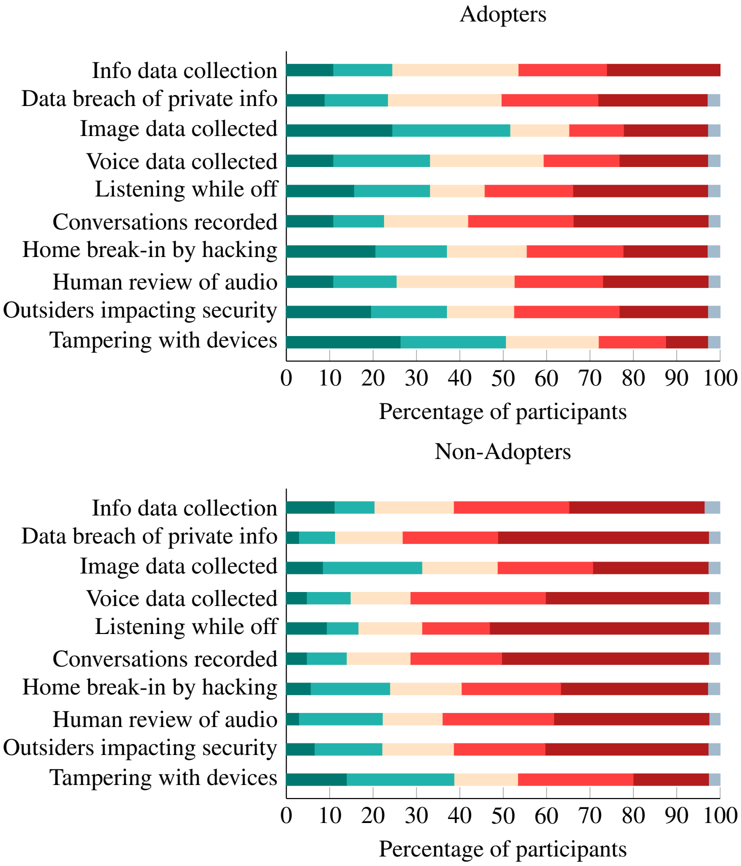

Fig. 4. 5-point Likert Scale responses to participants' Concerns relating to Smart Home digital assistants. 1 = 'Not at all concerned', represented in dark green; and 5 = 'Very Concerned', represented in dark red. An answer of "Not Sure" or "I don't know" was represented in grey.

4.4 Post-Hoc Analysis

Adopters had more Technology Experience, more positive views on the perceived protection of data by Smart Homes, and were less concerned about Smart Home digital assistants. However, we did not find any relationships between Technology Experience and perceived protection of data, nor with security and privacy concerns of Smart Home digital assistants. Given this, we conducted post-hoc analysis to determine whether the observed differences between adopters and non-adopters were due to other factors, such as geographical location, gender, or age.

Geographical location Most of our participants were from Europe or North America. Adopters consisted of 50 North Americans and 44 Europeans, and non-adopters consisted of 37 North Americans and 57 Europeans. We explored whether there was a

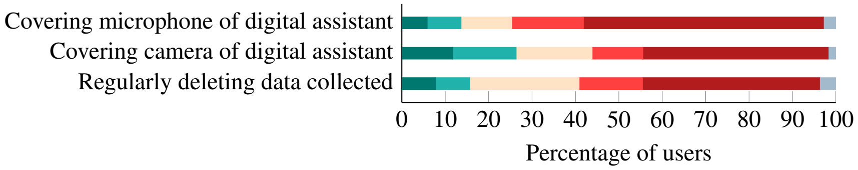

Fig. 5. 5-point Likert Scale responses to participants' the likelihood of adopters using protective strategies on their Smart Home devices. 1 = 'All the Time', represented in dark green; and 5 = 'Never', represented in dark red. An answer of "Not Sure" or "I don't know" was represented in grey. *Note: The deleting data question was missing the 'rarely' (4) option for approximately the first one third of participants.

difference between the two geographical areas in terms of Technology Experience and participants' likelihood of adopting Smart Home devices.

A Kruskal-Wallis H test found no statistically significant differences in Technology Experience scores between European (M = 3.70, Md = 3.73, SD = 0.60) and North American (M = 3.68, Md = 3.73, SD = 0.66) participants ($\chi^2(1) = 0.012, p = 0.913$).

