"My Best Friend's Husband Sees and Knows Everything": A Cross-Contextual and Cross-Country Approach to Understanding Smart Home Privacy

Tess Despres
University of California, Berkeley

Marcelino Ayala Constantino
El Colegio de la Frontera Norte

Naomi Zacarias Lizola
Universidad de Tijuana CUT

Gerardo Sánchez Romero
Mutua Social Research & Innovation

Shijing He
King's College London

Xiao Zhan
King's College London

Noura Abdi
Liverpool Hope University

Ruba Abu-Salma
King's College London

Jose Such
King's College London & Universitat Politecnica de Valencia

Julia Bernd
International Computer Science Inst.

Abstract

As smart home devices proliferate, protecting the privacy of those who encounter the devices is of the utmost importance both *within their own home* and *in other people's homes*. In this study, we conducted a large-scale survey (N=1459) with primary users of and bystanders to smart home devices. While previous work has studied people's privacy experiences and preferences either as smart home primary users or as bystanders, there is a need for a deeper understanding of privacy experiences and preferences *in different contexts and across different countries*. Instead of classifying people as either primary users or bystanders, we surveyed the same participants across different contexts. We deployed our survey in four countries (Germany, Mexico, the United Kingdom, and the United States) and in two languages (English and Spanish). We found that participants were generally more concerned about devices in their own homes, but perceived video cameras—especially unknown ones—and usability as more concerning in other people's homes. Compared to male participants, female and non-binary participants had less control over configuration of devices and privacy settings—regardless of whether they were the most frequent user. Comparing countries, participants in Mexico were more likely to be comfortable with devices, but also more likely to take privacy precautions around them. We also make cross-contextual recommendations for device designers and policymakers, such as nudges to facilitate social interactions.

Keywords

Privacy, Primary users, Bystanders, Multi-user smart homes

Proceedings on Privacy Enhancing Technologies 2024(4), 413–449

https://doi.org/10.56553/popets-2024-0124

1 Introduction

As of 2023, 60.4M, 5.3M households in the USA and the UK own a smart home device, respectively [98, 103]. In Germany and Mexico, this number is expected to encompass 39.6M and 9.3M users by 2028 [123, 124]. While these devices can be extremely helpful, they come with challenges. Sensor and usage data is collected by various stakeholders, from the smart home device providers to third parties [41]. Differing goals among people who come into contact with devices can lead to conflicts, e.g. about device location, which can in turn lead to security and privacy risks [2, 11, 49, 56, 129, 149, 151].

Different types of stakeholders have varying degrees of agency in those interactions, from primary users (i.e., those who make the decision to purchase and deploy a smart home device) to secondary users, incidental users, and bystanders (i.e., those who did not make the decision to purchase and deploy the device, but whose privacy is affected by it, like guests and domestic workers).

Bystanders and incidental users can be uniquely vulnerable to surveillance because devices are usually not in their control. Privacy expectations, and ideas about what constitutes a privacy violation, are highly social, depend on context-specific norms, and change over time [102]. While separate stakeholders in smart homes have different privacy concerns and preferences, there is a need to understand how the *same* person has differential privacy experiences, preferences, and concerns based on shifting contextual roles, as differences across demographic and geographic factors.

In a survey with 1459 participants, we study two contexts: participants' own smart homes (as primary or secondary users) and other people's smart homes (as incidental users or bystanders), considering how people's roles in those contexts affect their agency and control over devices and over data collection.

We also study four countries, Germany, Mexico, the United Kingdom, and the United States.[1] We hypothesize that country-specific cultural, governmental, and economic factors might impact smart home experiences and perspectives, especially about privacy. This

[1] We chose these countries for high rates of Spanish or English fluency, large participant pools on Prolific, and because research team members or close collaborators could screen instruments for comprehensibility and cultural appropriateness.

study does not aim to decompose such cultural, governmental, and economic factors, particularly as cultural lines are ambiguous and difficult to draw in a large-scale survey. However, we hope that supplying robust findings about geographical differences will provide a foundation for future work to break down these nuances (see §5.3). In addition, to capture a broader participant pool, we conducted our survey in both Spanish and English.[2]

Research Questions. In this study, we extend the current bystander privacy research to include a cross-contextual and cross-country understanding of how people interact with smart home devices. We aim to answer three main research questions.

(1) What are people's adoption patterns, usage patterns, and configuration processes for different smart home devices?
(2) What are people's concerns about and privacy perspectives on smart devices in their own and others' homes?
(3) How do people protect their privacy around smart home devices, and what privacy protections do they wish existed?

For each RQ, we consider the effects of context (one's own home vs. other people's homes), geography (country), and demographic and socioeconomic factors.

Summary of Contributions.

- We conducted a large-scale survey in four countries to explore people's experiences, needs, and concerns across two contexts: their own home and other people's homes. This is the first study that combines cross-country with cross-context analysis for smart home adoption and privacy.
- We present qualitative and quantitative evidence about people's relationships with and control of smart home devices; their attitudes, concerns, and privacy perceptions about them; and actual and desired protections —including variation across contexts, countries, and demographic factors.
- Our quantitative findings are supported by robust statistical analysis of a dataset balanced for demographic and socioeconomic factors across four countries.
- Technical solutions are not enough to improve smart home privacy. We therefore suggest a set of recommendations for both sociotechnical design and policy.

2 Related Work

Privacy within smart homes has been studied extensively [e.g. 1, 2, 12, 37, 51, 79, 99, 153]; [overviews in 6, 81, 106]. Much of this work focuses on primary users, but recent work explores privacy of secondary and incidental users as well.

Multi-User Smart Homes. There has been a wealth of work studying how stakeholders in a multi-user smart home navigate control of devices, concerns, and privacy experiences and preferences [e.g. 9, 23, 59, 69, 78, 89, 92, 135, 150, 151]; [overview in 97]. Selection, installation, device malfunction, and use are areas for both tension and cooperation [49]. Huang et al. [56] found conflicts arose from inability to control access to the device. Devices can enable surveillance of cohabitants—but can also provide opportunities for connection [11]. Studies with couples revealed that there is often a pilot user, who sets up and adds functionality to the device, and passenger user, who can access the device but did not configure it [65]. In a UK survey on family households, Kraemer et al. [68] found that social relationships played a large part in who had access to devices. In particular, they found that women may be viewed as less capable and willing to configure and administer smart home devices—though that opinion was held by more men than women. Strengers et al. found that women did have lower interest and adoption rates than men [125]. Other recent work has highlighted gender imbalances in purchasing, installation, and maintenance [49] [overview in 100], and discussed the impact of cultural associations between masculinity and smart home technologies [27, 35, 110]. This body of work inspires our focus on gender and other demographic factors, but we look at a larger, broader sample.

Contextual Integrity in Smart Homes. The theory of Privacy as Contextual Integrity (CI) [16, 101, 102, 105] frames privacy in terms of the appropriateness of information flows based on socio-cultural norms in a given context. CI has been used for quantitative elicitation of privacy norms (decomposed into situational parameters) [e.g. 91, 119], including about smart homes [2, 13, 14, 24, 53]. Though we do not employ CI-based parametric analysis, the theory provides background and inspiration for our cross-contextual approach.

Bystanders in Smart Homes. Recent studies have examined privacy experiences, concerns, and preferences of incidental users of and bystanders to smart home devices [e.g. 5, 9, 18, 28, 38, 86, 96, 109, 122, 140, 142, 143, 147, 149, 152]. For example, Alshehri et al. [9] found many bystanders did not expect owners to understand their devices' data practices. Marky et al. [87–90] examined visitor comfort, privacy perceptions, and coping strategies from both a guest and host perspective. A study of multiple situations and roles showed how conflicts can arise between incidental users and device owners [30]. Technical interventions have been suggested [e.g. 5, 149]; however, privacy awareness mechanisms for users and bystanders have different pros and cons for different stakeholders [130]. Domestic workers' agency over data collection is complicated by power imbalances and social norms [7, 8, 18, 60, 62]. Prior research tended to classify participants as either bystanders or primary users for the purposes of a study; the few exceptions [30, 130, 145] were US-specific. However, as Wong et al. [145] point out, the same person is likely to fill both roles at different times. We aim to capture more nuance by asking a single participant about their own home and others' homes, and compare across countries.

Disparities in Privacy Impacts. Privacy norms and harms due to privacy violations can vary across socioeconomic groups, and impact people from marginalized or underserved groups disproportionately [21, 45, 83, 84, 104, 115, 154]. Socioeconomic status can impact how people relate to smart home devices [15, 66, 108, 141]. Smart home devices can be used as a tool to reinforce existing power dynamics, and even enable abuse [20, 47, 60, 76, 77, 120]. Specific groups are at an increased risk of unique harms, such as undocumented immigrants [50], female and LGBTQ individuals [20, 29, 60, 76], oversurveiled ethnic minorities [61], and children

[2] As the survey included many free-answer questions and the research team did not include German speakers, we did not translate it into German. While this is a clear limitation, there is a large pool of English speakers in Germany on Prolific. We included Germany in the study despite this limitation because we wanted to explore how known differences in privacy attitudes interact with adoption and behavior.

[14, 94]. Our analysis takes demographics and socioeconomic factors into account as independent variables.

Privacy Across Countries and Cultures. Studies have frequently found differences in privacy perceptions between people in different countries [e.g. 43, 54, 72, 113, 133, 139]. These perceptions are often related to different expectations about privacy regulation [e.g. 33, 39, 116, 137]. Li [80] provided an overview and discussed the relationship between cross-country studies and a concept of national culture—as well as calling for more cross-cultural and cross-country studies in the emerging area of IoT privacy. To our knowledge, only three relatively small surveys have been conducted in this vein. In a survey of 232 adopters and non-adopters across different regions (in the US, Europe, and India), Lafontaine et al. showed different comfort levels with IoT devices, driven in part by different expectations about regulatory protection [74]. The study also found differences in comfort across contexts, such as public spaces, work, or home, but did not consider others' homes. Relatedly, a survey of 431 participants by Bombik et al. [19] found that perceptions regarding regulatory protections in the US, UK, and EU countries impact adoption of smart home devices. Interestingly, despite these differences in perspective, a 212-participant survey by Shlega, Maqsood, and Chiasson [118] across Europe and North America did not find significant geographical differences in actual smart home adoption (though this may have been an effect of sample size). Our survey expands on this work, with a much larger sample than previous surveys and a comparison across contexts.

3 Methodology

We designed a large-scale survey (N=1459) with free-response and multiple-choice questions.

3.1 Study Design.

Structure of the Survey. In the first section, we asked participants to select the types of smart home devices in their homes, then answer a series of general questions about conflicts and concerns due to those devices. We then repeated the device inventory and the conflicts and concerns questions for devices in other people's homes. (We did not randomize the order of contexts, choosing instead to have a consistent conceptual progression from own home to not-own-home within survey sections.) If participants did not have devices in their own home, or encounter devices in others' homes, we still asked general questions about concerns (including why they did not have devices) and conflicts, but did not ask device-specific privacy questions. N's therefore vary by question.

In the second section, we asked privacy-related questions, both generally and about specific devices. We chose this ordering to avoid priming participants to list privacy as a concern. We asked about the impact of smart home devices on privacy in both their homes and others' homes. We then showed participants the lists of devices they had encountered, and asked them to identify up to three that had the largest impact on their privacy for each context. Of the devices selected, we randomly picked one to ask follow-up questions about. In our Findings, we will refer to this as the ***Selected Device***. For the Selected Device, we asked about account structure and control, privacy settings, intended use, and privacy protection strategies. We chose this approach, rather than asking about all devices encountered, to reduce survey fatigue. We then asked a set of questions about comfort with IoT devices generally, as a comparison point, and also asked about technical background, current housing situation, and reasons for visiting other people's homes, as well as demographics.[3]

	Total	Germany	Mexico	UK	USA
Total	1459	347	383	358	371
English	990	320	22	333	315
Spanish	469	27	361	25	56

Table 1: Number of participants by country and language

Development Process. Since this survey was distributed in four countries (Germany, Mexico, the UK, and the US), in Spanish and English, we took steps to make sure all versions were understandable and consistently interpretable by speakers of the relevant national dialects, without overly culture-specific references. An initial draft was prepared collaboratively by UK and US researchers on the team, with close discussions of whether the intended meaning of each question would be understood similarly by speakers of both European and North American varieties of English. A research team member in Mexico translated the survey into Spanish; we then reviewed and reworded questions in both language versions to maximize comparability. The translation was reviewed by a speaker of Castilian (European) Spanish on the team, and further adjusted. Finally, the instrument was reviewed by a researcher working in Germany, to confirm English speakers in Germany would likely interpret questions as intended.

