Patrick Bombik, Tom Wenzel, Jens Grossklags, and Sameer Patil*

A Multi-Region Investigation of the Perceptions and Use of Smart Home Devices

Abstract: Smart Home Devices are household objects and appliances that are augmented with network connectivity and interactive capabilities. However, the benefits and conveniences of such augmentation are tempered by corresponding increases in privacy and security threats. Studies of user perceptions of these threats and user practices for addressing them are limited mostly to specific devices and/or small samples from a single region. To address this gap, we compared perceptions and practices of people in three geographic regions regarding privacy and security matters related to Smart Home Devices. Across these regions, we found differences in perceived regulatory protection and other regional factors. Our findings suggest that a co-evolution of the design and public policy related to Smart Home Devices could enhance privacy protection and drive increased adoption of these devices.

Keywords: smart home devices, privacy, security, regulation, regional differences, household

DOI 10.56553/popets-2022-0060
Received 2021-11-30; revised 2022-03-15; accepted 2022-03-16.

1 Introduction

Recent years have seen an increasing interest in augmenting everyday household objects and appliances with interactive capabilities and Internet connectivity, turning familiar physical objects, such as speakers, toasters, doorbells, etc., into what are commonly known as 'Smart Home Devices.' A network of such devices creates what is termed as the 'Internet of Things' (IoT) [5]. These devices can be standalone and/or controlled via an auxiliary device, such as a smartphone.

Patrick Bombik: Technical University of Munich, E-mail: patrick.bombik@tum.de
Tom Wenzel: Technical University of Munich, E-mail: tom.wenzel@tum.de
Jens Grossklags: Technical University of Munich, E-mail: jens.grossklags@tum.de
***Corresponding Author: Sameer Patil:** School of Computing, University of Utah, E-mail: sameer.patil@utah.edu

Smart Home Devices are *by definition* embedded within a home, the most intimate and personal of settings [50]. While the data collected by Smart Home Devices can be stored locally, it is often transferred to an external service for processing and/or storage in the cloud [39]. Therefore, the data-handling operations of these devices can have a profound impact on the privacy of the people in the household and their visitors [40]. Understanding people's privacy perceptions and practices when interacting with these devices is therefore necessary to verify whether the device operation adequately meets user privacy expectations. Such an understanding can in turn be applied to improve privacy management and security protection for the data collected by these devices. Research efforts in this regard have typically covered individual devices, such as Smart TVs [26] or Smart Speakers [1, 34], instead of taking an ecological approach that examines Smart Home Devices more generally.

Given the highly personal nature of the data collected by Smart Home Devices, their data practices must comply with privacy regulation, such as the General Data Protection Regulation (GDPR) in the European Union (EU) [23], the California Consumer Privacy Act (CCPA) in California [8], etc. Yet, it is unclear whether people actively consider such regulatory protection when adopting and using novel technologies [47].

It is well-known that privacy expectations and practices are nuanced [2], highly contextual [43], and socially grounded [19]. Analogously, regulatory requirements regarding privacy differ across regions. Similarly, local differences can impact the characteristics of a 'home' and everyday domestic practices within it. Therefore, a rich understanding of the privacy expectations and practices related to Smart Home Devices requires covering multiple locales with social and regulatory differences. Yet, existing studies of the users of Smart Home Devices typically involve samples from a single region [22, 25, 64].

To fill the various gaps mentioned above, we conducted a multi-region study to address the following research questions:

RQ1: How are the *perceptions* and *use* of Smart Home Devices affected by *perceived regulatory protection* for the personal data collected by these devices?

RQ2: How do *regional variations in privacy concerns* impact the *perceptions* and *use* of Smart Home Devices?
RQ3: How are the *perceptions* and *use* of Smart Home Devices influenced by the *characteristics of the home*?

By analyzing the responses ($n = 431$) to an online questionnaire administered in three regions (i.e., i. United States, ii. United Kingdom, and iii. Austria, Germany, and Switzerland, the three major German-speaking countries in Europe), we found that the perceptions, adoption, and use of Smart Home Devices are connected to perceived regulatory protection, regional differences, and household parameters. For instance, perceived regulatory protection is associated with lower perceived privacy risk, greater adoption, and higher use of Smart Home Devices. Our findings contribute to broadening the scope of the research on real-world preferences and practices of users of Smart Home Devices across regions and devices.

In the sections that follow, we cover the salient work on the privacy aspects of Smart Home Devices and develop specific hypotheses connected to the research questions listed above. We proceed to provide detail on the questionnaire used to collect the data to verify the hypotheses. Next, we present the findings pertaining to each research question followed by a discussion of their practical relevance and implications. We conclude with thoughts on promising future research directions.

2 Related Work and Research Hypotheses

We first summarize the various concepts related to Smart Home Devices followed by the privacy aspects connected to the operation and use of these devices. Next, we describe the literature connected to each of our research questions and derive the corresponding hypotheses.

2.1 Concepts of Smart Home and Smart Home Device

A Smart Home has been conceptualized as "a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond" [3]. As such, a Smart Home contains a variety of devices and technological subsystems connected to various domestic functions [11]. Apart from general-purpose domestic tasks, Smart Home technology can be applied to serve niche purposes, such as at-home care for the elderly [11], sustainable living [36], etc.

A Smart Home *Device* has not been explicitly defined in the literature, instead being included within a variety of descriptions such as Internet of Things (IoT), household devices or appliances that can be manipulated over the network (e.g., speakers [1, 34], TVs [26]), Internet-connected physical objects (e.g., door locks [44]), sensors embedded within a Smart Home [15], and so on. We unify these descriptions by defining a Smart Home *Device* as a hardware-software combination deployed within a home to perform one or more of a broad range of domestic functions. A Smart Home Device may combine and automate routine domestic tasks to increase the quality, safety, and efficiency of domestic life [35].

2.2 Privacy and Smart Home Devices

The increasing proliferation of Smart Home Devices has led to numerous privacy incidents involving these devices that have been reported by the popular press (e.g., [9]). In response, researchers have been studying how individuals perceive the privacy risks associated with these devices. Typically, the focus of these investigations has been on specific devices, such as Smart Speakers [34], Smart TVs [26], etc. For instance, Lau et al. [34] found that many users of Smart Speakers report low levels of privacy concerns and do not typically use the available privacy controls because they lack a full understanding of the potential privacy risks. Abdi et al. [1] similarly uncovered that users have incomplete mental models of the operation of Smart Speakers, leading to a variety of false perceptions regarding how Smart Speakers handle data storage, processing, and sharing, a point raised also by Hadan and Patil [27] and Haney et al. [29].

In a study of users of Smart TVs, Ghiglieri et al. [26] discovered that people are generally unaware of the associated privacy risks, but would disconnect the device when shown messages mentioning the potential harm. Still, if the core functionality is negatively impacted, users of Smart TVs are typically unwilling to employ privacy-protecting measures. More generally, researchers have found that users harbor privacy and security concerns regarding Smart Home Devices, but

mostly lack the knowledge to implement the appropriate measures to counter the perceived threats [27, 29].

Perhaps unsurprisingly, a study by Emami-Naeini et al. [41] exploring the broader IoT landscape indicates that devices collecting data in private living spaces are seen as more problematic in comparison to those collecting information in public. Developing an understanding of a range of such contextual factors can facilitate the design of awareness-enhancing measures, such as IoT product labels [21], that could help address the uncertainty users experience regarding the data practices of device manufacturers [34, 57].

Individuals often differ in their expectations regarding the data practices and responsibilities of manufacturers of Smart Home Devices. Zeng et al. [67] found that users of Smart Home Devices focus more on avoiding physical security risks than on addressing privacy issues. Zheng et al. [69] showed that early adopters trust the device manufacturers to protect their privacy, even though they typically do not verify if the manufacturers have actually implemented the advertised protective measures. Similarly, Haney et al. [28] uncovered that users of Smart Home Devices assign the responsibility for privacy and security protection to the device manufacturers, the government, themselves, or a combination of the three. In general, users perceive an interdependent relationship between these actors in the pursuit of robust privacy and security for their Smart Homes. When users are unwilling or unable to take the desired protective actions themselves, they demand better built-in protection from the manufacturers, facilitated by government regulation [28].

In addition, users may trust specific manufacturers based on experiences with their devices, while non-users lack such trust [34, 41]. Instead, non-users typically rely on social influence [42] and often do not consider privacy and security features prior to purchasing Smart Home Devices [22]. However, privacy and security concerns may become important post-purchase as individuals transition from non-users to users. In fact, privacy and security concerns are one of the top blockers of the adoption of Smart Home Devices [6].

2.3 Cross-Cultural Differences in Privacy

It is well-known that privacy perceptions and practices vary across cultures [16]. For instance, Cho et al. [13] showed that privacy concerns and behavior of Internet users vary significantly across nationalities and demonstrated such differences in the context of social media, where people from different countries interpret privacy management features in different ways [12]. Similarly, it has been observed that American and German users hold different perceptions regarding their abilities to control the privacy of their personal data [18].

Such national differences can be explained by a variety of factors, such as national cultural values [13] and their connection with the national regulatory framework [7]. For instance, Trepte et al. [58] found that cultural characteristics, such as uncertainty avoidance [30], can significantly influence the perceptions of the risks and benefits and affect user behavior on Social Network Sites (SNS).

2.4 Hypotheses

The above discussion of prior work provides an initial assessment of the contextual and operational aspects that shape the perceptions and adoption decisions of users and non-users of Smart Home Devices. We contribute to the understanding of the perceptions and use of Smart Home Devices by examining their associations with regulatory, regional, and household factors. Specifically, we captured the perceptions regarding the *risk*, *responsibility*, *benefits*, and *comfort* related to Smart Home Devices and operationalized the use of the devices in terms of *adoption*, *usage frequency*, and *disabling of device features*.

2.4.1 Regulatory Environment

Researchers have highlighted the importance of the regulatory environment on user privacy and attempted to investigate the relationship between privacy attitudes and practices and the overarching regulatory framework. In the context of social networks, Cecere et al. [10] investigated the institutional influence on privacy concerns and awareness within European countries, finding that greater national efforts to safeguard personal data are associated with increased perceptions of privacy protection. In addition, researchers have found that institutional frameworks can be helpful when users are not able to address privacy and security concerns on their own [28].

While researchers have been examining the challenges that IoT devices pose for the existing regulatory frameworks [61], we are unaware of research investigating the connection between user perceptions and practices and the regulatory environment. Therefore,

our first research question focuses on studying how perceived regulatory protection is related to people's perceptions and use of Smart Home Devices. We surmised that those who feel greater regulatory protection are likely to feel safer. Therefore, we hypothesized that higher perceived regulatory protection would be associated with lower negative perceptions and greater use of Smart Home Devices, as captured in the following hypotheses:

H1a: *Perceived regulatory protection is positively associated with positive perceptions regarding Smart Home Devices.*

H1b: *Perceived regulatory protection is positively associated with the adoption of Smart Home Devices.*

H1c: *Perceived regulatory protection is positively associated with the use of Smart Home Devices.*

2.4.2 Regional Influences

Most studies on Smart Home Devices focus on specific countries, regions, or markets. The majority of these studies have been conducted either in the United States [22, 25, 34] or in a single other country, such as the United Kingdom [55, 62] or Germany [31]. Investigations that span multiple regions are rare and typically cover regions within the same continent. For example, Kulyk et al. [32] found that privacy and security awareness was higher in Germany than in Spain and Romania. Further, Miltgen et al. [38] found that Northern and Southern Europeans differ in the importance they place on responsibility and trust when disclosing or protecting personal data. Miltgen et al. [38] additionally discovered that people in Southern and Eastern Europe perceive data disclosure differently. However, we are unaware of cross-regional studies regarding Smart Home Devices that cover multiple regions beyond Europe. We addressed this research gap with the following hypotheses:

H2a: *The perceptions of Smart Home Devices differ across regions.*

H2b: *The adoption of Smart Home Devices differs across regions.*

H2c: *The use of Smart Home Devices differs across regions.*

To test the above hypotheses, our study included individuals from three socioculturally different regions: United States (US), United Kingdom (UK), and the three primarily German-speaking (GS) European countries (i.e., Austria, Germany, and Switzerland).