We conducted a Mann-Whitney test, which found no relationship between geographical location and likelihood of adopting Smart Home devices (U = 3782.5, $n1$ = 87, $n2$ = 101, p = .058 two-tailed).

Gender We further explored the role of gender in the differences observed between adopters and non-adopters. A Kruskal-Wallis H test found a statistically significant difference in Technology Experience between men (M = 3.93, Md = 3.97, SD = 0.57) and women (M = 3.52,Md =3.60 , SD = 0.61), with men having a higher Technology Experience ($\chi^2(1)$ = 20.833, p = 0.000005).

We then conducted a Mann-Whitney test and found no relationship between gender and likelihood of adopting Smart Home devices (U = 5140.0, $n1$ = 92, $n2$ = 116, p = .600 two-tailed).

Age Prior work has shown a potential relationship between participants' age and their mental models of Smart Home devices, with older users having less complete mental models [6]. Thus, we explored whether participants' age could be a factor in the differences observed between adopters and non-adopters.

A Pearson product-moment correlation, found no linear relationship between participants' Technology Experience and age (r = .015, n = 212, p = .824). We then conducted an independent samples t-test to see if there was a difference in age between adopters and non-adopters. We found that adopters (M = 30.51, Md = 26.0, SD = 11.34) were significantly younger compared to non-adopters (M = 37.41, Md = 34.00, SD = 13.54) (t (210) = -4.005, p = 0.025).

5 Discussion

5.1 Answering RQ1

Returning to our first research question, we expected to find a relationship between Technology Experience and each of our dependent variables. However, this was not the case and we found no statistically significant results for this research question. This leaves two possibilities: that there is no relationship, or that our instrument was unable to detect it.

Let us first assume that our results are in fact correct, and consider its implications. First, we see quite a range of responses from participants, so it may be that another trait, besides Experience, is at play. For example, previous research has found that emotion had a stronger effect on concerns and trust [10] than knowledge of the subject matter. Thus, there may be other unexplored traits that together with Experience, or alone, are more closely related to the concern of users' and their behaviour.

Contrary to our findings, other researchers have pointed to a likely connection (see Section 2), and it would seem plausible that a connection exists between Technology Experience and perceived protection of data, behaviours, and concerns. Although we carefully created our Technology Experience measure as an aggregate score of questions covering several areas, we may have failed to capture the relevant aspects of Technology Experience. Similarly, we may have failed to measure the right elements relating to perceived protection of data, concerns, or behaviours. Given that many other works identify a possible link used qualitative methods, perhaps the relationship between Experience and behaviours, perceived protection of data, and concerns is too nuanced to be captured in a quantitative survey.

5.2 Answering RQ2

On this research question, we have identified some statistically significant results. It may be that adoption is a more relevant differentiator than Experience.

We found that adopters held more positive views towards data protection within Smart Home devices and held a higher self reported trust in the associated companies, adopters also expressed fewer concerns related to privacy and security, and they generally had more Technology Experience. In post-hoc analysis, we further found that adopters were younger than non-adopters.

These findings highlight the importance of considering non-adopters in research related to Smart Home technologies. It is possible that their reluctance in engaging with this technology stems in part from significant privacy and security concerns (i.e., note the proportion of non-adopters saying they are very concerned in Figure 4). As Smart Home technologies become ubiquitous, it will be increasingly difficult for non-adopters to purchase 'non-smart' devices even if that is their preference. Non-adopters must already cope with Smart Home technology as bystanders or unknowing users when they visit other homes, or even within their own homes if another occupant chooses to adopt Smart Home devices.

We also note that although adopters had fewer concerns than non-adopters, this did not mean that they were wholly comfortable with the technology. The proportion of adopters who expressed *no* concern was roughly equivalent to the proportion of adopters expressing *a high degree* of concern. This high variability is interesting and suggests that other factors play an important role in users' decisions to adopt Smart Home technology. Despite their concerns, our adopters were very unlikely to use any of the three listed mitigation strategies that had been most commonly identified in the literature.