During initial design, we asked experts in smart home privacy to review our instrument and give feedback, e.g. on how we might be priming privacy based responses. Once designed, we tested the survey iteratively using three recorded UserFeel [136] user-testing walkthroughs per language (six total), and edited questions that were unclear to testers. We then ran a pilot with 10 participants across each of the 8 groups (matrix of countries and languages) for a total of 80, and further updated the survey.

Ethics. We submitted our research protocol to our respective institutions' human subjects protection programs, and it was deemed exempt from full IRB review. In the survey, we reminded participants to avoid sharing personal information such as names. Our consent forms complied with the European and UK GDPRs [48, 57] and Mexico's LGDPPSO [25], as well as the Belmont Report [131].

3.2 Recruitment and Participants

Our survey was hosted on Qualtrics [114], and we recruited participants through Prolific [112] who were fluent in either Spanish or English. To maximize data quality, we screened out participants who had Prolific approval rates less than 98%, and discarded data from participants who failed more than one 1 of 4 attention checks. To avoid selection bias, we did not mention privacy and security in the recruitment blurb. We did not require experience with smart home devices. We paid $4.25, and the median time was 17.39 minutes, which equates to above minimum wage in all four countries.

[3]The full survey instrument, including versions for all countries and languages, can be found at https://bit.ly/3Vlfn82

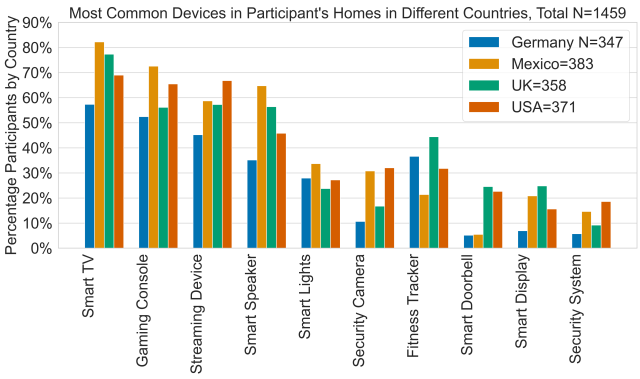

Figure 1: Breakdown by country of devices participants currently have in their homes, out of the overall top ten.

After collecting initial batches of data, we compared the demographics of the sample so far to the demographics of each country, and posted additional Prolific tasks targeted to populations heavily underrepresented in the initial sample.

A breakdown of participants by country and language version is shown in Table 1. A full summary of participant characteristics is included in Appx. D.

3.3 Data Analysis.

Qualitative. We followed inductive thematic analysis [22] to analyze free-response questions. A six-person codebook-development team including both native English and native Spanish speakers reviewed the first 50 English responses to develop a codebook. The team then met to discuss and came to a consensus on a codebook for each set of questions. (Where we asked about the same topic in separate questions about one's own home and others' homes, we largely used the same codebook for both.) An initial coding team then coded the rest of the responses, splitting coders between Spanish and English and between different sets of questions, meeting in groups of two to three to compare codes and suggest changes and clarifications to the codebook. We also checked our results code-by-code across languages, and addressed differences between the Spanish and English coding team's interpretations.[4]

A final coding team of seven researchers divided up the question sets, with four coders per set, and conducted additional tests of the codebook, then coded all of the responses. In this round, the four Spanish-competent coders were assigned both English and Spanish responses, to avoid any further discrepancies. Each response was coded by two coders, who then met to resolve any disagreements. Throughout the codebook development and testing process, we checked Kupper-Hafner interrater agreement [73]. Though we did not ever achieve consistently high agreement within all pairs of *individuals*, when we conducted a test where two pairs of coders coded the same set of responses, we achieved agreement levels *between pairs* ranging between 0.7520 and 0.9892, indicating that the pair-resolution process produced a reasonably consistent result.

[4]The final codebook and coding rubric can be found at https://bit.ly/3Vlfn82. A simple list of codes can be found in Appx. E.

Quantitative. To analyze multiple choice questions, we used descriptive statistics to understand our data quantitatively, along with chi-squared tests [93] and Kruskal-Wallis [71] to check significance levels, and Cohen's f statistic [32] and Cramér's V [34] to check effect sizes, along with binary regression [64]. To account for multiple comparisons, we use a conservative α of $p = 0.002$ as the criterion for significance (based on a maximum of 25 hypotheses tested per outcome). We also used descriptive statistics to understand the free-answer data based on our qualitative coding. However, because the codes are necessarily subjective, we mostly did not attempt further statistical analysis for free-answer questions. Prior to quantifying coded responses, we dropped all unclear or off-topic responses; in addition, some participants declined to respond. The N for any given quantitative finding about free-answer questions includes only the remaining usable responses, so different N's are reported for different qualitative questions.

4 Findings

In Sections 4.1, 4.2, and 4.3, we present findings for each of our three research questions, respectively. Except where noted, findings are based on multiple-choice questions. In §4.4, we describe common themes across the RQs, based on our thematic analysis.

4.1 RQ1: Exposure, Adoption, & Configuration

We aim to understand device exposure, adoption patterns, usage patterns, and configuration processes across different types of devices, across contexts (participants' homes vs. other people's homes), and across countries, as well as large demographic trends.

4.1.1 Device Exposure. Asked about device types, 96% of participants had devices in their own homes and 97% had encountered them in others' homes.

Fig. 10 in Appx. A shows the top ten devices selected by participants across the two contexts combined. The most common devices in both contexts were smart TVs and gaming consoles, followed by streaming devices in participants' own homes and smart speakers in others' homes; other device types were noticeably less common in both contexts. Unsurprisingly, participants encountered a larger variety of device types across others' homes, an average of 7.4, versus 4.9 in their own home.

Additional Variation in Device Exposure. Overall, participants in Germany had the fewest device types in their own homes, average 3.9, while the other countries averaged just over 5 device types per participant. This difference is statistically significant (H stat = 67.9, $p < 0.000001$), but the effect is minimal (Cohen's *f-value* = 0.05). (See Table 3 in Appx. A for details per country.) Fig. 1 breaks down the devices participants had in their homes across countries, out of the top ten encountered in total. Average device types encountered in others' homes ranged from 6.7 in the UK to 7.9 for Mexico, but again, the effect is minimal ($H = 21.4$, $p = 0.00009$, $f = 0.02$).

Average device types in participants' homes increased with household income, from 3.6 for the lowest quintile to 5.9 for the highest (though minimal effect: $H = 99.2$, $p < 0.000001$, $f = 0.07$; $N = 1326$). Income had no significant influence at all on number of device types encountered in others' homes—so exposure was more equal where the benefit was less. Age and gender differences

	I did for my account	I did, for everybody	Me and others for everybody	Others in the house for everybody	Default settings	Total
Female	17%	31%	9%	29%	14%	625
Male	23%	51%	4%	11%	12%	655
Non-binary	17%	31%	10%	30%	10%	29

Table 2: Control over privacy settings for the Selected Device, by gender. ('Other' and 'I don't know' responses not included.)

in either context were not statistically meaningful.[5] Locality type also did not have a significant effect, suggesting that inter-country differences are not driven by skews in (sub)urban vs. rural.

4.1.2 Device Adoption. For many questions, participants responded based on their experiences with a single device, the Selected Device assigned by the process described in §3.1. Unless otherwise noted, for all multiple-choice questions about the Selected Device, N=1404 for participant's own home and N=1417 for others' homes.

For adoption, we asked *"Who decided to get the <insert Selected Device> in your home?"* and *"Who purchased the <insert Selected Device> in your home?"* to understand how collaborative decisions about—and implementation of—device adoption are. We also asked who in the home *owns* the Selected Device. Patterns were similar, with "Me" as the majority response to all three questions.

Additional Variation in Adoption. Males were more actively involved in processes of adoption in their own homes. Either on their own or with someone else in the home, males were somewhat more likely to have decided to get the device ($\chi^2 = 48.4$, $p < 0.000001$, Cramér's $V = 0.19$; $N = 1353$) and to have purchased the device ($\chi^2 = 60.9$, $p < 0.000001$, $V = 0.21$; $N = 1342$), compared to females.

Looking at each country individually, the effects of gender were similar (a small effect for each question) for decisions and implementation of purchase in Germany, Mexico, and the US; however, the effect was not statistically significant for the UK. Gender had a smaller effect on whether participants viewed themselves as owning the device than on active adoption processes ($\chi^2 = 15.3$, $p < 0.0001$, $V = 0.11$; $N = 1353$), and only met the threshold for significance when all countries were considered together.

Age also had an effect, with participants 25–45y.o. most likely to be involved with adoption (decided to get: $\chi^2 = 34.3$, $p < 0.000001$, $V = 0.16$, $N = 1385$; purchased: $\chi^2 = 105.1$, $p < 0.000001$, $V = 0.28$, $N = 1372$; owns device:$\chi^2 = 53.6$, $p < 0.000001$, $V = 0.20$, $N = 1383$).[6] Fuller data on variation by age and gender may be found in Table 4 in Appx. A, along with by-country breakdowns for effect of gender in Tables 5-7.

4.1.3 Device Usage. We asked participants device-specific usage questions for their own home; the five most common Selected Devices were used intensively, most commonly 'Multiple Times a Day'. Use of any device was less frequent in others' homes (than the Selected Device in own home), but still somewhat common; 17% *used* devices in others' homes at least weekly, and 51% at least monthly. Encountering devices without using them—i.e. exposure without benefit—was much more common; 38% of participants *encountered* at least one smart device (without using it) at least weekly, and 83% at least monthly. (Encounter/use questions for others' homes were general, not device-specific.)

Additional Variation in Usage. Usage frequency for the Selected Device in own home did not vary meaningfully across gender, country, income, or age. Usage frequency for devices in others' homes did not vary meaningfully across gender, income, or age, but did vary somewhat across country. Parallel to their being exposed to the most types of devices in others' homes (§4.1.1), participants in Mexico were most likely to use a device at least weekly in someone else's home ($\chi^2 = 29.3$, $p < 0.00001$, $V = 0.14$ for country).

Encountering devices in others' homes without using them did not vary significantly. See Figs. 11–13 in Appx. A for cross-country details for both contexts.

We also asked who was the most frequent user of the Selected Device in participants' homes; it did not vary meaningfully by age or gender. This is notable because it means that gendered differences in control of device configuration (§4.1.4) and configuration of privacy settings (§4.1.5) cannot be explained by usage differences.

4.1.4 Control of Device Configuration and Profiles. To understand how much control participants had over their devices, we asked *Who configured the <insert Selected Device> in your home?* Overall, 62% said they had configured the Selected Device in their home, while 22% said someone else in the house configured it. Only 11% had configured the device together with someone else in the house.

We also asked *Have you ever configured an IoT device in someone else's home?* 30% of participants had done so, most commonly Smart TVs, Streaming Devices, and Smart Speakers, and most often because the owner needed help.

If participants used the Selected Device, we asked whether they had their own account or profile. In their own homes, 57% had their own accounts/profiles, 33% shared an account/profile, 9% had no account/profile, and 1% said the device didn't offer that option (N=1271). On Selected Devices in others' homes, 9% had their own account/profile , 16% shared one, 72% had none, and 2% said there was no option (N=548). ($\chi^2 = 798.9$, $p < 0.00001$, $V = 0.66$ for effect of context—own-home vs. others'-home.) A large majority, 87%, of those who had individual accounts were admins in their own homes, but 37% had admin accounts in others' homes as well.