2.4.3 Household Characteristics

It has been suggested that the domestic environment of the user of Smart Home technologies has an influence on the user's actions [42]. Further, households are often composed of individuals spanning multiple generations, and previous research has discovered significant differences between the privacy concerns expressed by older generations and young adults/children [38]. For example, Zhao et al. [68] discovered that children may be better at identifying certain risks, such as information oversharing. At the same time, researchers have found that people tend to be more concerned when the privacy of children or guests is involved [28, 37]. However, the influence of household characteristics on the perceptions and use of Smart Home Devices is largely unexplored in the literature.

We examined *home ownership*, *household size* (i.e., number of household members), and the *presence of children* within the household as the characteristics likely to be the most relevant for the adoption and use of Smart Home Devices. We hypothesized that owning (vs. renting) the home and having more members in the household is likely to be associated with greater *adoption* and *use* of Smart Home Devices. Further, we conjectured that the *presence of children* in the home is likely to be associated with negative perceptions of these devices. Based on these suppositions regarding the three household characteristics, we developed three corresponding hypotheses:

H3a: *The perceptions, adoption, and use of Smart Home Devices differ based on home ownership.*

H3b: *The perceptions, adoption, and use of Smart Home Devices are positively associated with household size.*

H3c: *The perceptions, adoption, and use of Smart Home Devices are negatively associated with the presence of children.*

3 Method

We addressed our research questions via an online questionnaire deployed on the Prolific crowd work platform.[1] The following subsections describe the study design, recruitment procedures, and sample characteristics. The

1 https://www.prolific.co/

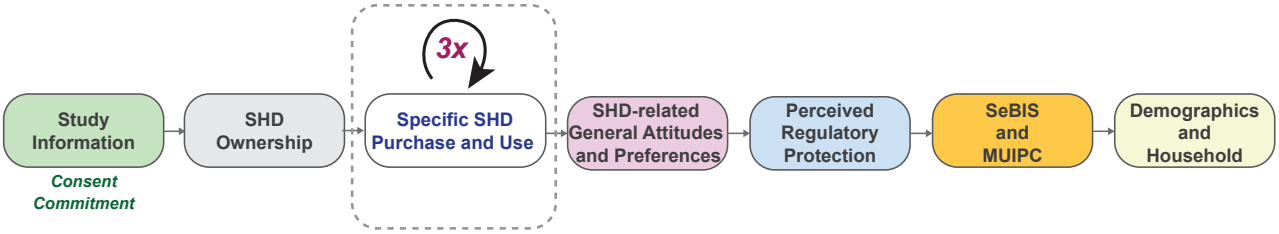

Fig. 1. The organization and flow of the various components of the questionnaire. The block of questions within the dotted rectangle was repeated three times for three specific Smart Home Devices (SHD).

Technical University of Munich does not require ethics approval for questionnaire-based online studies. We followed the standard procedures for ethical research, seeking informed consent prior to participation and not collecting personally identifiable information. We hosted the questionnaire on the SoSci platform,[2] compliant with the EU GDPR.

3.1 Questionnaire

Figure 1 shows the organization and flow of the various components of the questionnaire we developed for the study. We divided the questionnaire into four main parts:

1. **Consent and Introduction:** At the beginning, we provided information about the study to seek informed consent for participation. Upon consent, we asked a 'commitment question' to seek a commitment to respond attentively [4]. We then informed participants of the scope of the study by providing a definition of Smart Home Devices as "any appliances or technologies that enhance the functionality of the home. Such devices aim to provide features not otherwise available to the household. Further, the devices may combine and automate routine domestic tasks. As such, Smart Home Devices aim to increase the quality, safety, and efficiency of domestic life." We further informed participants that "general purpose devices, such as smartphones and smartphone voice assistants" were not deemed as Smart Home Devices within the scope of the research.
   Next, the participants provided information regarding their knowledge and ownership of 20 Smart Home Devices based on popular device categories listed in the Statista Digital Market Outlook for the year 2019 [51]. We chose the 20 Smart Home Devices to cover a variety of common domestic functions: entertainment, home monitoring for security, domestic assistance, lighting, and climate control [51].
2. **Use of Specific Smart Home Devices:** In the second part, we asked the participants a set of questions regarding their use of three specific Smart Home Devices chosen randomly from those they indicated owning in response to the earlier question. If a participant owned two or fewer devices, we picked devices at random to complete the bucket of three devices, with the wording of the questions for the randomly selected devices changed to reflect hypothetical, instead of actual, ownership. When asking hypothetical questions, we excluded a few questions, such as price, purchase location, etc., which would not have made sense in the hypothetical.
3. **Attitudes and Preferences Regarding Smart Home Devices:** Next, we asked the participants several sets of questions pertaining to Smart Home Devices in general. These questions covered topics such as perceived regulatory protection, updates and service, privacy and security aspects, etc. Additionally, we included two standard scales from the literature to measure relevant privacy attitudes (Mobile Users' Information Privacy Concern [MUIPC] [65]) and the intention to engage in secure usage practices (Security Behavior Intention Scale [SeBIS] [20]). Based on relevance to our study, we used only the 'Perceived Surveillance,' 'Perceived Intrusion,' and 'Secondary Use of Personal Information' subscales within the MUIPC scale and adapted the items to the Smart Home Device context by replacing the terms 'mobile app' or 'mobile device' with the term 'Smart Home Device.' Similarly, we used only the 'Device Securement,' 'Proactive Awareness,' and 'Updating' subscales within SeBIS and dropped the 'Password Generation' subscale because it was not relevant to our research. Further, we replaced the 5-point choice options used in the

2 https://www.soscisurvey.de/en/index

	Age					Gender		
Region	n	Median	Mean	SD	Minimum	Maximum	Female	Male	Non-binary
US	143	30	32.62	10.25	19	69	53.85% (77)	44.06%(63)	2.10%(3)
UK	155	35	37.03	12.07	19	70	69.03%(107)	30.97%(48)	0.00%(0)
GS	133	27	29.15	7.97	19	58	36.84% (49)	63.16%(84)	0.00%(0)

Table 1. Summary of participant demographics split by the three regions covered in the study.

original SeBIS with 7-point choice options consistent with the rest of the questions in the questionnaire.

4. **Demographics:** At the end, we collected standard demographic information, including household characteristics relevant to our hypotheses (see Section 2.4.3).

We embedded a question within the study to check for attentive participation. Prior to deploying the study, we conducted several pilots of the questionnaire with individuals unconnected to the research and made iterative improvements based on the feedback from these pilots. The English version of the questionnaire is included in the Appendix. We translated the English version into German for deployment within the GS region. Note that the authors include native speakers of both languages, with three of the four authors being fluent in English and German.

3.2 Participant Recruitment

We recruited participants during November and December of 2019 by using several filters provided by the Prolific platform to solicit individuals from the targeted populations. Specifically, we advertised the English version of the study to those located in the US and the UK and the German version to those residing in the GS region. Although the UK has retained the GDPR despite leaving the EU, it is socially different from the GS region, and the US differs from the UK and GS regions in regulatory as well as social aspects.

To ensure high-quality responses, we required that participants have a task approval rating of 95% or higher and be fluent in the respective languages without any language-related disorders. In addition, we restricted participation to those who use a screen-based device (e.g., smartphone, tablet, laptop, desktop, etc.) more than once a week.

Those who qualified to participate based on the selection criteria and chose to accept the task received a link to the online questionnaire. The participants could respond to the questionnaire using any device of their choice. A "Return to Prolific" link on the final page of the questionnaire enabled the participants to indicate the completion of the task on the Prolific platform.

We recruited participants from the US and the UK from the 8th to the 15th of November and those from the GS region from the 25th of November to the 7th of December, 2019. To avoid any influence of sampling at specific times or on particular days, we spread out the recruiting efforts over the recruitment period by releasing three batches of seven study slots each day, distributed evenly across the day with a five-hour gap, the first at 10am, the second at 3pm, and the last at 8pm local time in the respective time zones[3] of the regions targeted for recruitment.

The participants took about 20 minutes on average to complete the questionnaire. We paid the participants the equivalent of £1.80, which was the compensation suggested by the Prolific platform.

3.3 Sample

Prolific timed out nineteen individuals who accepted the task but did not complete it within 56 minutes. Twenty-eight individuals returned the task without completing, and we removed five others who did not enter a valid prolific ID. Further, we excluded ten participants who did not provide a country of residence or indicated residing in a country outside the three targeted regions, nine who did not certify attentive participation at the end of the study, and eight who failed the attention check embedded within the questionnaire. After these exclusions, we were left with 431 valid responses, distributed roughly evenly across the three targeted regions (US: 143, UK: 155, and GS: 133). Table 1 provides an

3 For the United States, we used the Eastern time zone.

Region	Types of Smart Home Devices				
	0	**1**	**2**	**3**	**> 3**
US	22	41	24	24	32
UK	18	43	36	34	24
GS	17	31	19	34	32
TOTAL	57	115	79	92	88

Table 2. The distribution of participants based on *the number of types of Smart Home Devices* they reported owning, split by the three regions covered in the study.

overview of the demographics of the sample. Table 2 shows the distribution of these 431 individuals in terms of the *number of types of Smart Home Devices* they reported owning.

3.4 Limitations

Our data is affected by the inherent limitations of self-selection and self-reporting. Moreover, we cannot claim that the participants constitute a representative sample of people from the respective regions.

Our sample is drawn from the regions we selected based on the considerations of access (e.g., our own locations), resource constraints (e.g., translation and recruitment expenses), and availability of novel technologies at relatively early stages (e.g., technological advancement). While the sample does not cover all regions in the world, it is substantially broader than the small samples within a single country typically included in most empirical investigations. We invite future work that replicates our study for comparisons with populations from regions that we did not cover.

Three of the authors fluent in English and German translated the questionnaire from English to German. We conducted multiple pilots in each language to ensure a match in the meaning of the questions in the two versions. However, it is possible that some questions might have been interpreted differently in the two languages.

3.5 Analysis

Whenever the sample size was sufficiently large to tolerate violations of the assumption of normality, we tested our hypotheses (see Section 2.4) using ANOVAs, with follow-up Tukey Honestly Significant Difference (HSD) tests, t-tests, or Pearson correlation tests. Otherwise, we compared means with the Wilcoxon rank-sum tests (single comparisons) or Dunn's tests (multiple pairwise comparisons). Where applicable, we accounted for conducting multiple statistical tests by adjusting the corresponding p-values with Bonferroni correction.

4 Findings

We measured *perceptions* regarding Smart Home Devices in terms of *perceived privacy risk* and *perceived manufacturer responsibility* for the maintenance and security of the device, each measured on a 7-point scale. For obtaining a measure of the *adoption* and *use* of Smart Home Devices, we excluded the 57 participants who indicated not owning any Smart Home Devices. For the rest, we considered the *number of types of Smart Home Devices* owned as a measure of the *adoption* of Smart Home Devices.