Furthermore, we see that two privacy risks relating to eavesdropping and surveillance were especially concerning. The concern of digital assistants listening while turned off and the concern about conversation being recorded were the highest rated concerns amongst both adopters and non-adopters.

5.3 Relationship to previous work

Haney et al. [8] found that while users expressed concerns, this did not deter them from adopting Smart Home technologies, with mitigation measures. Our work also suggests that adopters had significant concerns but few reported using common mitigation strategies. Our work extends previous findings by putting them into perspective: we demonstrate that the levels of concern expressed by adopters are significantly lower than for non-adopters. Participants in studies about security and privacy may be primed to express such concerns simply because the study brings this topic to the forefront. By surveying non-adopters as well, we supply context for the responses of adopters; any over-estimates would be present in both groups, thus the relative levels of concern can still offer insight. Barbosa et al.'s MTurk survey [4] had a mix of adopters and non-adopters, but their questions focused on hypothetical scenarios. Despite our different approach, our results do closely align with Barbosa et al.'s findings.

5.4 Limitations

In an attempt to minimize inattention, our survey was relatively short and focused mostly on closed types of questions. Such self-reported data may not entirely reflect users' actual behaviours and concerns. We tried to briefly cover the most important topics but it is possible that we missed some. In particular, our Technology Experience score may not adequately capture the actual Experience of individuals. We also note that our survey does not consider other reasons why users might not adopt Smart Homes technology, besides privacy and security. For example, recent work by Hong et al. [9] and Barbosa et al. [4] found that monetary considerations may negatively impact such decisions.

Furthermore, it is important to note that due to this being an online survey, participants may have skimmed the definition questions in which we note that the digital assistants discussed within the survey are in relation to Smart Home devices. Therefore, some may have considered all digital assistants in their responses. In terms of age, 91% of our participants were between the ages of 18-40, meaning that our study results may not accurately represent the older population. Despite this limitation, our results may reflect typical users as adoption have been shown to be primarily done by adults ranging from the ages of 18-50 [16]. Lastly, our survey did not explore *how* users became adopters. Adopters may have unwittingly become adopters due to a member of their residence purchasing a Smart Home device. Rather, than simply asking if one has adopted a device, we recommend future studies more closely differentiate between an active adoption and a passive adoption.

6 Conclusion

Through an online survey of 212 participants, we compared responses of adopters and non-adopters in relation to Smart Home digital assistants. We explored privacy and security concerns, security and privacy behaviors, and Technology Experience levels of participants. Our results showed that adopters were more optimistic about the perceived protection of data by Smart Home devices, had fewer concerns towards Smart Home digital assistants, and self-reported a higher level of Technology Experience than non-adopters. Nevertheless, many adopters still reported being very concerned about several security and privacy issues relating digital assistants. Adopters were also unlikely to use mitigation techniques to alleviate their concerns. Non-adopters expressed significant concern related to security and privacy. Our results further showed no relationship between Technology Experience score and our dependent variables, suggesting that adoption may be a better differentiator. There is, therefore, a definitive need for considering the perspectives of non-adopters in relation to Smart Home technologies.

A Survey questions

A.1 Understanding of definitions

- This survey applies to *digital assistants* within *Smart Homes*
- Smart Homes are equipped with systems and appliances that can be operated remotely using a computer or mobile phone. Examples of Smart Homes are homes that include appliances/systems such as thermostats, fridges, locks, light switches, TVs, sound systems, or security cameras that can be controlled by the user through a computer or phone.
- Digital assistants are digital AI meant to assist a user by carrying out voice commands. When this survey talks about digital assistants, it refers to devices such as the Amazon Alexa, Google Assistant, SmartThings, Siri, and other voice-controlled assistants. These assistants can perform tasks such as search the web, control other smart devices, play music, set timers, check the weather, make phone calls, or run other voice-controlled apps.