Additional Variation in Control of Configuration. Males were somewhat more likely to be involved ("I did it" or "Me and others in the house did it together") with configuration of the device, as shown in Table 8 in Appx. A, compared with females ($\chi^2 = 74.7$, $p < 0.00001$, $V = 0.24$; $N = 1354$). The correlation held across each country with similar small effects; see Tab. 9 in Appx. A.

[5] We use $p < 0.002$ and at least a small effect size (e.g. Cramér's $V > 0.1$ for one degree of freedom) as our threshold for statistically meaningful.

[6] We do not report effects of household income and country on dependent variables comparing participants to others within their household.

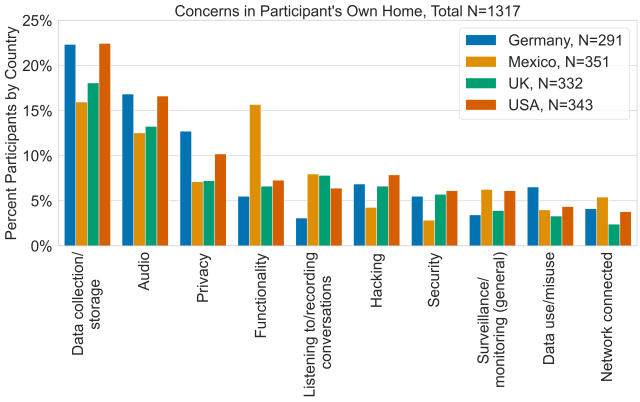

Figure 2: Most common concerns for own home.

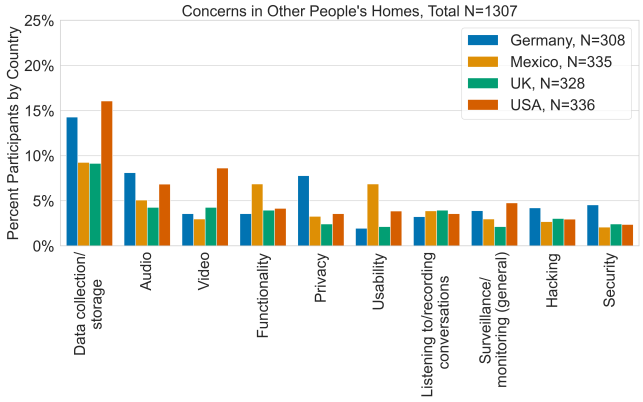

Figure 3: Most common concerns for others' homes.

As we noted above, gender variation in frequency of use, or being the most frequent user, was not significant, indicating that gender imbalance in control of devices is independent of use. Indeed, among male participants who were the most frequent user of their Selected Device (either alone or equal with someone else) 95% were involved in configuring it, as opposed to 78% of female and 88% of non-binary most-frequent users ($N = 1013$).

A gender breakdown of account access by gender is in Tab. 10 in Appx. A. We did not see a statistically meaningful age trend for control of configuration.

4.1.5 Control of Privacy Configuration Beyond general device configuration, we also asked, (*Who configured the* privacy settings *on the <insert Selected Device> in your home?*) 19% of participants had configured privacy settings for their account only, 38% had configured privacy settings for everyone in the home, and 19% said someone else in the home configured them. Only 12% had left the default settings.

We also asked whether participants knew what the privacy settings were for Selected Devices in both contexts. 63% knew some or all of the privacy settings in their own home, while only 10% knew some or all for the device in someone else's home ($\chi^2 = 854.4$, $p < 0.0001$, $V = 0.55$ effect of context).

Additional Variation in Control of Privacy. Results for configuration of devices in own home across genders are shown in Table 2. Males were somewhat more likely to be involved with privacy configuration ("I did, for everybody", "I did, for my account only" or "Me and others in the house did it together"), compared with females ($\chi^2 = 70.2$, $p < 0.00001$, $V = 0.25$; $N = 1280$). This correlation was similar across countries, but stronger for the UK (medium effect rather than small); see Table 12 in Appx. A for details.

Again, gender imbalance is not simply an effect of use. Even among participants who were the most frequent user of their Selected Device (either alone or equal with someone else), males were more likely to be involved in privacy configuration (96%) than female (78%) or non-binary (77%) participants ($N = 987$). Binary logistic regression reveals that being the (sole or equal) most frequent user has the stronger effect on privacy control ($B = 1.63$, $p < 0.000001$), but gender has a significant independent effect ($B = 0.90$, $p < 0.000001$), with no significant interaction between the variables ($p = 0.57240$ for the interaction term) ($N = 1411$.

Participants 25–40y.o. were most likely to be involved in configuring privacy settings in their homes ($\chi^2 = 15.9$, $p = 0.00121$, $V = 0.12$ effect of age; $N = 1309$); see Tab. 11 in Appx. A.

4.2 RQ2: Concerns, Conflicts, and Privacy Perspectives

We examine how concerns, conflict, comfort with devices, and privacy impacts differ across contexts and countries.

4.2.1 Concerns. We asked free-answer questions about what concerns participants had with smart home devices in their own and others' homes. To avoid biasing participants, we did not mention privacy or security prior to asking about concerns.

In their own homes, 51% of participants mentioned concerns, while 47% said they had no concerns (N=1317 usable responses). [7] In others' homes, 33% of participants mentioned concerns, while 66% had none (N=1307) ($\chi^2 = 92.0$, $p < 0.000001$, $V = 0.19$ effect of context, for classifiable answers).

Likelihood of concern was moderately correlated across contexts; participants having at least one concern in their own home predicts having a concern in others' homes, with a medium effect size (χ^2=207.3, $p < 0.00001$, $V = 0.42$; $N = 1188$).

Fig. 2 shows the common concerns people had about smart devices in their own homes, and Fig. 3 in other homes. (Percentages are out of usable answers, including no-concerns.)

In both their own and others' homes, participants were the most concerned with data collection and storage, especially being recorded by audio devices—and in particular, devices listening to their conversations. For example, one participant said: "I've had concerns about Alexa because Alexa picks up audio data and I worry she may be listening to conversations in my household." (UsEn674)[8] Beyond this, participants had different concerns depending on the

[7] Percentages do not add up to 100% because some responses were generally usable (i.e. clear and on-topic) but difficult to classify as concerns vs. no concerns, for example those containing hypotheticals.

[8] The first and second letters of the participant ID indicate country (Gr, Mx, Uk, Us), and the third and fourth indicate language version (En, Sp); numbers were randomly assigned. Clear typos have been corrected, but quotes are otherwise verbatim. Translations are ours.

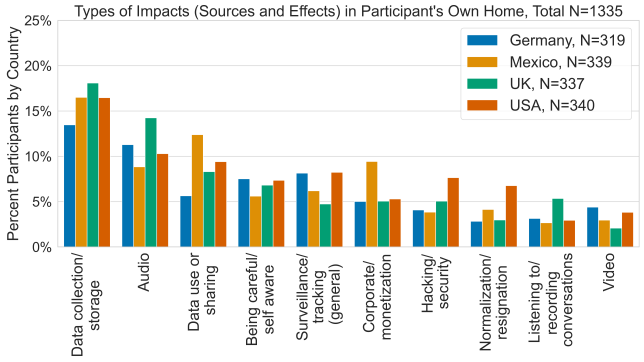

Figure 4: Most common types of impacts for own home.

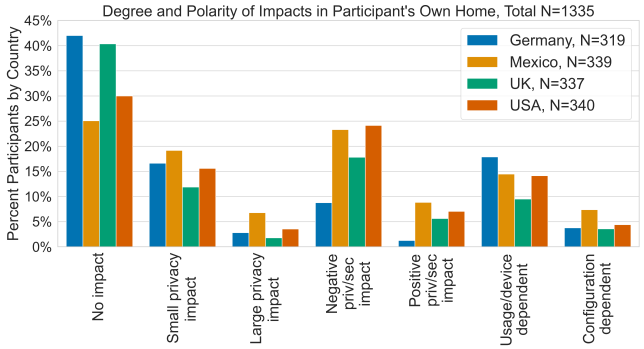

Figure 5: Participants' perceptions of degree and polarity of impacts across countries for their own home.

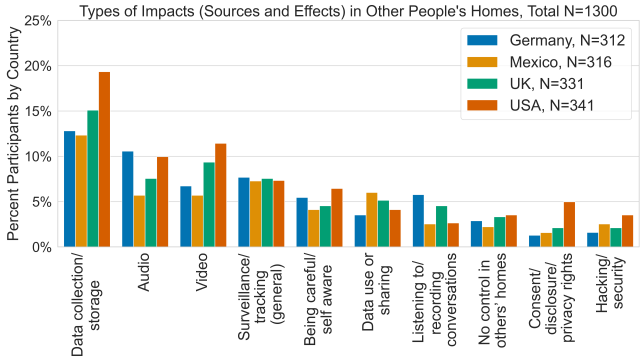

Figure 6: Most common types of impacts for others' homes.

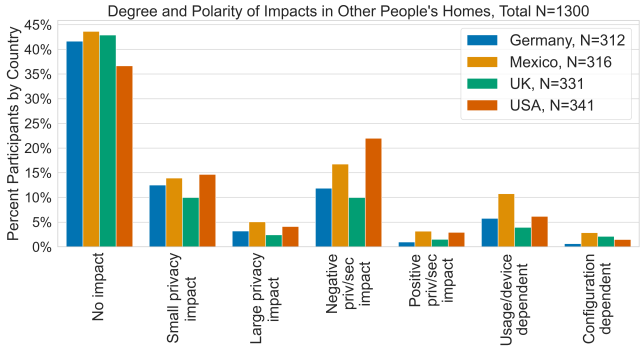

Figure 7: Participants' perceptions of degree and polarity of impacts across countries for other people's homes.

context that they were in. Video showed up as the third most common concern in others' homes but was not a common concern in participant's own home. Despite the much greater exposure, some participants mentioned that they were less worried about their own cameras because they were outdoors, or because they knew who had access to the data. Participants were particularly concerned about *unknown* video recording at other homes: "Only concern is privacy, as I could be worried that they have spy / nanny cams that I don't know about that are watching me." (UkEn1130)

Usability was also a more highly-ranked concern in others' homes, for example when participants were confused or frustrated by a device they encountered. Some were also concerned about other people having difficulty with a device: «solo preocupación de que una persona mayor no supiera manejar bien algún dispositivo» (MxSp11) *("Only a concern about an older person not knowing how to operate the device right")*. Within participants' own homes, there was more concern about data misuse and network connections.

For the 4% of participants who did not have any smart devices at home, we asked why not. Answers tended to focus on not needing them (especially given the cost), privacy/security, or both: "I don't feel like it's necessary and I don't want my home gadgets spying on me" (UkEn906).[9]

[9]Due to the low N, we did not code and quantify responses to this question.

Additional Variation in Concerns. Whether a participant had at least one concern vs. no concerns varied somewhat across countries, both in their own home ($\chi^2 = 18.7$, $p = 0.00032$, $V = 0.12$) and in others' homes ($\chi^2 = 18.6$, $p = 0.00033$, $V = 0.12$). Participants in Mexico were the most likely to have concerns in both contexts, and those in the UK were least likely in both contexts; details in Table 13 in Appx. B. Breaking down types of concerns, participants in Germany were the most likely to mention concerns with privacy. Participants in Mexico were the most likely to mention functionality—possibly because they were most likely to use others' devices. US participants most frequently mentioned concerns with data collection and, in others' homes, video recording.

On the whole, participants in Germany and the US were more concerned about data collection, audio recording, and privacy compared with the UK and Mexico. Interestingly, some participants in Germany and the UK said they were not concerned about cameras due to GDPR protections; see §4.4.5.