We measured the *use* of Smart Home Devices based on the responses of the participants to the question that asked how often they interacted with each of the three owned devices they were asked about. Since only a handful of the participants owned several of the devices we listed in the questionnaire, we did not have sufficient statistical power for analyzing the *use* of the entire set of devices. Therefore, we measured *use* by considering only the three devices reported to be owned the most: Smart Speakers, Smart TVs, and Smart Light Bulbs. Three hundred twenty-nine participants (men = 49.85%, women = 49.85%, non-binary = 0.30%, median age = 30) reported owning at least one of these three Smart Home Devices (Smart TV = 231, Smart Speaker = 140, and Smart Light Bulb = 92) and, in turn, answered the questions about their *use*. The subsample of these 329 participants provided sufficient statistical power for examining the relationships between the *use* of these devices and the other variables of interest (see Sections 4.1.2, 4.2.2, and 4.3). Analyses that do not involve the *use* variable are based on the full set of responses.

We present the findings pertaining to each research question in turn.

4.1 Perceived Regulatory Protection for Personal Data

We measured *perceived regulatory protection* by averaging the participant responses to three Likert-type items scored on a scale of 1 (Strongly Disagree) to 7 (Strongly Agree). Specifically, these items asked the participants

	Correlation (r)	t	df	p
Perceived Regulatory Protection	**−0.17**	**−3.55**	**429**	**0.0017****
Smart TV	−0.18	−3.88	429	0.0004***
Smart Speaker	−0.16	−3.26	429	0.0036**
Smart Light Bulb	−0.09	−1.87	429	0.1860
Unwanted Access	**−0.16**	**−3.44**	**429**	**0.0026****
Smart TV	−0.17	−3.59	429	0.0011**
Smart Speaker	−0.17	−3.59	429	0.0011**
Smart Light Bulb	−0.10	−2.03	429	0.1303
Unwanted Sharing	**−0.16**	**−3.36**	**429**	**0.0034****
Smart TV	−0.19	−3.94	429	0.0003***
Smart Speaker	−0.15	−3.07	429	0.0069**
Smart Light Bulb	−0.08	−1.64	429	0.3063
Unwanted Processing and Analysis	**−0.16**	**−3.42**	**429**	**0.0028****
Smart TV	−0.17	−3.65	429	0.0009***
Smart Speaker	−0.13	−2.76	429	0.0183*
Smart Light Bulb	−0.08	−1.74	429	0.2510
Statistical significance levels:	$^{*}: p < 0.05$	$^{**}: p < 0.01$	$^{***}: p < 0.001$	

Table 3. Correlations between *perceived privacy risk* and *perceived regulatory protection* as well as its individual facets, for all Smart Home Devices in general (bold) and each of the three most-owned Smart Home Devices considered separately.

to indicate their levels of agreement with the following statements:
"I feel that current laws and regulations are adequate to protect my Smart Home Device data from:

1. ... unwanted access by third parties."
2. ... unwanted sharing with third parties."
3. ... unwanted processing and analysis by third parties."

We averaged the responses to the above three items to derive an overall measure of *perceived regulatory protection* along with the perceived protection for each of its three facets listed above. We used these measures to address H1 (see Section 2.4.1).

4.1.1 Perception

We found that *perceived privacy risk* exhibits a statistically significant negative correlation with *perceived regulatory protection*, overall as well as split into its various facets (see Table 3). For the three most-owned Smart Home Devices mentioned above (i.e., Smart TVs, Smart Speakers, and Smart Light Bulbs), we found that the statistically significant negative correlations between *perceived privacy risk* and *perceived regulatory protection* hold for Smart TVs and Smart Speakers, but not for Smart Light Bulbs.

We additionally examined the relationship between *perceived regulatory protection* and the MUIPC construct of *perceived intrusion* as the latter measure was provided by all participants regardless of whether they owned a Smart Home Device. In line with the results for *perceived privacy risk*, *perceived intrusion* showed a statistically significant negative correlation with *perceived regulatory protection* ($r = -0.37$, $t = -8.30$, $df = 429$, $p \sim 0$). Interestingly, the correlation was much stronger for non-users ($r = -0.57$, $t = -5.18$, $df = 55$, $p \sim 0$) than for users ($r = -0.33$, $t = -6.66$, $df = 372$, $p \sim 0$) of Smart Home Devices. In contrast, we found a statistically significant positive correlation between *perceived intrusion* ($r = 0.12$, $t = 2.46$, $df = 429$, $p = 0.014$) and *perceived manufacturer responsibility* for ensuring that Smart Home Devices are private and secure.

Overall, the above findings support hypothesis H1a that *perceived regulatory protection* is positively associated with positive *perceptions* regarding Smart Home Devices. As noted above, higher *perceived regulatory protection* is associated with lower perceptions of intrusion and privacy risk from Smart Home Devices. However, the strength of the association can vary for specific devices. Moreover, we found that greater *perceived intrusion* is associated with users ascribing greater responsibility to manufacturers for providing private and secure device operation.

4.1.2 Use

We found a small positive correlation between *perceived regulatory protection* and the *number of types of Smart Home Devices* owned ($r = 0.11$, $t = 2.21$, $df = 429$, $p = 0.028$), suggesting that perception of greater legal protection is associated with greater *adoption* of Smart Home Devices. The result indicates that *perceived regulatory protection* is likely to be one of the factors related to the *adoption* of Smart Home Devices, thus supporting hypothesis H1b. That said, we did not find a statistically significant relationship when separately examining each of the three facets of *perceived regulatory protection*, i.e., *unwanted access by third parties*, *unwanted sharing with third parties*, and *unwanted processing and analysis by third parties*. The results suggest that the various aspects of data handling covered by regulatory protection can create a cumulative influence stronger than that for each of the aspects considered separately.

When evaluating hypothesis H1c pertaining to the *use* of the three most-owned Smart Home Devices, we found statistically significant positive correlations between *perceived regulatory protection* and *use* for Smart TVs ($r = 0.17$, $t = 2.53$, $df = 229$, $p = 0.036$) and Smart Speakers ($r = 0.27$, $t = 3.278$, $df = 138$, $p = 0.004$). The *use* of Smart Light Bulbs was uncorrelated with *perceived regulatory protection* ($p = 0.783$).

Our results can only partially support hypothesis H1c that higher *perceived regulatory protection* is associated with greater *use* of Smart Home Devices. In particular, the relationship appears to hold only for some devices. Interestingly, the results suggest that the relationship might be present in the case of devices that provide more complex functionality and interactive capabilities, such as Smart TVs, but not for single-function ones, such as Smart Light Bulbs.

4.2 Cross-Regional Aspects

We examined the impact of the cross-regional aspects captured in RQ2 (see Section 1) by comparing the responses of the participants from the US, UK, and GS regions. In these analyses, we verified that the imbalances in the age and gender distributions across the three regions (see Table 1) do not affect the results.

4.2.1 Perception

Of the three participant groups, those from the GS region attributed the highest *perceived privacy risk* to Smart Home Devices. Additionally, compared to the participants from the GS region, we found that those from the two English-speaking regions placed greater responsibility for privacy and security on the manufacturers than on themselves (US mean = 4.66, UK mean = 4.57, GS mean = 3.92; ANOVA: $F = 6.17$, $p = 0.002$, US-GS: $p = 0.004$, UK-GS: $p = 0.012$). While such differences are observable for non-users in these regions as well (US mean = 4.77, UK mean = 5.06, GS mean = 3.65), they are not statistically significant.

We further examined the differences across the regions for the various *perceived benefits* of Smart Home Devices measured on corresponding Likert-type items from 1 (Strongly Disagree) to 7 (Strongly Agree) (see Table 4). As Table 4 shows, those from the English-speaking regions were aligned with each other, with no statistically significant differences in perceived benefits between them except for increasing property value. However, the responses of those from the English-speaking and GS regions for the various *perceived benefits* of Smart Home Devices were statistically significantly different. The participants from the US and the UK perceived that Smart Home Devices provide greater benefits for enhancing leisure activities, providing care, and increasing property value, while those from the GS region perceived that the greatest benefit of Smart Home Devices is providing comfort.

The various differences in the perceptions regarding the risks, responsibilities, and benefits pertaining to Smart Home Devices support hypothesis H2a. In particular, we found that the perceptions of those from the GS region differ from those from the US and the UK, with the latter two mostly aligned with each other.

4.2.2 Use

We conducted ANOVAs for cross-regional comparisons regarding the *adoption* of Smart Home Devices overall. We found no statistically significant differences in the *number of types of Smart Home Devices* in the households in the three regions covered in the study. When split by region, we found that the statistically significant positive correlation between *perceived regulatory protection* and the *adoption* of Smart Home Devices (see Section 4.1.2) holds only for the GS region ($r = 0.21$, $t = 2.40$, $df = 131$, $p = 0.05$). In other words, peo-

Perceived Benefit (Mean)	Comparison	F	df	Pr(>F)	Adjusted p
Enhancing leisure activities	US (5.45) - GS	5.44	2	0.0047**	0.0036**
	UK - GS (4.88)				0.4376
	US - UK (5.09)				0.0866
Providing peace of mind	US (5.27) - GS	4.09	2	0.0174*	0.0396*
	UK - GS (4.83)				0.0296*
	US - UK (5.28)				0.9977
Providing comfort	US (5.43) - GS	10.94	2	0.0000***	0.0007***
	UK - GS (6.00)				0.0000***
	US - UK (5.34)				0.8137
Increasing safety	US (5.30) - GS	6.10	2	0.0025**	0.0044**
	UK - GS (4.73)				0.0111*
	US - UK (5.24)				0.9314
Providing care	US (4.77) - GS	7.22	2	0.0008***	0.0084**
	UK - GS (4.23)				0.0011**
	US - UK (4.86)				0.8499
Increasing property value	US (4.93) - GS	9.43	2	0.0001***	0.0001***
	UK - GS (4.11)				0.1640
	US - UK (4.45)				0.0246*
Statistical significance levels:	* : $p < 0.05$	** : $p < 0.01$	*** : $p < 0.001$		

Table 4. ANOVA results showing the comparisons for the various *perceived benefits* of Smart Home devices on a scale of 1 (Strongly Disagree) to 7 (Strongly Agree) across the three regions covered in the study, with adjusted p values obtained via post-hoc Tukey HSD tests. The numbers in the parentheses in the 'Comparison' column provide the corresponding mean score for the respective region.

ple in the GS region seem more likely to adopt Smart Home Devices only if they feel protected by regulation. These results support hypothesis H2b that the *adoption* of Smart Home Devices differs between the regions. Further, the lack of a statistically significant relationship between the *adoption* of Smart Home Devices and *perceived regulatory protection* for the US and the UK indicates that these differences may be driven by regional influences that need further scrutiny.

A Dunn's test found no statistically significant differences across the three regions in terms of the overall *use* of the most-owned Smart Home Devices. However, when examining the most-owned Smart Home Devices separately, we found that those in the GS region reported using Smart TVs somewhat less often than those from the two English-speaking regions (US: 2.29, UK: 2.34, GS: 2.03). A Dunn's test confirmed that the differences between the English-speaking and GS regions are statistically significant (US-GS: $Z = -2.59$, $p = 0.019$; UK-GS: $Z = -3.13$, $p = 0.005$). The *use* of the other devices did not differ across the regions. Similarly, we did not find any statistically significant differences between the regions regarding whether the participants disabled any features of their Smart Home Devices. With the exception of Smart TVs, our data does not support hypothesis H3c that the *use* of Smart Home Devices differs across the three regions covered in our study. However, the differences in Smart TV use might be attributable to the regional differences in *TV viewing habits* [54] rather than to the *smart* aspects of the TV (see Section 5.2.2).

4.3 Characteristics of the Home

RQ3 addresses the connection between Smart Home Devices and household characteristics. Specifically, we examined the influence of *home ownership*, *number of household members*, and the *presence of children*.