1. Please select all examples of Smart Homes devices.
   - LG Smart TV; Ecobee voice controlled thermostat; Amazon Echo Speaker; Microsoft Cortana Speaker; Tesla Autopilot car; TP-Link mobile light switch; Voice controlled home security system
2. Please select all examples of voice-controlled digital assistants within Smart Homes.
   - Microsoft Cortana; Amazon Alexa; Siri; Microsoft Office spellcheck; Google Voice Assistant; Samsung Bixby

A.2 Demographics

3. What is your age?
4. Which of these best describes you
   - Male; Female; Non binary; Prefer to self-describe (please specify); Prefer not to say
5. In what region do you reside?
   - North America; Europe; Middle East; Southern Africa; Northern Africa; South America; Asia; Australia; Prefer to self-describe (please specify); Prefer not to say
6. What is the highest level of education you have completed?
   - Less than secondary school (e.g., up to grade 8); Some of secondary school (e.g., between grade 8 and 12); Completed secondary school (e.g., completed grade 12); Trade/Technical/Polytechnic; Some undergraduate(College/University); Completed undergraduate; Some graduate or professional degree (e.g., Masters, PhD, medical); Completed graduate or professional degree (e.g, Masters, PhD, medical)
7. Have you adopted Smart Home technology into your home?
   - Yes; No
8. If yes, which brand of Smart Home have you adopted?
   - Google; Amazon; Samsung; Wink; Other (Please specify)
9. Have you ever encountered a privacy breach of your data?
   - Yes; No; Not Sure
10. Please rate these topics in order of importance to you (1 = least important, 4 = most important)
    - Usability; Being connected; Privacy of data; Security of data

A.3 Understanding of data collection

11. What type of data do you think digital assistants collect
    - Medical information; Everything you say; Banking information; Voice patterns; Your searches/commands; Other (please specify); None
12. What is manufacturers' main purpose when collecting data through digital assistants
    - Building a digital profile of you for advertising purposes; Improving the quality of service provided; Selling your data to third parties; Other (please specify); Not sure
13. On a scale of 1 (not at all) to 5 (very likely), how likely is it that the manufacturer can identify the current user of the digital assistant?

A.4 Perceived Protection of Data

Questions in this section have the following options:

- *True of me; Mostly true of me; Halfway true of me; Slightly untrue of me; Not true of me; Not sure what the question entails; I don't know*

14. You trust the companies that hold your data
15. You believe that Smart Home devices are well protected in terms of security and privacy

A.5 Use of protective strategies

Questions in this section have the following options:

- *All the time; Most of the time; Sometimes; Rarely; Never; Not sure what the question entails; I don't know*

16. You cover the microphone of the digital assistant to prevent 'eavesdropping'
17. You cover the camera of the digital assistant to prevent video recording
18. You regularly delete the data that the digital assistant has collected

A.6 Technology Experience

Questions in this section have the following options:

- *True of me; Mostly true of me; Halfway true of me; Slightly untrue of me; Not true of me; Not sure what the question entails; I don't know*

19. You find it hard to decide what the best keywords are to use for online searches
20. You find it hard to find a website you visited before
21. You have an education related to cybersecurity or work experience in cybersecurity
22. All the different website layouts make working with the internet difficult for you
23. You find it hard to verify the accuracy of information you have retrieved online
24. You are comfortable using and understanding technology
25. You understand the impact of changing privacy settings online
26. You are comfortable navigating your computer/mobile device
27. You are comfortable working with the internet router in your home
28. You understand how cookies work on the web
29. You are comfortable configuring the firewall on your home network
30. You follow news stories relating to data leaks and privacy threats
31. You have customized the privacy settings on your browser or on your device
32. You have customized your devices or browser to limit ad trackers
33. You believe that you have a good understanding of how your data is being used online

A.7 Security and privacy concerns

34. You are concerned about the way digital assistants collect information about you
    - True of me; Mostly true of me; Halfway true of me; Slightly untrue of me; Not true of me; Not sure what the question entails; I don't know

The following questions have answer options on a scale of 1 (not all concerned) to 5 (very concerned). How concerned are you about the following in relation to digital assistants?