4.2.2 Comfort. We asked all participants a set of general Likert-scale questions about their comfort levels with IoT devices. Though the majority of participants were at least somewhat comfortable with IoT devices (81% generally, 80% in their own homes, and 73% in others' homes), only a minority were at least somewhat comfortable with devices sending data out of the home (31%).

If participants were comfortable with devices in their own home, they were likely to also be comfortable with devices in others'

homes, with medium effect size ($\chi^2 = 324.6$, $p < 0.00001$, $V = 0.47$ for correlation, binarized to comfortable/not comfortable). Participants who had concerns about smart devices in a given context (their own home or others') (see §4.2.1) were more likely to be uncomfortable with devices in that context ($\chi^2 = 22.4$, $p < 0.00001$, $V = 0.13$, $N = 1317$ for correlation with concerns in own home, and $\chi^2 = 81.3$, $p < 0.00001$, $V = 0.25$, $N = 1307$ for others' homes).

A binary regression found that the number of device types in one's own home correlates with being comfortable with IoT devices in one's own home ($B = 0.33$ and $P < 0.0001$, with the likelihood of being comfortable rather than uncomfortable rising by 39% for each type of device). On the other hand, there was no significant correlation between number of types of devices encountered in others' homes and comfort with IoT devices in others' homes. However, we found a significant relationship between types of devices in *one's own home* and comfort with devices *in others' homes* ($B = 0.15$, $p < 0.0001$), suggesting that familiarity and habituation can outrank discomfort with not having control.

Additional Variation in Comfort. Also using binary logistic regression, we investigated the impact of country, age, gender, and income level on aggregate comfort levels (where comfort level is averaged across the four questions to create a single composite dependent variable, then binarized). The results identified country as a significant independent variable.[10] More specifically, using Germany as the reference, the results show that the UK ($B = 0.37, p < 0.001$) and Mexico ($B = 0.47, p < 0.001$) influence comfort levels, with Mexico being the most important variable. Participants in Mexico were the most likely to be comfortable interacting with devices, despite being most likely to have concerns about them (see §4.2.1).

Age, gender, and income did not have a significant influence on the aggregate comfort level.

A by-country breakdown in comfort levels for each question can be found in Fig. 14, Appx. B. Looking at individual questions, general IoT comfort ($\chi^2 = 25.4$, $p < 0.0001$, $V = 0.13$) and comfort with devices in their own homes ($\chi^2 = 42.2$, $p < 0.00001$, $V = 0.17$) were the most strongly affected by country. Gender did not have a statistically significant influence on any comfort measure, across countries nor in any individual country; see Figs. 15–18 in Appx. B.

4.2.3 Conflicts. We asked if participants had previously had conflicts about smart devices. In their own homes, 19% of 1459 participants had had conflicts, while only 5% of 1417 participants who had encountered devices in others' homes had had conflicts about them ($\chi^2 = 119.8, p < 0.00001$, $V = 0.20$ effect of context).

Additional Variation in Conflicts. We did not see a significant difference in conflicts across age, income, or gender. We did see a statistically meaningful difference in conflicts in participants' own homes (only) across countries ($\chi^2 = 30.8$, $p < 0.00001$, $V = 0.15$), with participants in Mexico reporting the most conflicts, though this may be an effect of sampling bias. (A smaller percentage of participants in Mexico lived alone, and a higher percentage were younger and/or lived with parents; see Tables 23 and 26, Appx. D.) We asked participants who had conflicts to describe them. Many involved control over devices; others involved privacy: "My father, over his security devices. I felt like he was spying on me. He did shut them off while we were at home, but it was unsatisfactory because I couldn't tell a difference and they were controlled by his device." (UsEn614)[9] In their own home, out of 274 participants with conflicts, 63% were mostly or totally satisfied with the resolution—leaving a potentially worrying third of conflicts that were not resolved in a way that satisfied everyone. In others' homes, where participants had less control, fewer—52% out of 76—were satisfied.

4.2.4 Privacy Impacts. After asking about concerns (i.e. not privacy-specific) we asked free-answer questions specifically about privacy perceptions: "What is the impact of IoT devices {in your home/in other people's homes} on your privacy?" This phrasing was intentionally broad, to capture attitudes, concerns, and behaviors; it therefore allowed for responses about *how much* impact or about *types* of impacts, and was open to counterfactual reasoning.

Types of impacts in participants' own homes are shown in Fig. 4 (combining *sources* of impact and *effects* of impact; see breakdown in Appx. E), and degree and polarity of impacts are shown in Fig. 5. Types of impacts in others' homes are shown in Fig. 6, and degree and polarity are shown in Fig. 7. (Where degree and polarity were generally coded based on participants' explicit wordings; e.g., a response of "Not much" would be coded as *Small privacy impact.*)

Some privacy impacts that participants mentioned were consistent across their home and others' homes. For example, as with our open questions about concerns, data collection/storage and audio were listed often in both contexts. Other impacts were viewed differently. For example, video recording was more frequently mentioned with regard to others' homes—a similar pattern to stated concerns about video (see §4.2.1).

Again echoing concerns, participants noted that devices in others' homes can have a large privacy impact because they lack insight into the space: "You never know what to expect and nobody goes into someone else's home and asks for a tour of the IoT devices and their privacy policy first" (GrEn1163). (Discussion in §4.4.2.)

Additional Variation in Privacy Impacts. There are some differences between countries in likeliness of perceiving impact, with participants in Germany and the UK being somewhat less likely to see impacts in their own homes; details are in Table 14 in Appx. B.

However, cross-country variation in *types* of privacy impacts was not as striking as variation in more general types of concerns, though some minor patterns are discernable. Participants in Mexico, in their own homes, were more likely to note impacts from data use and sharing, e.g. for marketing, along with corporate control over data, compared with participants in other countries. Participants in the U.S. were more likely than other countries to note various types of impacts in others' homes, especially data collection/storage, audio recording, and video recording.

4.2.5 Devices With Highest Privacy Impact. As we noted in §3.1, for the latter part of the survey, participants chose up to three devices amongst those they had encountered in each context that they believed had the largest impact on their privacy (from which the survey selected a random one to ask more questions about). As we noted in §4.1.3, participants tended to choose heavily used device types; use may contribute to perception of high privacy impact.

[10] Country was independent from the other factors, suggesting that findings about comfort are not biased by differences in age, gender, and income distribution between participants in the countries in our sample.

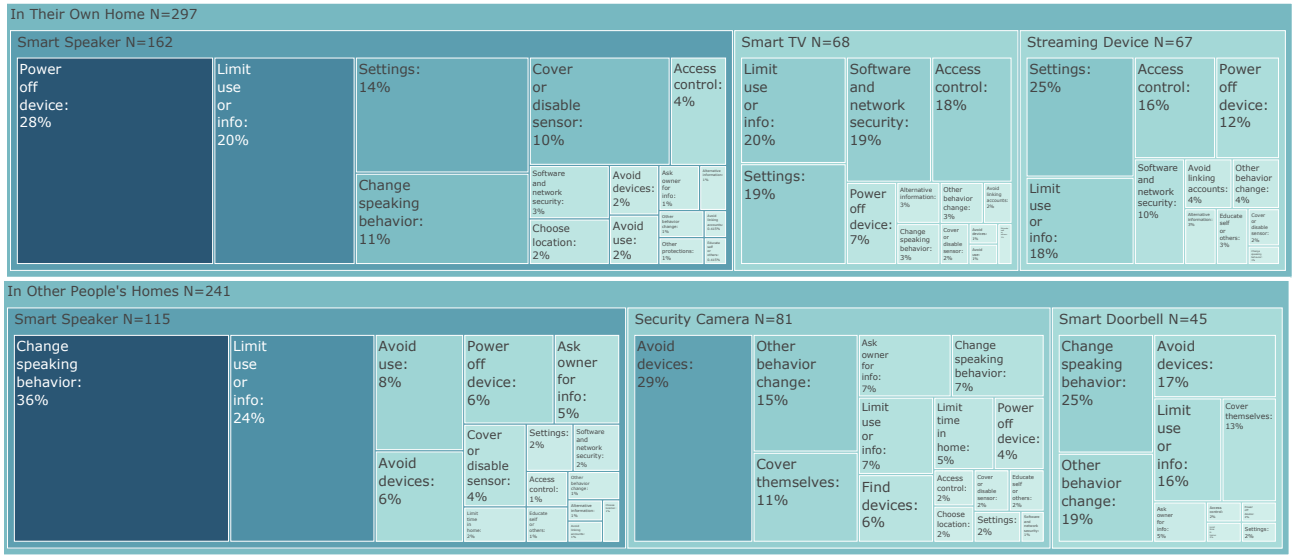

Figure 8: Actual privacy protection behaviors and mechanisms for participants' homes and others' homes, for the most commonly presented Selected Devices (see §3.1). (Overall N is only for those three devices, only participants who suggested options.)

Figs. 19 and 20 in Appx. B combine the twelve most commonly chosen devices in either environment. Though the percentages are not directly comparable (due to the wider variety of encounters in others' homes), the graphs highlight differences in *relative* concerns. E.G., while smart speakers were viewed as highest-impact in one's own home, they were comparable with or less concerning than devices with cameras in others' homes. This aligns with findings in §4.2.1 and §4.2.4, where audio data is relatively high-impact in both contexts, but video ranks lower in participants' own homes.

4.3 RQ3: Privacy Protection

We aim to understand what privacy-protective mechanisms or behaviors are commonly used, and what options, given freedom over design, would be desired to preserve privacy.

4.3.1 Actual Protective Behaviors and Mechanisms. We asked free-answer questions about how participants protect their privacy around Selected Devices. In their own homes, 53% of participants said they do not do anything to protect their privacy ($N = 1252$ usable responses), and 66% did not do anything in others' homes ($N = 1220$) (χ^2=46.1, $p < 0.000001$, $V = 0.14$ effect of context.).[11]

Protection behavior across contexts is related; participants having at least one privacy protection in their own home moderately correlated with having a privacy protection in others' homes (χ^2=83.3, $p < 0.00001$, V=0.25; $N = 1289$). The percentage of "None" responses across the top five Selected Devices and across countries are shown in Table 15 and Table 18 in Appx. C.

Fig. 8 shows the protective behaviors and mechanisms that were used around the three most commonly presented Selected Devices for each context; additional data is in Tables 16 and 17 in Appx. C.[12] For smart speakers, the most common strategy in participants' homes was to power off the device. Participants also changed settings, limited their use or information given to the speaker, and changed their own speaking behavior, e.g., censoring their conversations. For smart TVs, participants more frequently limited their use, changed settings, and managed security and access control.

In others' homes, the mechanisms were quite different: participants' primary protection against smart speakers was to change their speaking behavior and censor their conversations. They also limited or avoided use of the device, and avoided the speaker altogether. Security cameras were the highest concern in others' homes (see §4.2.5); to deal with cameras and smart doorbells, participants avoided the cameras or modified their behavior, for example, walking a different path to avoid being captured by a neighbor's camera or covering their face. For doorbells, participants also changed their speaking behavior, e.g. to avoid having their voice recorded.

Amongst participants who did not employ protective strategies, some offered explanations. In many cases, they didn't feel it was necessary, at least with the device in question: "Nothing really, it only records outside so I have no issues" (UsEn588). However, a sense of defeatism was also common; participants said they felt that they did not know how or did not have the ability to protect their privacy (see discussion in §4.4.3).

We found that participants were somewhat more likely to protect their privacy if they had concerns about devices, both in their home (χ^2=40.5, $p < 0.00001$, V=0.18; $N = 1310$), and in others' homes (χ^2=33.9, $p < 0.00001$, V=0.17; $N = 1241$). In participants'

[11] We did not include participants as saying "None" if they said, for example, "Nothing, because I avoid them" (i.e. None + a strategy). Rather, we counted these responses as having a protection strategy.