4.3.1 Home Ownership

We compared the *perception*, *adoption*, and *use* of Smart Home Devices between those who own a home vs. those who rent. We found that homeowners reported owning a higher *number of types of Smart Home Devices* on average (Mean number of types of Smart Home Devices: homeowners = 2.54 vs. renters = 2.15; $t = 2.17$, $p = 0.031$). There were no statistically significant differences in the *perception* and *use* of Smart Home Devices

based on home ownership. Similarly, an ANOVA comparing the *use* of the three most-owned Smart Home Devices by homeowners and renters was not statistically significant. In summary, our data provides partial support for hypothesis H3a, i.e., the *adoption* of Smart Home Devices is higher for homeowners, but their *perception*, and *use* appears to be unrelated to home ownership.

4.3.2 Number of Household Members

When trying to understand the impact of the *household size*, i.e., the number of people living in the household, we considered the *number of types of Smart Home Devices* in the home. Considering the unique *types* of devices instead of the total number of devices avoids the results being affected by the physical size of the home, since larger homes can be expected to have several devices of the same kind (e.g., smart speakers in multiple rooms). We found no statistically significant relationships between *household size* and the *perceptions* or *use* of Smart Home Devices. However, we did find a statistically significant positive correlation between *household size* and the *number of types of Smart Home Devices* ($r = 0.19$, $t = 4.07$, $df = 429$, $p = 0.0002$). These results partially support hypothesis H3b that larger household sizes are associated with greater *adoption* of Smart Home Devices.

4.3.3 Presence of Children

Children are considered a protected class in most privacy and other regulation. Since Smart Home Devices are likely to impact children's privacy, we used t-tests to examine the relationships between their presence in the household and the *perceptions*, *adoption* and *use* of these devices. we found no statistically significant differences in the *perceptions* based on the *presence of children*. However, those with children tended to report a higher *number of types of Smart Home Devices* (means: parents = 2.75, non-parents = 2.09; $t = -3.42$, $df = 219$, $p < 0.001$). Interestingly, the t-tests revealed that people with children reported statistically significantly higher ($t = -2.47$, $p = 0.04$) *use* of Smart Home Devices (mean = 2.39) compared to that reported by those without children (mean = 2.20). Upon further examination, we found that parents reported greater *use* of Smart TVs compared to non-parents (means 2.40 vs. 2.15 for parents and non-parents, respectively; $t = -2.40$, $p < 0.05$). However, the differences between parents and non-parents for Smart Speakers and Smart Light Bulbs were not statistically significant. We additionally found that the responses of parents showed a greater preference for voice-based interaction with Smart Home Devices via Smart Speakers or voice-based Smart Assistants on smartphones (Smart Speaker: means 4.95 vs. 4.21 for parents and non-parents, respectively; $t = -3.33$, $p < 0.007$; Smart Assistant: means 5.03 vs. 4.18 for parents and non-parents, respectively; $t = -4.59$, $p \sim 0.000$). Contradictory to hypothesis H3c, the *presence of children* appears to be associated positively with the *adoption* of Smart Home Devices. At the same time, the results partially support hypothesis H3c, i.e., the *presence of children* is associated with the differences in the *use* of some Smart Home Devices based on their functionality and interactive modes, particularly voice.

5 Discussion

Smart Home Devices are often rife with security vulnerabilities and bugs that impact user privacy. Our focus in the study was on the operation as *intended* by the manufacturer, without the presence of such unintended security issues. Similarly, manufacturers who intentionally violate laws and regulation are outside the scope of our study. That said, our study indirectly captures the impact of the typically poor attention to privacy and security by the manufacturers of these devices based on the extent to which the awareness of this matter impacts people's perceptions, adoption, and use. Although the focus of our study was on users of Smart Home Devices, our sample does include non-users. Therefore, our results reflect views of non-users as well, similar to the literature in this space (see Sections 2.2).

While the effect sizes of many of our statistically significant results are small, they are still noteworthy given the complex and highly contextual nature of privacy. Moreover, many of our measures are based on averaging multiple items, thus adding robustness to the observations.

Below, we discuss the salient insight provided by our findings for each base topic, i.e., regulation, region, and household.

5.1 Regulation

As mentioned in Section 4.1, we measured *perceived regulatory protection* with three items, in line with the number of items typically included in specific subscales of larger scales in the literature. It should be noted that the items are not about any *specific* law, but about any and all applicable regulation pertaining to privacy and security.

5.1.1 Perceptions – Perceived Regulatory Protection Is Associated with Lower Perceived Privacy Risk.

Our results show that *perceived regulatory protection* is negatively associated with the *perceived privacy risk* of using Smart Home Devices. Specifically, the risk assessments of the participants for Smart TVs and Smart Speakers were lower when they perceived greater protection from regulation. In contrast, the participants who used Smart Home Devices but did not believe that regulation could sufficiently protect their privacy felt that the devices pose greater risks. We found no statistically significant relationship between *perceived regulatory protection* and *manufacturer responsibility* for privacy and security protection, indicating that people do not appear to grasp or trust the role that regulation plays in creating obligations for the device manufacturers to protect user privacy and security and, in turn, in enforcing compliance with these obligations.

As common in the literature, we captured whether people *perceive* that they are protected by regulation, regardless of their knowledge of the specifics. The extent to which people's perceptions are connected to an accurate understanding of the regulatory specifics is outside the scope of our research questions. In future work, it would be useful to investigate *perceived regulatory protection* at a finer granularity by examining specific regulatory measures in the context of Smart Home Devices. For example, it would be interesting to explore whether users of Smart Home Device in the EU recognize their rights related to data erasure [46] or portability [56] under the GDPR and whether those in other regions would appreciate equivalent regulatory protection.

5.1.2 Adoption – Perceived Regulatory Protection May Facilitate the Adoption of Smart Home Devices.

We found that *perceived regulatory protection* is positively associated with the *adoption* of Smart Home Devices. As uncovered in previous research, purchase behavior differs between those who already own Smart Home Devices and first-time buyers [22]. Therefore, we investigated the decision to adopt Smart Home Devices in relation to *perceived regulatory protection* by splitting our sample into two groups: those who reported owning Smart Home Devices and those who did not. The mean for *perceived regulatory protection* for the non-owners was 2.36, whereas the owners of Smart Home Devices indicated perceiving higher protection from regulation (mean = 3.22). To check whether the apparent distrust of the non-owners regarding regulatory protection is connected to a greater awareness of privacy and security issues, we conducted a t-test to compare their MUIPC scores with those of the device owners. Interestingly, we found that the MUIPC mean for non-owners was *higher* than that for the device owners (5.87 vs. 5.23, $t = -3.73$, $p \sim 0.000$).

5.1.3 Use – Smart Home Device Use Is Related to Perceived Regulatory Protection.

Although we found that *perceived regulatory protection* is associated with greater *use* of Smart Home Devices *in general*, the association between *perceived regulatory protection* and *use* can vary across *specific* Smart Home Devices. Overall, the *use* of Smart Speakers exhibited the strongest correlation with *perceived regulatory protection*. The relationship might be driven by differences in *perceived privacy risk* since the participants deemed Smart Speakers to pose the highest privacy risk among the three most-owned Smart Home Devices (Mean privacy risk: Smart TVs = 3.59, Smart Speakers = 4.05, and Smart Light Bulbs = 2.26; ANOVA: $F = 105.10$, $p \sim 0.000$).

Additionally, we found that in 5.32% of the cases, owners of Smart Home Devices disabled one or more features of these devices. In open-ended responses, participants who owned Smart TVs stated that they switched off their Internet capabilities, disabled apps, and turned off the voice features. Some of those who reported owning Smart Speakers mentioned turning the devices off or actively disabling their voice-based capabilities to protect privacy. These findings are in line with the Hadan

and Patil's [27] work in which users reported trying to protect their privacy with radical actions such as switching devices off. Yet, the proportion of device owners who reported disabling features or turning the devices off is rather small (36/329, 10.94%) indicating that resignation to ongoing privacy encroachment might be widespread [34, 48, 49].

5.2 Region

We found that *perceptions*, *adoption*, and *use* of Smart Home Devices exhibited differences as well as similarities across the three regions covered in our study.

5.2.1 Perceptions – The Perceptions Toward Smart Home Devices Can Vary Across Regions.

Across their life cycles, devices are typically supported by the manufacturers who issue software updates that often enhance privacy and security along with providing other fixes. Counterintuitively, we found that the participants who reported perceiving greater regulatory protection, placed lower responsibility on the manufacturers for protecting privacy and security. Further research is needed to unpack this relationship.

5.2.2 Adoption – Smart Home Device Adoption Differs Across Regions.

In 2022, the worldwide market penetration of Smart Home Devices is estimated to reach 14.20% (adjusted for COVID-19), with the UK having the highest adoption at 45.80%, followed by the United States with 43.80% [52]. The GS region lags notably behind the UK and the US in the market penetration of Smart Home Devices, with Germany at 31.60%, Switzerland at 27.60%, and Austria at 26.60% [52]. These differences are reflected at the level of specific devices as well. For instance, Germany[4] has Smart TVs in the fewest households (65%) and UK residents in the most (73%), with the United States roughly in the middle (70%) [33]. The responses of the participants are generally consistent with these observations.

4 In cases where information for all three countries in the GS region is not available collectively or separately, we report numbers for the individual countries for which data is available.

5.2.3 Use – Smart Home Device Use May Be Similar Across Regions.

Surprisingly, we found no statistically significant differences across the three regions we studied in terms of the overall reported *use* of Smart Home Devices. While we did find that those from the GS region differed from those from the two English-speaking regions in their use of Smart TVs, the finding could be explained partially by the fact that Germans[4] on average watch TV to a lesser extent [54]. As mentioned above, fewer German households own Smart TVs compared to those from the other two regions we studied, which could further explain the result.

5.3 Household Characteristics

Apart from the differences in lifestyle based on larger regional influences, households differ in terms of parameters such as the number of inhabitants. Our findings show that the differences in the *perceptions*, *adoption*, and *use* of Smart Home Devices can be associated with variations in such household parameters.

5.3.1 Perceptions – Users Expect Greater Protection from the Manufacturers of Intrusive Devices.

We examined the relationship between the *perceived intrusion* construct in MUIPC with *manufacturer responsibility* for protecting privacy and security in the operation of Smart Home Devices. The participants who reported feeling greater intrusion were more likely to place the manufacturer in the position of taking care of vulnerabilities and bugs by updating the software as necessary. In other words, instead of demanding greater user control and taking charge of managing their own privacy and security in response to intrusive data practices of these devices, users seem to demand that the manufacturers act responsibly and protect their privacy and security.

SeBIS contains a construct that measures *proactive awareness* when interacting with devices, e.g., how an individual deals with matters such as suspicious links on the Internet. Individuals indicating high *proactive awareness* can be expected to be careful when dealing with their Smart Home Devices. However, we did not find a statistically significant relationship between *proactive awareness* and *manufacturer responsibility* or the *desire for privacy* (for adults, children, guests, or

pets), indicating that being proactively aware of privacy and security threats might be unrelated to the desire to guard against them when using Smart Home Devices. People do not seem to see a need for taking proactive actions to protect the privacy of themselves or others in the household even when they feel that their Smart Home Devices are invasive.

5.3.2 Adoption – Homeowners Adopt Smart Home Devices to a Greater Extent.

The GS region has a comparatively low home-ownership rate, with 50.40% of German households being owner-occupied in 2020, with Austria at 55.30% (2020), and Switzerland at 42.30% (2020) [24]. In contrast, the United States has a comparatively high home-ownership rate, with 67.90% of households occupied by homeowners in the second quarter of 2020 [59]. In the UK, 65.20% of the households were owner-occupied in 2018 [24]. These regional differences in home-ownership rates and their influence on living arrangements are further intertwined with local historical, economic, and cultural influences in these regions.