35. Data breach of private info gathered by the voice assistant
36. Image data collected by the voice assistant
37. Voice data collected by the voice assistant

38. Voice assistant listening while turned off
39. Conversations recorded by the voice assistant
40. Outsiders changing settings or interfering with home devices (thermostats, fridge, etc.)
41. Outsiders using your Smart Homes to open locks or turn off security systems
42. Human review by the manufacturer of audio recordings revealing sensitive information (bank info, lock code, medical info, etc.)
43. Someone breaking into your home by hacking the home device

References

1. Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019) (2019)
2. Adams, R.J.: 'Alexa, how can we increase trust in you?': An Investigation of Trust in Smart Home Voice Assistants. B.S. thesis, University of Twente (2019)
3. Barbosa, N.M., Zhang, Z., Wang, Y.: Do privacy and security matter to everyone? quantifying and clustering user-centric considerations about smart home device adoption. In: Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020). pp. 417–435 (2020)
4. Barbosa, N.M., Zhang, Z., Wang, Y.: Do privacy and security matter to everyone? quantifying and clustering user-centric considerations about smart home device adoption. In: Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020). pp. 417–435. USENIX Association (Aug 2020), https://www.usenix.org/conference/soups2020/presentation/barbosa
5. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into iot device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019)
6. Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F., Egelman, S.: Privacy and security threat models and mitigation strategies of older adults. In: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019) (2019)
7. Georgiev, A., Schlögl, S.: Smart home technology: An exploration of end user perceptions. Innovative Lösungen für eine alternde Gesellschaft: Konferenzbeiträge der SMARTER LIVES **18**(20.02) (2018)
8. Haney, J.M., Furman, S.M., Theofanos, M.F., Fahl, Y.A.: Perceptions of smart home privacy and security responsibility, concerns, and mitigations. In: Symposium on Usable Privacy and Security. USENIX (2019)
9. Hong, A., Nam, C., Kim, S.: What will be the possible barriers to consumers' adoption of smart home services? Telecommunications Policy **44**(2), 101867 (2020)
10. Lahno, B.: On the emotional character of trust. Ethical theory and moral practice **4**(2), 171–189 (2001)
11. Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 1–31 (2018)
12. Liao, Y., Vitak, J., Kumar, P., Zimmer, M., Kritikos, K.: Understanding the role of privacy and trust in intelligent personal assistant adoption. In: International Conference on Information. pp. 102–113. Springer (2019)
13. Lin, H., Bergmann, N.W.: Iot privacy and security challenges for smart home environments. Information **7**(3), 44 (2016)

14. Manikonda, L., Deotale, A., Kambhampati, S.: What's up with privacy? user preferences and privacy concerns in intelligent personal assistants. In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. pp. 229–235 (2018)
15. Singh, D., Psychoula, I., Kropf, J., Hanke, S., Holzinger, A.: Users' perceptions and attitudes towards smart home technologies. In: International Conference on Smart Homes and Health Telematics. pp. 203–214. Springer (2018)
16. Statista: Smart home technology ownership rates by age in the u.s. 2016. https://www.statista.com/statistics/756519/united-states-smart-home-survey-demographic-adoption-rates-by-age/ (2016)
17. Statista: Number of digital voice assistants in use worldwide from 2019 to 2024 (in billions). https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/ (2021)
18. Statista: Smart home - statistics & facts. https://www.statista.com/topics/2430/smart-homes/ (2021)
19. Statista: Smart homes. https://www.statista.com/outlook/279/109/smart-home/united-states (2021)
20. Tabassum, M., Kosinski, T., Lipford, H.R.: " i don't own the data": End user perceptions of smart home device data practices and risks. In: Symposium on Usable Privacy and Security ({SOUPS}. USENIX (2019)
21. Van Deursen, A.J., Helsper, E.J., Eynon, R.: Development and validation of the internet skills scale (iss). Information, Communication & Society **19**(6), 804–823 (2016)
22. Williams, M., Nurse, J.R., Creese, S.: 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). pp. 181–18109. IEEE (2017)
23. Yao, Y., Basdeo, J.R., Mcdonough, O.R., Wang, Y.: Privacy perceptions and designs of bystanders in smart homes. Proceedings of the ACM on Human-Computer Interaction **3**(CSCW), 1–24 (2019)
24. Zeng, E., Mare, S., Roesner, F.: End user security and privacy concerns with smart homes. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 65–80 (2017)
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)
26. Zimmermann, V., Bennighof, M., Edel, M., Hofmann, O., Jung, J., von Wick, M.: 'home, smart home'–exploring end users' mental models of smart homes. Mensch und Computer 2018-Workshopband (2018)