[12] Findings in §4.3 are organized around the most frequent Selected Devices, which do not exactly match the ranking of highest-impact devices given in §4.2.5 because of the randomized downselection from three devices to one.

own homes, there was no statistically significant correlation between comfort with devices and enacting privacy protections, but in others' homes, there was a small trend; participants who were comfortable were less likely to enact protections ($\chi^2 = 17.2$, $p < 0.0001$, $V = 0.11$). We conjecture that, in participants' own homes, the interaction may be more complex (discomfort may prompt protections, but protections may increase feelings of comfort), obscuring the relationship, whereas in others' homes, efficacy of protections against unfamiliar or unknown devices may be less certain.

Additional Variation in Privacy Protections. Whether participants take at least one privacy precaution varied somewhat across countries, in their own homes ($\chi^2 = 20.1$, $p < 0.001$, $V = 0.12$ effect of country) and in others' homes ($\chi^2 = 25.9$, $p < 0.00001$, $V = 0.14$), with participants in the US and Mexico being most likely to protect themselves in either context.

4.3.2 Desired Privacy Options. To explore creative ideas that might be beyond the scope of the existing mechanisms described in §4.3.1, we also asked free-answer questions about what privacy options participants would like for the Selected Device, if they could have any options they could imagine. In their own home, only 11% of participants ($N = 1252$ usable responses) said they do not want any privacy options for the Selected Device; see Table 19 and Table 22 in Appx. C for a breakdown by devices and countries.[13]

Desired privacy options for participants' own homes and others' homes are shown in Fig. 9, again broken down into the three most commonly presented Selected Devices; additional data is in Tables 20 and 21 in Appx. C. In their own homes, participants want control over the data collected and the use of that data, for all devices, along with access control. For smart speakers, they also wanted an easy method to disable microphones and control activation, echoing frequently mentioned concerns and perceived privacy impacts from unknown or unwanted collection of audio data by those devices (see §4.2.1 and §4.2.4). For smart TVs and streaming devices, participants also wanted to be able to restrict activity tracking.

In others' homes, 13% of participants ($N = 1233$) did not want any privacy options, and some opined that it is not their business. However, most did offer ideas. Similar to their own home, it was important for many participants to have control over data collected about them. For smart speakers, they suggested methods to disable microphones and control activation. For security cameras and smart doorbells, participants wanted ways to control access; as in §4.2.1, participants were especially concerned about who might have access to video data. It is striking that, while actual protections were different between own and others' homes, participants' suggested new options would be much more similar across contexts.

Participants often recognized that controlling data practices is more challenging in others' homes, but many still had specific ideas, e.g.: "I wouldn't want to impose on others, but an option to temporarily halt all data collecting would be nice." (GrEn1171) This general interest in privacy options even in situations where participants do not have power to implement them likely underlies the small magnitude (and lack of statistical significance) in the difference in number of participants suggesting privacy options between own-home and others'-homes contexts. Correlations between comfort with IoT devices in each context and wanting privacy options also were not statistically significant, further suggesting that participants' responses were more imaginative (as we asked for) and less rooted in specifics of their own situations. At the same time, the contexts were correlated with each other; wanting privacy options in one's own home predicts one is more likely to want options in others' homes ($\chi^2 = 60.3$, $p < 0.000001$, $V = 0.24$, $N = 1101$).

Variation across countries in whether participants suggested privacy options (see Tab. 22, Appx. C) was not statistically meaningful.

[13]Percentages are after dropping responses that were usable but difficult to classify as to whether options were wanted.

4.4 Common Themes

Our thematic analysis process uncovered a variety of themes that surfaced in answers across multiple qualitative questions.

4.4.1 Pervasiveness of Data Collection and Sharing. Participants had many concerns about excessive data collection and sharing. Particularly, collection that occurred in the background, included sensitive audio or video content, or was surveillance-focused was problematic. This included concerns about increasing the threat surface area with more devices and more collection: «Sospecho que mientras más dispositivos inteligentes menos privacidad se conserva» (MxSp284) *("I suspect that the more smart devices there are, the less privacy is preserved").* Always-listening devices were framed as a privacy concern because they could listen when conversations were not intended to be shared. A related concern focused on being monitored and tracked. Participants were sometimes explicit targets of surveillance: "My partner installed several security cameras in various locations of our apartment to monitor the activity of, well basically to monitor my activity" (UsEn561).

4.4.2 Uncertainty About Data Collection and Sharing. While many were concerned about pervasiveness of data collection and sharing, participants often were not sure whether or when it was occurring—and some viewed the uncertainty as a problem in itself: «Mucha preocupación. No sabes cuando te están grabando» (UsSp368). *("It's a big worry. You don't know when they're recording you.")*

Participants were more likely to feel like they knew what was going on in their own homes, where they had more control over the environment—but even then were often unsure about details of data practices. Some found it problematic not to know how well the device and its data were protected: "I believe that there is an obvious risk whenever you use a smart device as they can be hacked or they can stop working which means that can put you at risk sometimes when you don't know the reason." (UsEn723)

Uncertainty about unknown devices was especially a concern in other people's homes—either because the hosts did not happen to tell them, or because they were deliberately hiding them: "I haven't ever confirmed that someone may have hidden cameras in their house but I don't like being watched without consent" (UsEn689).

4.4.3 Agency, Power, and Control. Participants who were concerned about privacy impacts of smart home devices sometimes expressed it in terms of loss of control: «Quitan la privacidad de mi familia» (MxSp201) *("They take away my family's privacy").* In particular, they focused on loss of control over data: "I strongly suspect, that smart devices might 'listen' too much and transfer data that I may not be able to control." (GrEn1160)

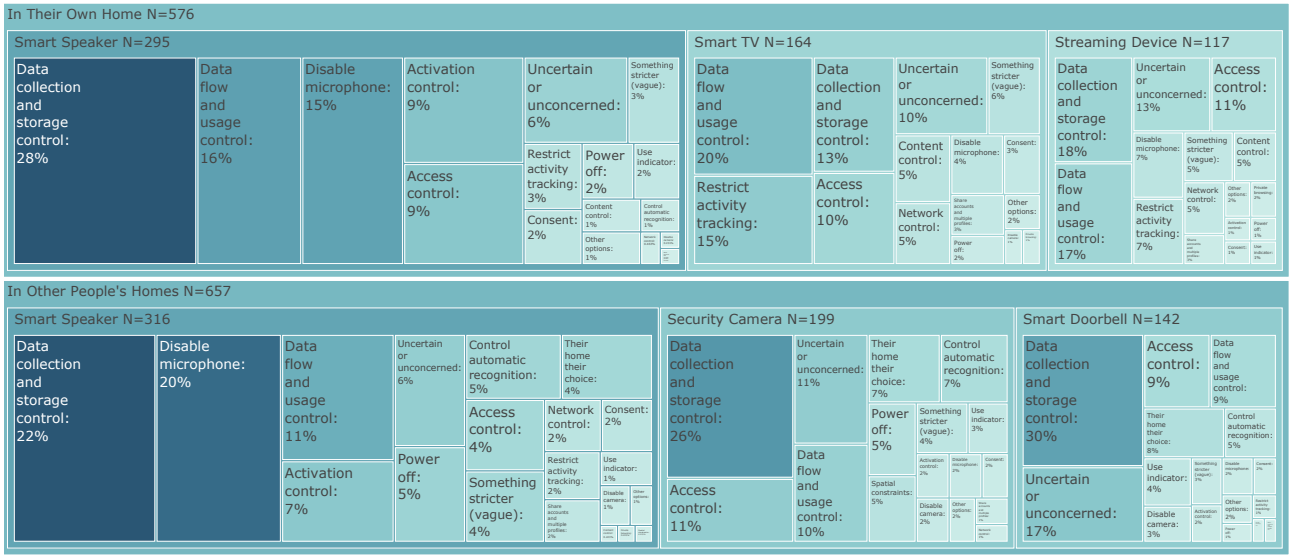

Figure 9: Desired privacy options for participants' homes and others' homes, for most commonly presented Selected Devices.

Some participants were concerned about social impediments to even asking for changes to others' devices, even if they might like to, for example viewing it as violating social norms about hospitality and domains of control: «Yo tengo menos control de mi privacidad porque hay que respetar los hogares de otros y como manejan su hogar» (UkSp427) *("I have less control of my privacy because I have to respect other people's homes, and how they run their home")* However, others were more comfortable with accepting these norms, though this could be mediated by other power dynamics, for example employment relationships: "I don't really worry about it because I don't expect to have privacy in other people's homes when I'm working, which is when I'm usually in other people's homes" (UsEn525).

4.4.4 Trade-Offs and Resignation. While many respondents took direct action to protect their privacy, many others took a more passive approach. Some felt the need to construct a discourse to justify and normalize the asymmetric status quo between users and the companies that manufacture smart home devices, as well as between bystanders and primary users or owners; indicating acceptance of privacy loss are a very important element of this discourse. Some users frame the situation in terms that privacy loss has been the norm in many contexts for some time: "Nothing is for sure 100% private anymore, even before smart devices" (UsEn511).

Others are categorical, suggesting that acceptance is a better option than self-complacency and self-deception: "No one has privacy anymore. Let's not pretend otherwise, comforting as it is to try" (UsEn677). However, justifications for the situation vary across contexts: in one's own home, privacy violation is often described as inevitable or normal; while in others' homes, it relates to not being able to control someone else's device, having to respect household rules, or trusting the owner's good judgment.

Trade-offs are another central element in this normalizing discourse. Participants point out that their privacy is being subjected to a form of exchange, often acceptable to them because of added convenience or security: «Me siento constantemente vigilada, pero es el precio justo a pagar por sentirme segura ya que vivo en una ciudad con altos índices de peligrosidad, entonces prefiero que estos dispositivos me mantenga vigilada a costa de mi privacidad con el fin de tener pruebas videograbadas en caso de un delito» (MxSp245) *("I feel constantly watched, but that's the fair price I pay for feeling safer since I live in a city with high crime rates, so I prefer to have these devices keeping an eye on me, even at the expense of my privacy, in order to get footage as proof in case of a crime").*

4.4.5 Trust as Protection. Another significant theme was trust in other people, companies who build devices, and privacy law as possible protections—or at least the only realistic ones. Some respondents chose to actively trust authority figures who can provide protection, e.g., privacy laws, academia, and companies; or spaces that they perceive as safe, e.g., family, friends, or people they visit frequently: «Sé que existe un riesgo, pero no lo tomo tan en serio porque sé que hay millones de dólares en investigación para ofrecer al cliente una seguridad adecuada» (MxSp341) *("I know there is a risk, but I don't take it that seriously because I know there are millions of dollars in research for providing clients with sufficient security").*

Although they have reservations, some participants cede their trust to formal legal mechanisms for regulating their information: "Under UK law we have the right to be informed how our data is used—I have no idea whether data is encrypted when being transmitted to my energy provider" (UkEn866).

5 Discussion

In this section, we discuss big picture takeaways, concrete recommendations for developers and policy makers, and future work.

5.1 Summary of Takeaways

Similarities, Differences, and Correlations Across Contexts. Participants encountered a more diverse set of devices in others' homes compared with their own home. Unsurprisingly, they also used them less (thus not receiving benefit from exposure of their data). For the most part, participants had less control over devices in others' homes, in terms of being less likely to have an account and to have input on, or even know about, privacy settings. But a surprisingly large portion had configured devices in others' homes, showing that sometimes visitors do have agency over settings.

Across contexts, participants voiced concerns about data collection and storage, especially when recorded by audio devices where participants were uncertain about activation. This agrees with previous literature [e.g. 7, 9, 30, 49, 75, 96]; we confirm these concerns at scale and across different countries, socioeconomic factors, and demographic backgrounds. For the most part, participants were less likely to have concerns in others' homes. However, in others' homes, video cameras—especially unknown video cameras—were cause for more concern, and seen as having a larger privacy impact compared with in participant's homes. Usability was also more of a concern in others' homes, possibly due to unfamiliarity.