Homeowners are likely to be reasonably affluent to be able to afford purchasing Smart Home Devices and have greater agency to install them within the home. In contrast, renters may not find it as convenient or feasible to install many Smart Home Devices, such as Smart Refrigerators, Smart Dishwashers, Smart Heating/Cooling Systems, etc. In addition, such devices tend to be more expensive, thus putting them out of reach of a large proportion of people. Since relatively few people in our sample reported owning devices other than the three most-owned ones, we do not have enough statistical power to test for the differences based on home ownership for the other Smart Home Devices included in our study. Future work should target larger samples of users of each device to examine how home ownership affects its adoption.

While it could be argued that homeowners are likely to be older, thus potentially less technically savvy, the data on homeowners indicates that all age ranges from 18 onward in the US [53], UK [14], and Germany[4] [45] contain a notably high proportion of homeowners. In fact, a majority of those in the 35-44 range in all three regions report owning homes. Moreover, the homeowners in our sample are from an online platform, thus likely to be reasonably comfortable with technology. Therefore, it is unlikely that our results are influenced by differences in technological orientation and expertise between homeowners and renters.

5.3.3 Use – Smart Home Device Use Can Vary Based on Household Size and the Presence of Children.

We confirmed that people interact differently with Smart Home Devices depending on the makeup of their households. This observation is further supported by the options chosen by the participants when explaining why they do *not* use Smart Home Devices. Excluding unaffordability (51.97%), the top three options selected were respectively: "I wish to preserve the privacy of the adults in my household" (74.49%); "I wish to preserve the privacy of my children" (48.96%); and "I wish to preserve the privacy of my guests" (41.53%).

Yet, parents must balance the desire for privacy with the competing need for convenience. We found that the *presence of children* in the household was associated with a greater preference for interacting with Smart Home Devices via voice commands. The preference may be the result of the convenience of invoking the functionality of the Smart Home Device in a hands-free manner because of the inability or inconvenience of using other modes of interaction while attending to children.

6 Implications

Our insight can be applied to improve the handling of privacy and security matters connected to Smart Home Devices in at least three distinct ways. We discuss each below.

6.1 Policy

As our findings show, the regulatory context can influence the market for Smart Home Devices through impacting the adoption of new devices as well as the use of currently owned devices. The generally low level of *perceived regulatory protection* in the responses indicates insufficient levels of trust toward the government. Non-users, in particular, trust device manufacturers even less, thus inhibiting adoption.

Region-specific regulation, such as the EU GDPR, may not be sufficient in the Smart Home domain. Of

course, the basic GDPR principles like minimizing unnecessary data collection during Internet use can, and should, apply to Smart Home Devices. Yet, the GDPR does not apply to several other facets of Smart Home Devices. For instance, the data that Smart Home Devices deal with may be explicitly provided, sensed, inferred, or predicted. GDPR arguably does not cover all of these types of data [17, 56]. As a result, for handling the privacy and security aspects of their Smart Home Devices, users may need to rely on good faith self-regulation from the manufacturers of the devices.

To that end, the manufacturers of Smart Home Devices could benefit from the Privacy by Default approach promoted by Willis et al. [63], with a particular attention to the collection, transmission, storage, and use of the various data streams handled by the device. While providing greater user privacy by default can potentially increase the costs of software development and lower the opportunities for using user data for business purposes, our findings suggest that these costs might be offset by greater use by those who value the regulatory protection and place importance on trusting the manufacturers with responsible handling of data protection. Further, privacy-preserving default settings could potentially convince current non-users to adopt the devices and become users.

In addition to refining the existing regulation, policymakers can promote the creation and use of privacy- and security-enhancing (technical) standards for Smart Home Devices, addressing the lack of trust of users and non-users. The development of an industry standard that addresses user concerns by committing to common privacy and security features can increase manufacturer accountability regarding these matters. Our findings suggested that an increase in manufacturer accountability can serve to engender user trust and increase the adoption and use of their products. Therefore, manufacturers should have a clear interest in cooperating with legislators and industry organizations for developing technical standards and regulatory frameworks.

6.2 Technology

Users currently have little insight and control over the data that leaves the local Smart Home ecosystem and gets transferred to the Internet. Except for receiving security patches, many Smart Home Devices do not need to communicate with servers outside of the home to provide their functionality. For instance, devices such as Smart Locks, Smart Light Bulbs, Smart appliances (e.g., Smart Dishwasher, Smart Coffee Maker, etc.) could be deployed to operate with limited or no Internet access, thus lowering the potential privacy and security threats, including those resulting from lax attention to privacy and security by the device manufacturers. To that end, we echo the suggestion of Yao et al. [66] that Smart Home Devices include a feature that enables end users to disconnect the devices from the Internet quickly and seamlessly, while still being available to use within the domestic perimeter.

In addition, users of Smart Home Devices can benefit from the ability to view, monitor, and manage the outgoing device connections and data flows for each individual device via a simple, concise interface, thereby adding transparency and control. To enable transparency regarding the types of data Smart Home Devices send to the Internet, users need a quick and convenient mechanism that categorizes the data streams. The upcoming 'Thread' standard for Smart Home Devices, for instance, could integrate these specifications [60]. Further, compliance with such standards could act as a trusted signal of regulatory compliance that assures users and raises their awareness of privacy and security protection pertaining to Smart Home Devices. Implementation of such a feature may require the integration of two pieces: the Smart Home Device that is in charge of capturing the data and the router that controls the data flows between the Smart Home and the Internet.

6.3 End Users

We further propose user interface enhancements that enable more nuanced privacy-protective actions. That said, adding granularity and control is typically associated with greater user burden and higher device costs. Understanding the optimal trade-off between these competing factors requires empirical investigation.

6.3.1 Enabling Privacy Settings by Room

Smart Home Devices can be invasive because they occupy the living quarters of their users. Since many of the devices require specifying the room in which they are located, we propose the provision of a mechanism to regulate privacy settings on a room-by-room basis. With such a feature, settings could auto-adjust when a Smart Home Device is moved to another room. For instance, when a Smart Speaker is moved from the living

room to the bedroom, it can automatically change its data practices to match the privacy expectations for the bedroom.

6.3.2 Showing Data Access at Setup

Easily understandable information on the operation and data practices of Smart Home Devices is typically unavailable. To this end, initial setup of these devices can emulate the setup procedures used for the installation of apps on mobile devices where privacy-invasive features require that the app disclose its data practices and seek appropriate permissions.

7 Conclusion

In a multi-region study of user expectations and practices related to Smart Home Devices, we found that variations in perceived regulatory protection, regional influences, and household characteristics are associated with differences in the perceptions, adoption, and use of these devices. Moreover, we found that these differences can vary for specific devices. Importantly, our findings suggest that a stronger regulatory environment could help increase user trust and boost the adoption of Smart Home Devices. Effective policy interventions can thus simultaneously serve the interests of the users, policymakers, and device manufacturers. Our findings underscore the importance of developing a broad understanding that includes multiple regions and a variety of Smart Home Devices when studying user preferences and practices. Given the regional differences across the globe in what constitutes a "home," we call for additional research to cover understudied regions that are likely to be emerging markets for Smart Home Devices.

Acknowledgments

We thank the participants of the study. We appreciate the help of the colleagues who piloted the study and provided feedback. We are grateful to the anonymous reviewers for their constructive comments. Jens Grossklags gratefully acknowledges support from the Bavarian Research Institute for Digital Transformation (bidt). Sameer Patil's involvement in the research was supported through a Visiting Professorship at the Technical University of Munich funded as part of the Bavarian State Ministry's visiting professor program. The content of the paper is the work of the authors and does not necessarily reflect the views of the sponsors.

References

[1] N. Abdi, K. M. Ramokapane, and J. M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 451–466, Santa Clara, CA, Aug 2019. USENIX Association. https://www.usenix.org/conference/soups2019/presentation/abdi.

[2] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, 2005. https://doi.org/10.1109/MSP.2005.22.

[3] F. K. Aldrich. Smart homes: Past, present and future. In R. Harper, editor, *Inside the Smart Home*, pages 17–39. Springer London, London, UK, 2003. https://doi.org/10.1007/1-85233-854-7_2.

[4] H. Allcott and M. Gentzkow. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2):211–236, May 2017. https://doi.org/10.1257/jep.31.2.211.

[5] K. Ashton. That 'Internet of Things' thing. *RFID Journal*, 22(7):97–114, 2009.

[6] N. M. Barbosa, Z. Zhang, and Y. Wang. Do privacy and security matter to everyone? Quantifying and clustering user-centric considerations about smart home device adoption. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 417–435. USENIX Association, Aug 2020. https://www.usenix.org/conference/soups2020/presentation/barbosa.

[7] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004. https://doi.org/10.1080/01972240490507956.

[8] California State Legislature. California consumer privacy act of 2018, 2018. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[9] J. Campbell. That smart TV you just bought may be spying on you, FBI warns. *CNN Politics*, Dec 2019. https://www.cnn.com/2019/12/02/politics/smart-tv-fbi-warning-cyber-monday/index.html.

[10] G. Cecere, F. Le Guel, and N. Soulié. Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change*, 96:277–287, 2015. https://doi.org/10.1016/j.techfore.2015.01.021.

[11] M. Chan, E. Campo, D. Estève, and J.-Y. Fourniols. Smart homes — Current features and future perspectives. *Maturitas*, 64(2):90–97, 2009. https://doi.org/10.1016/j.maturitas.2009.07.014.

[12] H. Cho, B. Knijnenburg, A. Kobsa, and Y. Li. Collective privacy management in social media: A cross-cultural validation. *ACM Trans. Comput.-Hum. Interact.*, 25(3), Jun 2018. https://doi.org/10.1145/3193120.

[13] H. Cho, M. Rivera-Sánchez, and S. S. Lim. A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3):395–416, 2009. https://doi.org/10.1177/1461444808101618.

[14] D. Clark. Percentage of households who own their home in the United Kingdom in 2017, by age of household reference person, 2019. https://www.statista.com/statistics/988842/household-ownership-in-the-uk/.

[15] B. Copos, K. Levitt, M. Bishop, and J. Rowe. Is anybody home? Inferring activity from smart home network traffic. In *2016 IEEE Security and Privacy Workshops*, SPW, pages 245–251, 2016. https://doi.org/10.1109/SPW.2016.48.

[16] M. De Boni and M. Prigmore. Cultural aspects of Internet privacy. In *Information Systems Research, Teaching and Practice: Proceedings of the 7th Annual UKAIS Conference*, Apr 2002. http://eprints.hud.ac.uk/id/eprint/4207.

[17] P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 34(2):193–203, 2018. https://doi.org/10.1016/j.clsr.2017.10.003.

[18] L. Dogruel and S. Joeckel. Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and U.S. smartphone users. *International Journal of Communication*, 13, Apr 2019. https://ijoc.org/index.php/ijoc/article/view/9824.

[19] P. Dourish and K. Anderson. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human–Computer Interaction*, 21(3):319–342, 2006. https://doi.org/10.1207/s15327051hci2103_2.

[20] S. Egelman and E. Peer. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2873–2882, New York, NY, USA, 2015. Association for Computing Machinery. https://doi.org/10.1145/2702123.2702249.

[21] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *2020 IEEE Symposium on Security and Privacy*, IEEE S&P 2020, pages 447–464, 2020. https://doi.org/10.1109/SP40000.2020.00043.

[22] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–12, New York, NY, USA, 2019. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300764.

[23] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504.

[24] Eurostat. Distribution of population by tenure status, type of household and income group – EU-SILC survey, 2022. https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_lvho02&lang=e.

[25] R. Garg. An analysis of (non-)use practices and decisions of Internet of Things. In D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, and P. Zaphiris, editors, *Human-Computer Interaction*, volume 11749 of *Lecture Notes in Computer Science, INTERACT 2019*, pages 3–24, Cham, 2019. Springer International Publishing. https://doi.org/10.1007/978-3-030-29390-1_1.