On the other hand, in participants' own homes, concerns were more focused on how device data was being used and shared. Generally, while a majority of participants in most countries were at least somewhat comfortable interacting with the devices in both contexts, a majority were uncomfortable with those devices sending data outside the home. We found that feeling comfortable with smart home devices, having concerns, having privacy protection strategies, and having ideas for better privacy options were each correlated across the two contexts for the same participant.

Participants were more likely to implement protective behaviors if they had concerns in a given context, though the effect was small. Protections differed across contexts; e.g., for smart speakers in their own home, participants most frequently turned off the device, reflecting concerns with uncertainty about data collection in standby mode. In others' homes, where direct control is less possible, the primary protections around smart speakers were to alter speaking behavior and censor conversations. This gives evidence at a larger, cross-national scale to support practices that had been reported before [e.g. 1, 75, 88], particularly differences between contexts in types of protections [30]. Desired privacy options were more similar across contexts than were actual protective behaviors, with participants suggesting means of controlling data collection and use in both contexts, along with access control. This adds breadth from an international sample to prior findings in the U.S. that bystanders are most interested in proposed designs that offer them control of data, sometimes valuing it even more highly than owners [e.g. 36, 130]. However, in others' homes, some of our participants mentioned feeling they do not have an expectation of privacy, e.g. due to social norms—but nonetheless, most participants (in all countries) had ideas for what they would control if they could.

Cross-Country Differences in Exposure, Concerns and Protections. Internationally, participants in Germany showed the most concern specifically about privacy, and were the least comfortable. This is aligned with the fact that participants in Germany had the fewest device types in their own homes, following the correlation we found between own-home exposure and comfort generally. This finding contrasts with findings in a smaller survey by Bombik et al. [19] that found similar patterns of smart home device ownership and use between Germany-Austria-Switzerland, the UK, and the USA, despite differing levels of concern. However, our results are more in line with cross-national privacy research suggesting that, in general, technology penetration and habituation seem to play a much bigger role in being comfortable / having less privacy concern than any cultural differences [43].

Participants in Mexico expressed the most concerns about functionality, and were more comfortable with smart home devices, in both their own homes and others', despite being most likely to have concerns and to notice privacy impacts. The relationship between discomfort and having concerns may be less tightly correlated in Mexico, demonstrating how nuanced relationships can be between specific perceived issues and general attitudes [cf. 31, 126].

Meanwhile, participants in the US and Mexico were more likely to take privacy precautions, in both contexts, while UK and Germany participants were less likely. Some previous studies similarly found that German participants were less comfortable sharing information online than in the UK and US [e.g. 19, 33]—though not necessarily by much [e.g. 70, 132]—however, they had mixed results for protective behaviors. Teasing this out, a small interview study [39] found that US participants were more likely than German participants to believe they *could* control their privacy. A similar belief with regard to smart home privacy may explain the otherwise counterintuitive lack of correlation we found between comfort with devices and likelihood of protecting privacy in one's own home.

Demographic Differences In Control and Exposure. Significant differences emerged in adoption, usage, and configuration patterns between male and female respondents. For instance, males were more involved in deciding to get the device, making the purchase, and owning the device, compared to non-male participants. Additionally, male participants were more likely to be involved in configuring the device and setting privacy options—and this pattern held regardless of whether the participant was the most frequent user of that device. These effects were similar across Germany, Mexico, and the US. However, gender effects on adoption were insignificant in the UK, while gender effects on control of privacy were larger; this merits further exploration.

These findings confirm and generalize qualitative work suggesting that women are more often in secondary-user or passenger-user roles in smart homes [49, 67, 125], and demonstrates the consequences of negative assumptions about women's ability to administer smart home devices [cf. 27, 68]. In addition, our findings show how gender dynamics play out specifically in terms of *who controls privacy settings*. Participants from the 25–45 age group were more involved with device adoption and configuring privacy settings. However, age did not have a significant impact on attitudes; no age group was more comfortable with devices than any other.

5.2 Limitations

We recruited on Prolific to maximize data quality [40, 107], so we are limited to the participant pool on the platform. This could bias our sample towards a younger, more technically comfortable participant pool. (And, especially in the case of Mexico, a more highly urban one,

given higher Internet penetration in urban areas [58].) We made an effort to balance our demographics to be representative of the population within each country, but there are still skews, and our participants may not fully represent the range of experiences and preferences across populations in each country. In addition, because we required participants to be fluent in English or Spanish (so we could include free-answer questions), participants in Germany on average are more highly educated than the general population.

Finally, we limited the study to four countries so we could recruit enough participants per country to make robust statistical comparisons. Although a survey in four countries via two languages allows for some breadth of comparison, deploying in more languages and in more countries—particularly, countries outside North America and Europe—would provide a more comprehensive picture.

5.3 Future Avenues for Research

Our research highlights some ways that interpersonal, demographic, and geographic factors interact with people's experiences in their own and others' smart homes. These findings should be expanded by exploring the most interesting factors in a study in more countries (on more continents), facilitated by deploying surveys in more languages. At the same time, we suggest future research should explore in more depth factors that might drive the cross-national variation uncovered in some of our findings. Prior research has suggested that cross-country differences in data privacy views can be affected or mediated by policies and regulatory climate in different countries [e.g. 33, 39, 116, 137], as can comfort with IoT devices generally [19, 74]). E.G., as we noted in §5.1, Dogruel and Joeckel [39] found US participants had a stronger bent towards do-it-yourself privacy protection and viewed themselves as having better control of their smartphone data than German participants. This may help explain the complex interaction of attitudes and behaviors in our finding that US participants were both more comfortable with devices and more likely to take active privacy precautions.

Other cross-national factors that could be explored include the role of economic structures and Internet penetration [cf. 43, 116]; characteristics of prevalent vendors [cf. 46]; and cultural factors [overview in 80], e.g., dimensions of cultural difference suggested by Hofstede et al. [55].[14] So far, there is contradictory evidence on the role the proposed cultural dimensions play in digital privacy views, with some literature suggesting their role is significant [82, 133] and others that they are not [43]. Clearly, more exploration of cultural factors is needed, particularly *within countries* (e.g., beginning with small focus groups to tease out how culture-specific perspectives on the home domain impact privacy views). Such nuanced cultural analyses could be supported by existing theoretical frameworks for identifying how people perceive and apply cultural norms of privacy, such as Contextual Integrity [13, 102] (see §2).

Empirical findings such as ours can suggest directions for studying relationships between between what people say they value about privacy (attitudes) and what they actually do (behaviors) in different cultural contexts with different norms —and at the same time, how cultural norms are adapting to the way smart devices are reshaping home, family, and society [cf. 111].

[14]Though critiques of Hofstede et al. point out methodological weaknesses and problematic assumptions about, e.g., homogeneity of national cultures [e.g. 63, 95].

5.4 Recommendations for Design and Policy

Our free-answer questions about desired privacy options aimed to provide a balance of systematicity and depth—between the depth of participatory design studies [e.g. 30, 77, 144, 148, 149], which provide opportunity for imagination and collaboration but have small sample sizes, and the generalizability of multiple-choice surveys.

Participants' common suggestions (see §4.3.2) tended to focus on empowerment through control over data practices, such as disclosing data practices [see 44, 117, 130, 144, 148], reducing data collection and use [see 8, 26, 30, 86, 109], reducing storage duration [see 30, 87, 129, 149], access control [see 52, 85, 135, 148, 151], and tangible shutoff mechanisms [see 5, 36, 109, 144, 151]. An example could be guest profiles that allow customization [see 30, 109, 144, 149, 151] Lastly, participants wanted to manage information *flow* via transparency about data handling, as well as implement recognition control features [see 86, 87, 109, 127, 138]. Other common suggestions included consent mechanisms like clear opt-in/opt-out.

Participants' focus on control and transparency indicates these aspects are important, at least as a necessary minimum standard. However, those approaches are limited by time, attention, usability constraints, and social norms [overview in 4]. In particular, some participants suggested control options but noted they might not be attainable in someone else's home [cf. 30, 87]. Additional approaches are needed to mitigate imbalances in control of configuration and social norms for guests, such as high-privacy defaults [see 2, 17, 85, 86, 127], and social interaction mechanisms that could nudge users in shared spaces like rentals, e.g. to reconsider privacy settings [see 10, 18, 86, 109, 120, 140].

Similarly, while few of our participants commented explicitly on law and policy, some concerns they raised about systemic problems would best be addressed at that level (for arguments, see [e.g. 121, 134]). From a policymaker's perspective, advocating for transparent data practices for bystanders could include implementing IoT privacy nutrition labels directly on the devices [see 42, 87–89, 153]. Policymakers can also encourage smart home companies to make it easy to disclose device presence, activity status, and data collection processes without compromising usability.

Finally, though our findings did not concretely suggest different designs for different countries, we believe this could be a fruitful area for research—especially covering both WEIRD and non-WEIRD countries, with more varied privacy governance structures.

6 Conclusion

We examined smart home device exposure, adoption, usage, and configuration, along with general concerns, patterns of comfort and conflict, privacy impacts, privacy protection mechanisms and options across different contexts (at your own home and at others homes), countries, and sociodemographic factors. This allowed us to observe trends such as a higher tendency for males to decide to get, purchase, manage, and configure smart home devices, and less privacy protection strategies in the US. Across countries and contexts, we noticed broad concerns over data collection and storage (and uncertainty about when and how this happens); loss of agency and control over privacy and data; the weaving of a normalizing discourse around privacy trade-offs; and the necessity of trusting one's privacy to others.

Acknowledgments

We are grateful to Priyasha Chatterjee, Junghyun Choy, Alisa Frik, David Harper-Clark, Mobin Javed, Nathan Malkin, and Franziska Roesner for advice and feedback on the study design and analysis, and to Prabal Dutta and Serge Egelman for additional support. Suggestions were also contributed by members of Lab11 and the BLUES Lab at UC Berkeley and ICSI, by attendees of the 2022 Symposium on Applications of Contextual Integrity, and by the anonymous PoPETs reviewers and shepherd. Special thanks are due to Junghyun Choy and Ichchitaa Sawrikar, who contributed to the initial development and testing of the qualitative codebook.

This research was funded in part by grants to ICSI from the U.S. National Science Foundation (award CNS-2114229, "Foregrounding Bystanders as Stakeholders in Smart Home Product Design") and the US National Security Agency (contract H98230-18-D-0006); by a grant to KCL from the Engineering and Physical Sciences Research Council, *SAIS: Secure AI assistantS* (EP/T026723/1) and a King's-China Scholarship Council (K-CSC) PhD Scholarship; by the CONIX Research Center at UC Berkeley, one of six centers in JUMP, a Semiconductor Research Corporation (SRC) program sponsored by DARPA; and by INCIBE's strategic SPRINT (Seguridad y Privacidad en Sistemas con Inteligencia Artificial) project C063/23, with funds from NextGenerationEU.

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Fifteenth USENIX Symposium on Usable Privacy and Security (SOUPS 2019)* (Santa Clara, CA, USA). Santa Clara, CA, USA, 451–466.

[2] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. Privacy Norms for Smart Home Personal Assistants. In *ACM Conference on Human Factors in Computing Systems (CHI) (CHI '21)*. New York, NY, USA, 1–14. https://doi.org/10.1145/3411764.3445122

[3] Ruba Abu-Salma and Benjamin Livshits. 2020. Evaluating the End-User Experience of Private Browsing Mode. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376440

[4] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2022. Privacy and Behavioral Economics. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, Cham. https://link.springer.com/10.1007/978-3-030-82786-1

[5] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW (2020), 1–28.

[6] Ali Ahmed, Victor Ungureanu, Tarek Gaber, Craig Watterson, and Fatma Masmoudi. 2024. Smart Home Privacy: A Scoping Review. 635–642. https://www.scitepress.org/Link.aspx?doi=10.5220/0012255900003648

[7] Wael Albayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA. https://doi.org/10.1145/3491102.3502097

[8] Wael S. Albayaydh and Ivan Flechais. 2024. Co-designing a mobile app for bystander privacy protection in Jordanian smart homes: a step towards addressing a complex privacy landscape. In *USENIX Security Symposium*. To appear.