[26] M. Ghiglieri, M. Volkamer, and K. Renaud. Exploring consumers' attitudes of smart TV related privacy risks. In T. Tryfonas, editor, *Human Aspects of Information Security, Privacy and Trust*, volume 10292 of *Lecture Notes in Computer Science, HAS 2017*, pages 656–674, Cham, 2017. Springer International Publishing. https://doi.org/10.1007/978-3-319-58460-7_45.

[27] H. Hadan and S. Patil. Understanding perceptions of smart devices. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, and M. Sala, editors, *Financial Cryptography and Data Security*, volume 12063 of *Lecture Notes in Computer Science, FC 2020*, pages 102–121, Cham, 2020. Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_8.

[28] J. Haney, Y. Acar, and S. Furman. "It's the Company, the Government, you and I": User perceptions of responsibility for smart home privacy and security. In *30th USENIX Security Symposium*, USENIX Security 2021, pages 411–428. USENIX Association, Aug 2021. https://www.usenix.org/conference/usenixsecurity21/presentation/haney.

[29] J. M. Haney, S. M. Furman, and Y. Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In A. Moallem, editor, *HCI for Cybersecurity, Privacy and Trust*, volume 12210 of *Lecture Notes in Computer Science, HCII 2020*, pages 393–411, Cham, 2020. Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_26.

[30] G. Hofstede. Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture, Unit 2*, 2(1), Dec 2011. https://doi.org/10.9707/2307-0919.1014.

[31] T. Jakobi, S. Patil, D. Randall, G. Stevens, and V. Wulf. It is about what they could do with the data: A user perspective on privacy in smart metering. *ACM Trans. Comput.-Hum. Interact.*, 26(1), Jan 2019. https://doi.org/10.1145/3281444.

[32] O. Kulyk, B. Reinheimer, L. Aldag, P. Mayer, N. Gerber, and M. Volkamer. Security and privacy awareness in smart environments – A cross-country investigation. In M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, and M. Sala, editors, *Financial Cryptography and Data Security*, volume 12063 of *Lecture Notes in Computer Science, FC 2020*, pages 84–101, Cham, 2020. Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_7.

[33] F. Laricchia. Share of individuals who have access to a smart TV in their household in 2020, by country, 2020. https://www.statista.com/statistics/1107844/access-to-smart-tv-in-households-worldwide/.

[34] J. Lau, B. Zimmerman, and F. Schaub. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), Nov 2018. https://doi.org/10.1145/

3274371.

[35] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang. Smart home: Architecture, technologies and systems. *Procedia Computer Science*, 131:393–400, 2018. Recent Advancement in Information and Communication Technology. https://doi.org/10.1016/j.procs.2018.04.219.

[36] R. Y. M. Li, H. Li, C. Mak, and T. Tang. Sustainable smart home and home automation: Big data analytics approach. *International Journal of Smart Home*, 10(8):177–187, 2016. https://ssrn.com/abstract=2834497.

[37] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner. Privacy attitudes of Smart Speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4):250–271, Oct 2019. https://doi.org/10.2478/popets-2019-0068.

[38] C. L. Miltgen and D. Peyrat-Guillard. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2):103–125, 2014. https://doi.org/10.1057/ejis.2013.17.

[39] D. Mocrii, Y. Chen, and P. Musilek. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, 1–2:81–98, 2018. https://doi.org/10.1016/j.iot.2018.08.009.

[40] Mozilla. 46 gadgets slapped with *privacy not included warning labels in mozilla's annual holiday shopping guide, Nov 2021. https://foundation.mozilla.org/en/blog/46-gadgets-slapped-with-privacy-not-included-warning-labels-in-mozillas-annual-holiday-shopping-guide/.

[41] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security*, SOUPS 2017, pages 399–412, Santa Clara, CA, Jul 2017. USENIX Association. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

[42] S. Nikou. Consumers' perceptions on smart home and smart living. In *Twenty-Sixth European Conference on Information Systems*, ECIS 2018, 2018. https://aisel.aisnet.org/ecis2018_rp/47.

[43] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of social life*. Stanford University Press, Redwood City, CA, USA, 2009. https://doi.org/10.1515/9780804772891.

[44] Y. T. Park, P. Sthapit, and J.-Y. Pyun. Smart digital door lock for the home automation. In *2009 IEEE Region 10 Conference*, TENCON 2009, pages 1–6, 2009. https://doi.org/10.1109/TENCON.2009.5396038.

[45] V. Pawlik. Wohnsituation in der Bevölkerung in Deutschland nach Altersgruppen im Jahr 2021, 2022. https://de.statista.com/statistik/daten/studie/273824/umfrage/wohnsituation-der-bevoelkerung-in-deutschland-nach-altersgruppen/.

[46] E. Rupp, E. Syrmoudis, and J. Grossklags. Leave no data behind – Empirical insights into data erasure from online services. *Proceedings on Privacy Enhancing Technologies*, 2022(3), 2022.

[47] K. Sarikakis and L. Winter. Social media users' legal consciousness about privacy. *Social Media + Society*, 3(1), 2017. https://doi.org/10.1177/2056305117695325.

[48] J. S. Seberger, M. Llavore, N. N. Wyant, I. Shklovski, and S. Patil. Empowering resignation: There's an app for that. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery. https://doi.org/10.1145/3411764.3445293.

[49] J. S. Seberger, E. Swiatek, I. Shklovski, and S. Patil. Still creepy after all these years: The normalization of affective discomfort in app use. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery. https://doi.org/10.1145/3491102.3502112.

[50] P. Somerville. The social construction of home. *Journal of Architectural and Planning Research*, 14(3):226–245, 1997.

[51] Statista Digital Market Outlook. Smart Home report 2019, 2019.

[52] Statista Digital Market Outlook. Smart Home report 2021, 2021. https://www.statista.com/study/42112/smart-home-report/.

[53] Statista Research Department. Homeownership rate in the United States as of 2nd quarter 2021, by age, 2021. https://www.statista.com/statistics/1036066/homeownership-rate-by-age-usa/.

[54] J. Stoll. Average daily on-demand TV and video viewing time in selected countries worldwide as of October 2018, by age group (in hours), Statista, 2018. https://www.statista.com/statistics/276748/average-daily-tv-viewing-time-per-person-in-selected-countries.

[55] J. Sturgess, J. R. C. Nurse, and J. Zhao. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *Living in the Internet of Things: Cybersecurity of the IoT – 2018*, pages 1–8, 2018. https://doi.org/10.1049/cp.2018.0037.

[56] E. Syrmoudis, S. Mager, S. Kuebler-Wachendorff, P. Pizzinini, J. Grossklags, and J. Kranz. Data portability between online services: An empirical analysis on the effectiveness of GDPR Art. 20. *Proceedings on Privacy Enhancing Technologies*, 2021(3):351–372, 2021. https://doi.org/10.2478/popets-2021-0051.

[57] M. Tabassum, T. Kosinski, and H. R. Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security*, SOUPS 2019, pages 435–450, Santa Clara, CA, Aug 2019. USENIX Association. https://www.usenix.org/conference/soups2019/presentation/tabassum.

[58] S. Trepte, L. Reinecke, N. B. Ellison, O. Quiring, M. Z. Yao, and M. Ziegele. A cross-cultural perspective on the privacy calculus. *Social Media + Society*, 3(1), 2017. https://doi.org/10.1177/2056305116688035.

[59] United States Census Bureau. Quarterly residential vacancies and homeownership, Third Quarter 2020, Oct 2020. Release Number: CB20-153. https://www.census.gov/housing/hvs/files/qtr320/Q320press.pdf.

[60] I. Unwala, Z. Taqvi, and J. Lu. Thread: An IoT protocol. In *2018 IEEE Green Technologies Conference*, GreenTech 2018, pages 161–167, 2018. https://doi.org/10.1109/GreenTech.2018.00037.

[61] R. H. Weber and E. Studer. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 32(5):715–728, 2016. https://doi.org/10.1016/j.clsr.2016.

07.002.

[62] M. Williams and J. R. C. Nurse. Optional data disclosure and the online privacy paradox: A UK perspective. In T. Tryfonas, editor, *Human Aspects of Information Security, Privacy, and Trust*, volume 9750 of *Lecture Notes in Computer Science, HAS 2016*, pages 186–197, Cham, 2016. Springer International Publishing. https://doi.org/10.1007/978-3-319-39381-0_17.

[63] L. E. Willis. Why not privacy by default? *Berkeley Technology Law Journal*, 29(1):61–133, 2014. https://www.btlj.org/data/articles2015/vol29/29_1/29-berkeley-tech-l-j-0061-0134.pdf.

[64] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin. Benefits and risks of smart home technologies. *Energy Policy*, 103:72–83, 2017. https://doi.org/10.1016/j.enpol.2016.12.047.

[65] H. Xu, S. Gupta, M. B. Rosson, and J. M. Carroll. Measuring mobile users' concerns for information privacy. In *Thirty-Third International Conference on Information Systems*, ICIS 2012, pages 2278–2293. Association for Information Systems, 2012. https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10.

[66] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–12, New York, NY, USA, 2019. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300428.

[67] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, Jul 2017. USENIX Association. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

[68] J. Zhao, G. Wang, C. Dally, P. Slovak, J. Edbrooke-Childs, M. Van Kleek, and N. Shadbolt. 'I make up a silly name': Understanding children's perception of privacy risks online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–13, New York, NY, USA, 2019. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300336.

[69] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home IoT privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), Nov 2018. https://doi.org/10.1145/3274469.

Appendix: Questionnaire

The questionnaire contained the following components:

Consent and Introduction

Statement of Informed Consent

You are being invited to participate in a research study on Smart Home Devices. This study is being done by [Names of Researchers] from [University].

Purpose of This Study: In this study, we aim to investigate people's preferences and use of Smart Home technologies.

Procedures to Be Followed: After providing your Prolific ID, you will proceed to answer a series of questions. You are required to enter your Prolific ID and click the confirmation link at the end of the survey.

Discomforts and Risks: We do not anticipate any risks from participating in this study beyond those experienced in everyday life. Your responses and behavior during the study will NOT be used to identify you in any way.

Duration/Time: On average, the study takes about 20 minutes.

Confidentiality: Your participation in this study is confidential. Your responses are anonymous. We do not ask for any personally identifiable information. Your name is not linked to your responses in any way. The reporting or presentation of the results of the research will not contain any personally identifiable information.

Questions?: If you have any questions, concerns, or complaints about the study, please contact any of the researchers: [Contact Information of the Researchers]

Payment for Successful Participation: For completing the study, you will receive compensation of £1.80 via Prolific.

Voluntary Participation: Your decision to participate in this study is strictly voluntary. You may stop at any time. You do not have to answer any questions that you do not wish to answer. Your decision to participate in the study will not affect your relationship with the [University]. Completion of the study implies that you have read and understood the information on this page and consent to taking part in this research.

- Do you agree with the above terms for participating in the study?
  - ○ Yes
  - ○ No

Commitment

- We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in the study.
  Will you provide your best answers to each question in this study?
  - ○ I will provide my best answers.
  - ○ I will NOT provide my best answers.
  - ○ I cannot promise either way.

Preferences and Knowledge Regarding Smart Home Devices

The following sections of the questionnaire ask about Smart Home Devices. Before you proceed, we would like to explain what we mean by Smart Home Devices.

Smart Home Devices are any appliances or technologies that enhance the functionality of the home. Such devices aim to provide features not otherwise available to the household. Further, the devices may combine and automate routine domestic tasks. As such, Smart Home Devices aim to increase the quality, safety, and efficiency of domestic life.

NOTE: We are primarily interested in your thoughts and experiences regarding Smart Home Devices that fit the above characterization. General purpose devices, such as smartphones and smartphone voice assistants, are NOT the main focus of the study.

- In your opinion, which of the household devices listed below would benefit from Smart capabilities?
  - ○ Coffee Maker
  - ○ Dishwasher
  - ○ Door Lock
  - ○ Doorbell
  - ○ Electricity Meter
  - ○ Electrical Outlet
  - ○ Fridge
  - ○ Gardening Equipment
  - ○ Heating/Cooling System
  - ○ Home Monitoring System
  - ○ Light Bulb
  - ○ Oven
  - ○ Speaker
  - ○ Stove
  - ○ TV
  - ○ Thermostat
  - ○ Toy
  - ○ Vacuum Cleaner
  - ○ Washing Machine
  - ○ Other (Please specify): [Text field]
- In your opinion, which of household devices listed below would present a security risk if they were equipped with Smart capabilities?
  - ○ Coffee Maker
  - ○ Dishwasher
  - ○ Door Lock
  - ○ Doorbell
  - ○ Electricity Meter
  - ○ Electrical Outlet
  - ○ Fridge
  - ○ Gardening Equipment
  - ○ Heating/Cooling System
  - ○ Home Monitoring System
  - ○ Light Bulb
  - ○ Oven
  - ○ Speaker
  - ○ Stove
  - ○ TV
  - ○ Thermostat
  - ○ Toy
  - ○ Vacuum Cleaner
  - ○ Washing Machine
  - ○ Other (Please specify): [Text field]
- On a scale of 1 to 7, please indicate the extent to which you believe the following functionalities add Smart capabilities to a device:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  - ○ Playing media content (e.g., videos, music, etc.)
  - ○ Controlling appliances (e.g., lights, coffee maker, stove, oven, etc.)
  - ○ Adjusting internal climate (e.g., temperature, air quality, etc.)
  - ○ Managing power consumption
  - ○ Detecting malfunction
  - ○ Monitoring health
  - ○ Improving safety
  - ○ Enabling more communication modes (e.g., voice, text, email, etc.)
  - ○ Other (Please specify): [Text field]
- On a scale of 1 to 7, please indicate the extent to which you find the following factors to be benefits of Smart Home technologies:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  - ○ Saving money
  - ○ Saving energy

- ○ Increasing convenience
- ○ Enhancing leisure activities
- ○ Providing peace of mind
- ○ Providing comfort
- ○ Increasing safety
- ○ Providing care
- ○ Improving the quality of life
- ○ Increasing property value
- ○ Other (Please specify): [Text field]

- On a scale of 1 to 7, please indicate the extent to which you use Smart Home Devices for the following purposes:
  (1 indicates 'Not at all' and 7 indicates 'All the time.')
  - ○ Controlling appliances (e.g., lights, coffee maker, stove, oven, etc.)
  - ○ Controlling home monitoring systems
  - ○ Communicating with the inside of the home (e.g. calling Smart Home Devices within the home)
  - ○ Communicating with the outside of the home (e.g. using a video doorbell or home monitoring system installed on the outside of the home)
  - ○ Automating tasks
  - ○ Other (Please specify): [Text field]
- How would you rate your experience in using Smart Home Devices?
  (1 indicates 'Very Unfamiliar' and 7 indicates 'Very Familiar.')
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ 5
  - ○ 6
  - ○ 7
- How would you rate your overall knowledge of Smart Home Devices?
  (1 indicates 'Very Unfamiliar' and 7 indicates 'Very Familiar.')
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ 5
  - ○ 6
  - ○ 7

Questions on Specific Smart Home Devices[5]

The next section of the questionnaire will ask you to indicate the Smart Home Devices you own. We will then ask you questions about three of the devices you own. If you own fewer than three devices, we will ask you hypothetical questions that you can answer by imagining that you own the device.

- Which of the following Smart Home Devices do you own? (*Select all that apply.*)
  - □ Smart Coffee Maker
  - □ Smart Dishwasher
  - □ Smart Door Lock
  - □ Smart Doorbell
  - □ Smart Electricity Meter
  - □ Smart Electrical Outlet
  - □ Smart Fridge
  - □ Smart Gardening Equipment
  - □ Smart Heating/Cooling System
  - □ Smart Home Monitoring System
  - □ Smart Light Bulb
  - □ Smart Oven
  - □ Smart Robot
  - □ Smart Speaker
  - □ Smart Stove
  - □ Smart TV
  - □ Smart Thermostat
  - □ Smart Toy
  - □ Smart Vacuum Cleaner
  - □ Smart Washing Machine
  - □ Other (Please specify): [Text field]

The following set of questions pertain to your [device].

- *What was the purchase price of the [device] in US Dollars? (You may convert currencies at: https://www.xe.com)
  - ○ Free/Gift

5 In this set of questions, the term [device] was replaced with one of the three specific Smart Home Devices owned by the participant from the list of 20 devices included in the questionnaire. The set of questions was repeated three times, once per device. If a participant owned two or fewer devices, we picked devices at random to complete the bucket of three devices and asked a subset of the questions with the wording of the questions for the randomly picked devices changed to reflect hypothetical, instead of actual, ownership. The questions marked with a * do not make sense in the hypothetical and were asked only if the participant owned the device in question.

- ○ Less than $5
- ○ $5.01 - $10.00
- ○ $10.01 - $20.00
- ○ $20.01 - $40.00
- ○ $40.01 - $60.00
- ○ $60.01 - $80.00
- ○ $80.01 - $100.00
- ○ $100.01 - $120.00
- ○ $120.01 - $140.00
- ○ $140.01 - $160.00
- ○ $160.01 - $180.00
- ○ $180.01 - $200.00
- ○ $200.01 - $250.00
- ○ $250.01 - $300.00
- ○ $300.01 - $350.00
- ○ $350.01 - $400.00
- ○ $400.01 - $450.00
- ○ $450.01 - $500.00
- ○ $500.01 - $750.00
- ○ $750.01 - $1000.00
- ○ $1000.01 - $1250.00
- ○ $1250.01 - $1500.00
- ○ $1500.01 - $2000.00
- ○ $2000.01 - $2500.00
- ○ $2500.01 - $3000.00
- ○ More than $3000

- *Where did you purchase this [device]?
  - ○ Budget online store from your own country
  - ○ Online store from another country
  - ○ Brick-and-mortar store other than that of the manufacturer (but not a general purpose or departmental store)
  - ○ Brick-and-mortar general purpose or departmental store
  - ○ Received as a gift
  - ○ Other (Please specify): [Text field]
- *Did you purchase a used [device]?
  - ○ Yes
  - ○ No
- What [is/would be] the primary use of the [device]? (*Select all that apply.*)
  - ☐ Increasing convenience
  - ☐ Saving money
  - ☐ Reducing power consumption
  - ☐ Providing safety for household members
  - ☐ Automating tasks
  - ☐ Experimenting with the latest trends in technology
  - ☐ Other (Please specify): [Text field]
- *Why did you purchase the [device]?
  [Text field]
- Which of the following sources [did/would] you consult prior to purchasing a [device]? (*Select all that apply.*)
  - ○ Online reviews
  - ○ Online forums
  - ○ Print media (e.g., Newspapers, Magazines, etc.)
  - ○ Friends and Family
  - ○ Online news sites
  - ○ Other (Please specify): [Text field]
- How [did you hear/have you heard] about the [device] you purchased? (*Select all that apply.*)
  - ☐ TV
  - ☐ Internet
  - ☐ Print media (e.g., Newspapers, Magazines, etc.)
  - ☐ Friends and Family
  - ☐ Brick-and-mortar store
  - ☐ Trade show
  - ☐ Other (Please specify): [Text field]
- *On a scale of 1 to 7, please indicate your level of agreement with the following statements as they pertain to your [device].
  (1 indicates 'Never' and 7 indicates 'Always.')
  - ○ I believe my [device] possesses adequate security measures to protect my data.
  - ○ My [device] has adequate security measures to prevent third-party access to my data.
- *Do you continue to educate yourself about the [device] after purchase (e.g., via tutorials)?
  - ○ Yes
  - ○ No
- *[If the answer to the question 'Do you continue to educate yourself about the [device] after purchase (e.g., via tutorials)?' is 'Yes']
  Please tell us how you continue to educate yourself?
  [Text field]
- *How long ago was the [device] purchased?
  - ○ 0-6 months
  - ○ 7-12 months
  - ○ 13-24 months
  - ○ 25-36 months
  - ○ 37-48 months
  - ○ More than 48 months
- *On average, how often do you use the [device] each day?
  - ○ 0 times
  - ○ 1-5 times
  - ○ 6-10 times
  - ○ 11-20 times
  - ○ 21-30 times
  - ○ 30+ times
  - ○ Don't know

- *Is the [device] always on?
  - ○ Yes
  - ○ No
  - ○ Don't know
- [Have you disabled/Would you disable] any of the features of the [device]?
  - ○ Yes
  - ○ No
- [If the answer to the question '[Have you disabled/Would you disable] any of the features of the [device]?' is 'Yes']
  Which feature(s) of the [device], if any, [did/would] you disable?
  [Text field]
- If you mentioned disabling any feature(s) above, why [did/would] you disable the above feature(s)? (*Select all that apply.*)
  - ☐ Conserving battery life
  - ☐ Reducing power consumption
  - ☐ Protecting your privacy
  - ☐ Reducing security risks
  - ☐ Enhancing the user experience
  - ☐ Turning off unneeded or unused features
  - ☐ Other (Please specify): [Text field]
- Which types of data do you believe the [device] [uses/would use]? (*Select all that apply.*)
  - ☐ Location
  - ☐ Routines
  - ☐ Speech (via microphone)
  - ☐ Video (via camera)
  - ☐ Still images (via camera)
  - ☐ Environmental parameters (e.g., temperature, humidity, noise levels, etc.)
  - ☐ Internet activity
  - ☐ Online purchases
  - ☐ Offline purchases
  - ☐ Power consumption
  - ☐ Activities and gestures
  - ☐ Other (Please specify): [Text field]
- Where do you believe the [device] [stores/would store] data? (*Select all that apply.*)
  - ☐ On the Internet router in the home
  - ☐ On a cloud platform
  - ☐ Locally on the device itself
  - ☐ Servers of the Internet Service Provider (ISP)
  - ☐ Servers of the [device] manufacturer
  - ☐ Servers of third parties
  - ☐ Other (Please specify): [Text field]
- Where in your home [is/would] the [device] [be] located? (*Select all that apply.*)
  - ☐ Attic
  - ☐ Balcony
  - ☐ Basement
  - ☐ Children's room
  - ☐ Dining room
  - ☐ Garage
  - ☐ Guest bedroom
  - ☐ Hallway
  - ☐ Kitchen
  - ☐ Living room
  - ☐ Master bedroom
  - ☐ Patio
  - ☐ Yard
  - ☐ Other (Please specify): [Text field]
- How [do/would] you interact with the [device]? (*Select all that apply.*)
  - ○ Voice Assistant
  - ○ App on your phone
  - ○ Physical buttons on the [device]
  - ○ Screen on the [device]
  - ○ Internet-based service connected to the [device]
  - ○ Home Internet router
  - ○ Other (Please specify): [Text field]

Attitudes and Preferences

- On a scale of 1 to 7, please indicate how you would rate the privacy risks for each of the following devices:
  (1 indicates the 'Lowest Risk' and 7 indicates the 'Highest Risk.')
  - ○ Smart Coffee Maker
  - ○ Smart Dishwasher
  - ○ Smart Door Lock
  - ○ Smart Doorbell
  - ○ Smart Electricity Meter
  - ○ Smart Electrical Outlet
  - ○ Smart Fridge
  - ○ Smart Gardening Equipment
  - ○ Smart Heating/Cooling System
  - ○ Smart Home Monitoring System
  - ○ Smart Light Bulb
  - ○ Smart Oven
  - ○ Smart Robot
  - ○ Smart Speaker
  - ○ Smart Stove
  - ○ Smart TV
  - ○ Smart Thermostat
  - ○ Smart Toy
  - ○ Smart Vacuum Cleaner
  - ○ Smart Washing Machine