[9] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. 2022. Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 99–119.

[10] Ahmed Mohammed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T Parker, Benjamin Gilbert, and Chuan Yue. 2023. Exploring the Negotiation Behaviors of Owners and Bystanders over Data Practices of Smart Home Devices. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023).

[11] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2020. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. *arXiv:2001.10608 [cs]* (July 2020). http://arxiv.org/abs/2001.10608

[12] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *ArXiv* (2017). arXiv:1708.05044

[13] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies (IMWUT)* 2, 2 (June 2018), 1–23. https://doi.org/10.1145/3214262

[14] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA. In *28th USENIX Security Symposium (USENIX Security)*. Santa Clara, CA, USA, 123–140. https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

[15] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. 2018. Ethical Design in the Internet of Things. *Science and Engineering Ethics* 24, 3 (01 June 2018), 905–925. https://doi.org/10.1007/s11948-016-9754-5

[16] Sebastian Benthall, Seda Gürses, and Helen Nissenbaum. 2017. *Contextual integrity through the lens of computer science*. Now Publishers.

[17] Arne Berger, Albrecht Kurze, Andreas Bischof, Jesse Josua Benjamin, Richmond Y. Wong, and Nick Merrill. 2023. Accidentally Evil: On Questionable Values in Smart Home Co-Design. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 629, 14 pages. https://doi.org/10.1145/3544548.3581504

[18] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA. https://www.usenix.org/conference/soups2022/presentation/bernd

[19] Patrick Bombik, Tom Wenzel, Jens Grossklags, and Sameer Patil. 2022. A Multi-Region Investigation of the Perceptions and Use of Smart Home Devices. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 6–32. https://petsymposium.org/2022/files/papers/issue3/popets-2022-0060.pdf

[20] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *New York Times* (June 2018). https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html Accessed: 23 July 2018.

[21] danah boyd and Kate Crawford. 2012. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication, & Society* 15, 5 (2012), 662–679. https://doi.org/10.1080/1369118X.2012.678878

[22] Virginia Braun and Victoria Clarke. 2012. *Thematic analysis*. American Psychological Association.

[23] Alice Jane Bernheim Brush and Kori Inkpen Quinn. 2007. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In *Ubiquitous Computing*.

[24] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2020. A Privacy-Centered System Model for Smart Connected Homes. *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (2020), 1–4.

[25] Cámara de Diputados del Congreso de los Estados Unidos Mexicanos. 2017. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (General Law on the Protection of Personal Data in the Posession of Obligated Entities). https://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm English translation at https://www.creel.mx/en/noticias/general-law-for-the-protection-of-personal-data/.

[26] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Number 555. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3411764.3445691

[27] D. Chambers. 2020. Domesticating the "Smarter Than You" Home: Gendered Agency Scripts Embedded in Smart home Discourses. *M&K Medien & Kommunikationswissenschaft* (2020). https://doi.org/10.5771/1615-634X-2020-3-304 Publisher: Newcastle University.

[28] Yi-Shyuan Chiang, Omar Khan, Adam Bates, and Camille Cobb. 2024. More than just informed: The importance of consent facets in smart homes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (, Honolulu, HI, USA,) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 849, 21 pages. https://doi.org/10.1145/3613904.3642288

[29] Danielle Keats Citron. 2022. *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. Chatto & Windus.

[30] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy Tensions Between Smart Home Device Owners and Incidental Users. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2021, 4 (2021), 54–75.

[31] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. 2020. How Risky Are Real Users' IFTTT

Applets?. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. 505–529. https://www.usenix.org/conference/soups2020/presentation/cobb
[32] Jacob Cohen. 1969. Statistical Power Analysis for the Behavioral Sciences. *The SAGE Encyclopedia of Research Design* (1969). https://api.semanticscholar.org/CorpusID:123217261
[33] Kovila P.L. Coopamootoo, Maryam Mehrnezhad, and Ehsan Toreini. 2022. "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 287–304. https://www.usenix.org/conference/usenixsecurity22/presentation/coopamootoo
[34] Harald Cramér. 1946. *Mathematical Methods of Statistics*. Princeton University Press.
[35] DD Furszyfer Del Rio, BK Sovacool, and M Martiskainen. 2021. Controllable, frightening, or fun? Exploring the gendered dynamics of smart home technology preferences in the United Kingdom. *Energy Research & Social Science* 77 (2021), 102105.
[36] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey–Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference*. 1–13.
[37] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer security and the modern home. *Commununications of the ACM* 56 (2013), 94–103.
[38] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J Wisniewski. 2020. Exploring Smart Home Device Use by Airbnb Hosts. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*. New York, New York, United States, 1–8.
[39] Leyla Dogruel and Sven Joeckel. 2019. 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, 0 (2019). https://ijoc.org/index.php/ijoc/article/view/9824
[40] Benjamin D. Douglas, Patrick J. Ewell, and Markus Brauer. 2023. Data quality in online human-subjects research: Comparisons between MTurk, Prolific, CloudResearch, Qualtrics, and SONA. *PLOS ONE* (14 March 2023). https://doi.org/10.1371/journal.pone.0279720
[41] Jide Edu, Jose Such, and Guillermo Suarez-Tangil. 2020. Smart home personal assistants: A security and privacy review. *ACM Computing Surveys (CSUR)* 53, 6 (2020), 1–36.
[42] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2022. An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy* 20, 2 (2022), 31–39. https://doi.org/10.1109/MSEC.2021.3132398
[43] Emma Engström, Kimmo Eriksson, Marie Björnstjerna, and Pontus Strimling. 2023. Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports* 9 (2023), 100268. https://doi.org/10.1016/j.chbr.2023.100268
[44] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. 2022. Transparency for Bystanders in IoT regarding audiovisual Recordings. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. 649–654. https://doi.org/10.1109/PerComWorkshops53856.2022.9767212
[45] Virginia E. Eubanks. 2018. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.
[46] Bente Evjemo, Humberto Castejón-Martínez, and Sigmund Akselsen. 2019. Trust trumps concern: Findings from a seven-country study on consumer consent to "digital native" vs. "digital immigrant" service providers. *Behaviour & Information Technology* 38, 5 (2019), 503–518. https://doi.org/10.1080/0144929X.2018.1541254
[47] Diane Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3 (2019), 1–24.
[48] GDPREU. 2022. What is GDPR, the EU's new data protection law. https://gdpr.eu/what-is-gdpr/
[49] Christine Geeng and Franziska Roesner. 2019. Who's in Control? Interactions in Multi-User Smart Homes. In *Proceedings of the 2019 ACM CHI Conference on Human Factors in Computing Systems (CHI '19)* (Glasgow, Scotland UK). New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498
[50] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile?: Technology, risk and privacy among undocumented immigrants. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 1–15.
[51] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. 2020. Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. In *International Conference on Human-Computer Interaction*. Springer International Publishing, 393–411. https://doi.org/10.1007/978-3-030-50309-3_26
[52] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *USENIX Security Symposium (USENIX Security)*. Baltimore, MD, USA, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he
[53] Weijia He, Nathan Reitinger, Atheer Almogbil, Yi-Shyuan Chiang, Timothy J. Pierson, and David Kotz. 2024. Contextualizing Interpersonal Data Sharing in Smart Homes. *Proceedings on Privacy Enhancing Technologies* (2024). https://petsymposium.org/popets/2024/popets-2024-0051.php
[54] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, M. Angela Sasse, Yasemin Gülsüm Acar, and Markus Durmuth. 2022. A World Full of Privacy and Security (Mis)conceptions? Findings of a Representative Survey in 12 Countries. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2022). https://api.semanticscholar.org/CorpusID:254877449
[55] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov. 2010. *Cultures and Organizations: Software of the Mind* (3 ed.). McGraw Hill LLC.
[56] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems (CHI '20)*. New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376529
[57] Information Commissioner's Office. 2018. The UK GDPR. https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/
[58] Instituto Nacional de Estadística y Geografía (INEGI) and Instituto Federal de Telecomunicaciones (IFT). 2023. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022*. Technical Report. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf
[59] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 workshop on internet of things security and privacy*. 49–54.
[60] Mark Johnson, Maggy Lee, Michael McCahill, and Ma Rosalyn Mesina. 2020. Beyond the 'All Seeing Eye': Filipino Migrant Domestic Workers' Contestation of Care and Control in Hong Kong. *Ethnos* 85, 2 (2020), 276–292. https://doi.org/10.1080/00141844.2018.1545794
[61] George Joseph. 2016. Racial Disparities in Police 'Stingray' Surveillance, Mapped. *CityLab* (October 2016). https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-surveillance-mapped/502715/ Accessed: 7 June 2020.
[62] Bei Ju, Xiao Yang, Xiao Hong Pu, and TL Sandel. 2023. (Re) making live-in or live-out choice: the lived experience of Filipina migrant domestic workers in Macao. *Gender, Place & Culture* (2023), 1–22.
[63] Min-Sun Kim. 2007. Our Culture, Their Culture, and Beyond: Further Thoughts on Ethnocentrism in Hofstede's Discourse. *Journal of Multicultural Discourses* 2, 1 (2007), 26–31. https://doi.org/10.2167/md051c.2
[64] Jason E King. 2008. Binary logistic regression. *Best practices in quantitative methods* (2008), 358–384.
[65] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *ACM Conference on Human Factors in Computing Systems (CHI)* (Yokohama, Japan). New York, NY, USA, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598
[66] M.J. Kraemer and I. Flechais. 2018. Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods. In *Proceedings: Living in the Internet of Things: Cybersecurity of the IoT (IET Conference Proceedings)*. Institution of Engineering and Technology. http://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0038
[67] Martin J. Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *ACM Halfway to the Future Symposium (HTTF)* (Nottingham, United Kingdom). New York, NY, USA, Article 5, 8 pages. https://doi.org/10.1145/3363384.3363389
[68] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further Exploring Communal Technology Use in Smart Homes: Social Expectations. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*. New York, New York, United States, 1–7. https://doi.org/10.1145/3334480.3382972
[69] Martin J. Kraemer, William Seymour, and Ivan Flechais. 2020. Responsibility and Privacy: Caring for a Dependent in a Digital Age. In *CHI Workshop on Privacy and Power (Networked Privacy)*.
[70] Hanna Krasnova, Natasha F. Veltri, and Oliver Günther. 2012. Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture. *Business & Information Systems Engineering* 4 (06 2012), 127–135. https://doi.org/10.1007/s12599-012-0216-6
[71] William H. Kruskal and Wilson Allen Wallis. 1952. Use of Ranks in One-Criterion Variance Analysis. *J. Amer. Statist. Assoc.* 47 (1952), 583–621. https://api.semanticscholar.org/CorpusID:51902974

[72] Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Elaine Newton. 2005. Privacy perceptions in India and the United States: An interview study. In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)*. 23–25.

[73] Lawrence L Kupper and Kerry B Hafner. 1989. On assessing interrater agreement for multiple attribute responses. *Biometrics* (1989), 957–967.

[74] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3411763.3451633

[75] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[76] Roxanne Leitão. 2018. Digital Technologies and Their Role in Intimate Partner Violence. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts* (Montreal, QC, Canada). New York, NY, USA. https://doi.org/10.1145/3170427.3180305

[77] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *ACM Conference on Designing Interactive Systems (DIS)* (San Diego, CA, USA). New York, NY, USA, 527–539. https://doi.org/10.1145/3322276.3322366

[78] Leigh Levinson, Christena Nippert-Eng, Randy Gomez, and Selma Sabanović. 2024. Snitches Get Unplugged: Adolescents' Privacy Concerns about Robots in the Home are Relationally Situated. In *Proceedings of the 2024 ACM/IEEE International Conference on Human-Robot Interaction (HRI '24)*. Association for Computing Machinery, New York, NY, USA, 423–432. https://doi.org/10.1145/3610977.3634946

[79] Jingjie Li, Kaiwen Sun, Brittany Skye Huff, Anna Marie Bierley, Younghyun Kim, Florian Schaub, and Kassem Fawaz. 2023. "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. *2023 IEEE Symposium on Security and Privacy (SP)* (2023), 2850–2866. https://api.semanticscholar.org/CorpusID:260002623

[80] Yao Li. 2022. Cross-Cultural Privacy Differences. In *Modern Socio-Technical Perspectives on Privacy*. Springer, 267–292.