- In your opinion, what risks, if any, are posed by the use of Smart Home Devices? [Text field]
- I may decide NOT to own Smart Home Devices for my home because: (*Select all that apply.*)
  - ☐ I wish to preserve the privacy of the adults in my household.
  - ☐ I wish to preserve the privacy of my children.
  - ☐ I wish to preserve the privacy of my guests.
  - ☐ I wish to preserve the privacy of my pets.
  - ☐ I perceive no benefit from using Smart Home Devices.
  - ☐ I find Smart Home Devices too expensive.
  - ☐ I do not have a domestic Internet connection suitable for the use of Smart Home Devices.
  - ☐ Other (Please specify): [Text field]
- For each of the following scenarios, indicate your level of comfort for controlling a Smart Home Device on a scale of 1 to 7:
  (1 indicates 'Extremely Uncomfortable' and 7 indicates 'Extremely Comfortable.')
  - ○ While you are at home
  - ○ While you are away from home
  - ○ From someone else's device or equipment
  - ○ From your own device or equipment
- For each of the following methods, indicate your level of comfort for using it to interact with a Smart Home Device on a scale of 1 to 7:
  (1 indicates 'Extremely Uncomfortable' and 7 indicates 'Extremely Comfortable.')
  - ○ Voice commands via a Smart Speaker
  - ○ Voice commands via a Voice Assistant on a smartphone
  - ○ Smartphone App for the device
  - ○ Smartphone Widgets or Shortcuts
  - ○ Sensors inside the home (e.g., motion sensors, light sensors, etc.)
  - ○ Sensors outside the home (e.g., motion sensors, light sensors, etc.)
  - ○ Automatic operation based on device programming
  - ○ Other (Please specify): [Text field]
- Between yourself and the manufacturer of a typical Smart Home Device, please indicate who you believe is more responsible for handling each of the following matters on a scale of 1 to 7:
  (1 indicates yourself, 4 both equally, and 7 the manufacturer.)
  - ○ Keeping the Smart Home Device software up-to-date
  - ○ Ensuring my privacy
  - ○ Protecting my Smart Home ecosystem as a whole
  - ○ Keeping the Smart Home Device secure
  - ○ Fixing hardware failure
  - ○ Fixing software failure
- On a scale of 1 to 7, please indicate the extent to which you agree with the following statements:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  - ○ My Smart Home Device should update itself.
  - ○ The manufacturer of my Smart Home Device should provide regular security updates.
  - ○ The servers of my Smart Home Device manufacturer should be equipped with adequate data security.
  - ○ The manufacturer of my Smart Home Device should remotely manage my Smart Home Device.
  - ○ I regularly make sure that my Smart Home Devices are kept up-to-date.
  - ○ I receive a timely notice when the manufacturer stops supporting my Smart Home Device.
  - ○ I am unsure if my Smart Home Device receives security updates.
  - ○ My Smart Home Device should receive updates as long as I use it.
- [If at least one of the 20 listed Smart Home Devices is checked in response to the question 'Which of the following Smart Home Devices do you own? (*Select all that apply.*)']
  On a scale of 1 to 7, please indicate the extent to which you agree with the following statements:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  My purchase of a Smart Home Device was influenced by:
  - ○ Low price
  - ○ Bundled offer (e.g., including other devices with purchase of one or more devices)
  - ○ Trial (e.g., 30-day free use of a service)
  - ○ Periodic sale
  - ○ Discount (e.g., coupons)
- On a scale of 1 to 7, please indicate your level of comfort with using Smart Home Devices purchased from each of the following stores:
  (1 indicates 'Extremely Uncomfortable' and 7 indicates 'Extremely Comfortable.')
  - ○ Budget online store from your own country
  - ○ Online store from another country

- ○ Brick-and-mortar store other than that of the manufacturer (but not a general purpose or departmental store)
- ○ Brick-and-mortar general purpose or departmental store

- On a scale of 1 to 7, please indicate the extent to which you agree with the following statements:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  I feel that current laws and regulations are adequate to protect my Smart Home Device data from:
  - ○ . . . unwanted access by third parties.
  - ○ . . . unwanted sharing with third parties.
  - ○ . . . unwanted processing and analysis by third parties.

  I feel that there are sufficient penalties in places for:
  - ○ . . . those who access my data without authorization.
  - ○ . . . those who share my data without permission.
  - ○ . . . those who do not employ proper safeguards for storing my data.
- On a scale of 1 to 7, please indicate the extent to which you agree with the following statements:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  - ○ I am aware of the kinds of data collected by my Smart Home Device.
  - ○ Smart Home Device data has monetary value.
  - ○ Smart Home Device data is collected by companies.
  - ○ Smart Home Device data is gathered regularly by a Smart Home Device.
  - ○ Smart Home Device data is sent continuously over the Internet.
  - ○ Smart Home Device data is a resource for corporations.
  - ○ Smart Home Device data is stored remotely.
  - ○ I am aware of where my Smart Home Device stores data.
  - ○ I am aware that my Smart Home Device data is analyzed to know about my preferences and practices.
  - ○ I am aware of the parties who analyze my Smart Home Device data.
  - ○ I would like my Smart Home Device data to be stored in my home.
  - ○ I would like my Smart Home Device data to be stored outside my home.
  - ○ I would like my Smart Home Device data to be processed and analyzed within my home.
  - ○ I would like my Smart Home Device data to be processed and analyzed outside of my home.
- On a scale of 1 to 7, please indicate your level of agreement with the following statements:
  (1 indicates 'Never' and 7 indicates 'Always.')
  [NOTE: The items below are based on the Security Behavior Intentions Scale (SeBIS) [20]. Items marked with ^{r} are reverse coded. The comments in parentheses after the items indicate the corresponding SeBIS subscales. The subscale lables were not included in the questionnaire.]
  - ○ I set my computer screen to lock automatically if I don't use it for a prolonged period of time. [Subscale: Device Securement]
  - ○ I use a password/passcode to unlock my laptop or tablet. [Subscale: Device Securement]
  - ○ I manually lock my computer screen when I step away from it. [Subscale: Device Securement]
  - ○ I use a PIN or passcode to unlock my mobile phone. [Subscale: Device Securement]
  - ○ When someone sends me a link, I open it without first verifying where it goes.^{r} [Subscale: Proactive Awareness]
  - ○ I know what website I'm visiting based on its look and feel rather than by looking at the URL bar.^{r} [Subscale: Proactive Awareness]
  - ○ I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon).^{r} [Subscale: Proactive Awareness]
  - ○ Please choose Never. [NOTE: Attention Check]
  - ○ When browsing websites, I mouse over links to see where they go before clicking them. [Subscale: Proactive Awareness]
  - ○ If I discover a security problem, I continue what I was doing because I assume someone else will fix it.^{r} [Subscale: Proactive Awareness]
  - ○ When I'm prompted about a software update, I install it right away. [Subscale: Updating]
  - ○ I try to make sure that the programs I use are up-to-date. [Subscale: Updating]
  - ○ I verify that my anti-virus software has been regularly updating itself. [Subscale: Updating]
- On a scale of 1 to 7, please indicate your level of agreement with the following statements:
  (1 indicates 'Strongly Disagree' and 7 indicates 'Strongly Agree.')
  [NOTE: These items are based on the Mobile Users' Information Privacy Concern (MUIPC) scale [65]. The comments in parentheses after the items indi-

cate the corresponding MUIPC subscales. The subscale lables were not included in the questionnaire.]

- ○ I believe that the location of my Smart Home Device is monitored at least part of the time. [Subscale: Perceived Surveillance]
- ○ I am concerned that Smart Home Devices are collecting too much information about me. [Subscale: Perceived Surveillance]
- ○ I am concerned that apps may monitor my activities on my Smart Home Device. [Subscale: Perceived Surveillance]
- ○ I feel that as a result of my using Smart Home Devices, others know about me more than I am comfortable with. [Subscale: Perceived Intrusion]
- ○ I feel that as a result of my using Smart Home Devices, information about me that I consider private is now more readily available to others than I would want. [Subscale: Perceived Intrusion]
- ○ I feel that as a result of my using Smart Home Devices, information about me is out there that, if used, will invade my privacy. [Subscale: Perceived Intrusion]
- ○ I am concerned that Smart Home Devices may use my personal information for other purposes without notifying me or getting my authorization. [Subscale: Secondary Use of Personal Information]
- ○ When I give personal information to use Smart Home Devices, I am concerned that apps may use my information for other purposes. [Subscale: Secondary Use of Personal Information]
- ○ I am concerned that Smart Home Devices may share my personal information with other entities without getting my authorization. [Subscale: Secondary Use of Personal Information]

Demographics

- How old are you?
  - ○ Below 18
  - ○ 18–25
  - ○ 26–35
  - ○ 36–45
  - ○ 46–55
  - ○ 56–65
  - ○ 66–75
  - ○ Older than 75
- What is your gender?
  - ○ Male
  - ○ Female
  - ○ Non-binary
  - ○ Something else (Please specify): [Text field]
- What is the highest level of education you have completed? (If currently enrolled, indicate the highest degree received.)
  - ○ Less than high school
  - ○ High school diploma
  - ○ Vocational training
  - ○ Some college (no degree)
  - ○ Bachelor's degree (B.S., B.A., or other degree)
  - ○ Master's degree
  - ○ Doctoral degree
  - ○ Professional graduate degree (e.g., law or medical degree)
  - ○ Other (Please specify): [Text field]
- How many children do you have?
  - ○ 0
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ 5
  - ○ 6 or more
- How many people live in your household (including you)?
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ 5
  - ○ 6
  - ○ More than 6
- What is your annual household income before taxes in US Dollars? (You may convert currencies at: https://www.xe.com)
  - ○ Less than $10,000
  - ○ $10,000 to $19,999
  - ○ $20,000 to $29,999
  - ○ $30,000 to $39,999
  - ○ $40,000 to $49,999
  - ○ $50,000 to $59,999
  - ○ $60,000 to $69,999
  - ○ $70,000 to $79,999
  - ○ $80,000 to $89,999
  - ○ $90,000 to $99,999
  - ○ $100,000 or more
  - ○ Prefer not to say
- Do you own or rent your home?
  - ○ Own

  - ○ Rent
  - ○ Something else (Please specify): [Text field]
- What is your ethnic background? (*Select all that apply.*)
  - ☐ African
  - ☐ Asian
  - ☐ Hawaiian
  - ☐ Hispanic
  - ☐ Native American
  - ☐ White
  - ☐ Something else (Please specify): [Text field]
- What is your current employment status? (*Select all that apply.*)
  - ☐ Employed full-time
  - ☐ Employed part-time
  - ☐ Unemployed looking for work
  - ☐ Unemployed NOT looking for work
  - ☐ Homemaker
  - ☐ Student
  - ☐ Retired
  - ☐ Something else (Please specify): [Text field]
- [If employed] What is your occupation? [Text field]
- [If student] What is your field of study? [Text field]
- Did you answer all questions in the study according to the provided instructions?
  Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.
  - ○ I answered all questions according to the provided instructions.
  - ○ I sometimes chose random answer options because I was not motivated to answer the question or did not know how to answer it.
  - ○ I often chose random answer options because I wanted to finish as quickly as possible.
- Could you complete the questionnaire without distractions?
  Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.
  - ○ I completed the study with full attention.
  - ○ I was sometimes distracted (by people, noises, etc.).
  - ○ I was often distracted (by people, noises, etc.).
- Please enter your Prolific ID to complete your study participation. [Text field]

Thank you for completing the study. We greatly appreciate your time and effort. Your answers have been recorded anonymously. Now that you are done with the study, please click the following link to receive approval of your completion on the Prolific platform: [Link]