[81] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P Knijnenburg. 2022. Privacy and the Internet of Things. In *Modern Socio-Technical Perspectives on Privacy*. Springer, 233.

[82] Paul Benjamin Lowry, Jinwei Cao, and Andrea Everard. 2011. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of management information systems* 27, 4 (2011), 163–200.

[83] Mary Madden. 2019. The Devastating Consequences of Being Poor in the Digital Age. *New York Times* (April 2019). https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html Accessed: 7 June 2020.

[84] Mary Madden, Michele E. Gilman, Karen Levy, and Alice E. Marwick. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review* 95, 1 (2017), 53–125. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930247

[85] Nathan Malkin, Alan F. Luo, Julio Poveda, and Michelle L. Mazurek. 2023. Optimistic Access Control for the Smart Home. In *2023 IEEE Symposium on Security and Privacy (SP)*. 3043–3060. https://doi.org/10.1109/SP46215.2023.10179475 ISSN: 2375-1207.

[86] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2020, 2 (2020), 436–458. https://doi.org/10.2478/popets-2020-0035

[87] Karola Marky, Nina Gerber, M Pelzer, and M. Khamis. 2022. "You offer privacy like you offer tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households. *Proc. Priv. Enhancing Technol.* 2022 (2022), 400–420.

[88] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19thInternational Conference on Mobile and Ubiquitous Multimedia (MUM)*. 83–95.

[89] Karola Marky, Sarah Prange, M. Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia* (2021).

[90] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *ACM Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI)*. New York, NY, USA, Article 4, 11 pages. https://doi.org/10.1145/3419249.3420164

[91] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: an empirical test using context to expose confounding variables. *Columbia Science & Technology Law Review* 18 (2016).

[92] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert W. Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016).

[93] Mary L McHugh. 2013. The chi-square test of independence. *Biochemia medica* 23, 2 (2013), 143–149.

[94] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and Internet-connected toys. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 5197–5207.

[95] Brendan McSweeney. 2002. Hofstede's Model of National Cultural Differences and their Consequences: A Triumph of Faith—a Failure of Analysis. *Human Relations* 55, 1 (2002), 89–118. https://doi.org/10.1177/0018726702551004

[96] Nicole Meng, Dilara Kekülüoğlu, and Kami Vaniea. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW, Article 45 (April 2021), 29 pages. https://doi.org/10.1145/3449119

[97] Nicole Meng-Schneider, Rabia Yasa Kostas, Kami Vaniea, and Maria Klara Wolters. 2023. Multi-User Smart Speakers - A Narrative Review of Concerns and Problematic Interactions. *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (2023).

[98] Meteorelectrical. 2023. Best Selling Smart Home Devices UK. https://www.meteorelectrical.com/blog/best-selling-smart-home-devices-uk.html

[99] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. 2016. Understanding the Privacy Design Space for Personal Connected Objects. In *International BCS Human Computer Interaction Conference: Fusion! (BCS HCI)* (Poole, UK). BCS Learning & Development Ltd., Swindon, UK, Article 18, 13 pages. https://doi.org/10.14236/ewic/HCI2016.18

[100] Larissa Nicholls, Yolande Strengers, and Jathan Sadowski. 2020. Social impacts and control in the smart home. *Nature Energy* 5, 3 (2020), 180–182.

[101] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79, 119 (2004), 101–139.

[102] Helen Nissenbaum. 2019. Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law* 20, 1 (2019), 221–256.

[103] Oberlo. 2022. US Households Using Smart Home Devices. https://www.oberlo.com/statistics/smart-home-statistics

[104] Cathy O'Neil. 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.

[105] Elizabeth O'Neill. 2022. Contextual Integrity as a General Conceptual Tool for Evaluating Technological Change. *Philosophy & Technology* 35, 3 (Aug. 2022), 79. https://doi.org/10.1007/s13347-022-00574-8

[106] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. 2022. A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *Comput. Surveys* 55 (2022), 1 – 38.

[107] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (May 2017), 153–163. https://doi.org/10.1016/j.jesp.2017.01.006

[108] Scott R. Peppet. 2014. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent. *Texas Law Review* 93 (2014), 85–178. https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr93&div=5&id=&page=

[109] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurle, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *ACM Conference on Designing Interactive Systems (DIS)*. To appear.

[110] Sarah Pink, Yolande Strengers, Rex Martin, and Kari Dahlgren. 2023. Smart Home Masculinities. *Australian Feminist Studies* (2023), 1–17.

[111] Nicholas Proferes. 2022. The Development of Privacy Norms. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-82786-1

[112] Prolific Academic. 2023. Prolific Participants Recruiting Platform. https://prolific.ac/

[113] Anju Punuru, Tyng-Wen Cheng, Isha Ghosh, Xinru Page, and Mainack Mondal. 2020. Cultural Norms and Interpersonal Relationships: Comparing Disclosure Behaviors on Twitter. In *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing (CSCW '20)*. Association for Computing Machinery, New York, NY, USA, 371–375. https://doi.org/10.1145/3406865.3418341

[114] Qualtrics. 2023. Qualtrics. https://www.qualtrics.com/uk/

[115] Laura Robinson, Shelia R. Cotten, Hiroshi Ono, Anabel Quan-Haase, Gustavo Mesch, Wenhong Chen, Jeremy Schulz, Timothy M. Hale, and Michael J. Stern. 2015. Digital inequalities and why they matter. *Information, Communication & Society* 18, 5 (2015), 569–582. https://doi.org/10.1080/1369118X.2015.1012532

[116] Răzvan Rughiniş, Cosima Rughiniş, Simona Nicoleta Vulpe, and Daniel Rosner. 2021. From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Computer Law & Security Review* 42 (Sept. 2021), 105585. https://doi.org/10.1016/j.clsr.2021.105585

[117] Vandit Sharma and Mainack Mondal. 2022. Understanding and Improving Usability of Data Dashboards for Simplified Privacy Control of Voice Assistant Data. 3379–3395. https://www.usenix.org/conference/usenixsecurity22/presentation/sharma-vandit

[118] Michael Shlega, Sana Maqsood, and Sonia Chiasson. 2022. Users, Smart Homes, and Digital Assistants: Impact of Technology Experience and Adoption. In *Proceedings of HCI International*. 20.

[119] Yan Shvartzshnaider, Schrasing Tong, Thomas Wies, Paula Kift, Helen Nissenbaum, Lakshminarayanan Subramanian, and Prateek Mittal. 2016. Learning privacy expectations by crowdsourcing contextual informational norms. In *Fourth AAAI conference on human computation and crowdsourcing*.

[120] Julia Słupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You":
Participatory Threat Modelling with Migrant Domestic Workers. In *USENIX Security Symposium (USENIX Security)*. Boston, MA, USA.

[121] Daniel J. Solove. 2021. The Myth of the Privacy Paradox. *George Washington Law Review* 89 (2021). Issue 1. https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr93&div=5&id=&page=

[122] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376585

[123] Statista. 2023. Smart Home - Germany. https://www.statista.com/outlook/dmo/smart-home/germany

[124] Statista. 2023. Smart Home - Mexico. https://www.statista.com/outlook/dmo/smart-home/mexico

[125] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[126] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2019. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 4 (Dec. 2019). https://doi.org/10.1145/3369807

[127] Madiha Tabassum and Heather Lipford. 2023. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies* 2023 (01 2023), 571–588. https://doi.org/10.56553/popets-2023-0033

[128] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. 2017. Can unicorns help users compare crypto key fingerprints?. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 3787–3798.

[129] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *ACM CHI Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 1–25.

[130] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 1–13. https://doi.org/10.1145/3491102.3502137

[131] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*. Technical Report. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html Accessed 16 May 2022.

[132] Sabine Trepte and Philipp K. Masur. 2016. *Cultural differences in social media use, privacy, and self-disclosure : research report on a multicultural study*. Technical Report. http://opus.uni-hohenheim.de/volltexte/2016/1218/

[133] Sabine Trepte, Leonard Reinecke, Nicole B. Ellison, Oliver Quiring, Mike Z. Yao, and Marc Ziegele. 2017. A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society* 3, 1 (Jan. 2017). https://doi.org/10.1177/2056305116688035 Publisher: SAGE Publications Ltd.

[134] Joseph Turow, Yphtach Lelkes, Nora Draper, and Ari Ezra Waldman. 2023. Americans Can't Consent to Companies' Use of Their Data: They Admit They Don't Understand It, Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data–Making What Companies Do Illegitimate. https://doi.org/10.2139/ssrn.4391134

[135] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)* (Seattle, Washington). New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[136] Userfeel. 2023. Userfeel. https://www.userfeel.com/

[137] Jessica Vitak, Yuting Liao, Anouk Mols, Daniel Trottier, Michael Zimmer, Priya Kumar, and Jason Pridmore. 2022. When Do Data Collection and Use Become a Matter of Concern? A Cross-Cultural Comparison of U.S. and Dutch Privacy Attitudes. *International Journal of Communication* 17 (2022). https://ijoc.org/index.php/ijoc/article/view/19391

[138] Yuntao Wang, Zirui Cheng, Xin Yi, Yan Kong, Xueyang Wang, Xuhai Xu, Yukang Yan, Chun Yu, Shwetak Patel, and Yuanchun Shi. 2023. Modeling the Trade-off of Privacy Preservation and Activity Recognition on Low-Resolution Images. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3544548.3581425

[139] Yang Wang, Gregory Norice, and Lorrie Faith Cranor. 2011. Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. In *Trust and Trustworthy Computing*, Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 146–153.

[140] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring tenants' preferences of privacy negotiation in Airbnb. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*. 535–551. https://api.semanticscholar.org/CorpusID:260777548

[141] Miranda Wei, Pardis Emami Naeini, Franziska Roesner, and Tadayoshi Kohno. 2023. Skilled or Gullible*f* Gender Stereotypes Related to Computer Security and Privacy. *2023 IEEE Symposium on Security and Privacy (SP)* (2023), 2050–2067. https://api.semanticscholar.org/CorpusID:252667404

[142] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian Stefan Feger. 2022. SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proceedings of the ACM on Human-Computer Interaction* 6 (2022), 680 – 699.

[143] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI (2022), 1–21.

[144] Maximiliane Windl, Albrecht Schmidt, and Sebastian S Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[145] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 1093–1113. https://doi.org/10.1145/3563657.3596012

[146] World Inequality Lab. 2022. *Income Comparator Tool (part of The World Inequality Database, WID.world)*. Retrieved 8 November 2022 from https://wid.world/income-comparator/

[147] Yanlai Wu, Xinning Gui, Pamela J. Wisniewski, and Yao Li. 2023. Do Streamers Care about Bystanders' Privacy? An Examination of Live Streamers' Considerations and Strategies for Bystanders' Privacy Management. *Proceedings of the ACM on Human-Computer Interaction* 7 (2023), 1 – 29.

[148] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[149] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 59 (Nov. 2019), 24 pages. https://doi.org/10.1145/3359161

[150] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[151] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 2019)*. Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[152] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. 2022. "If sighted people know, I should be able to know: " Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology. *ArXiv* abs/2210.12232 (2022).

[153] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–20.

[154] Nicole Zillien and Eszter Hargittai. 2009. Digital Distinction: Status-Specific Types of Internet Usage. *Social Science Quarterly* 90, 2 (2009), 274–291. https://doi.org/10.1111/j.1540-6237.2009.00617.x

A Additional Data and Analysis on Exposure, Adoption, Usage, and Configuration (RQ1)

Device Exposure

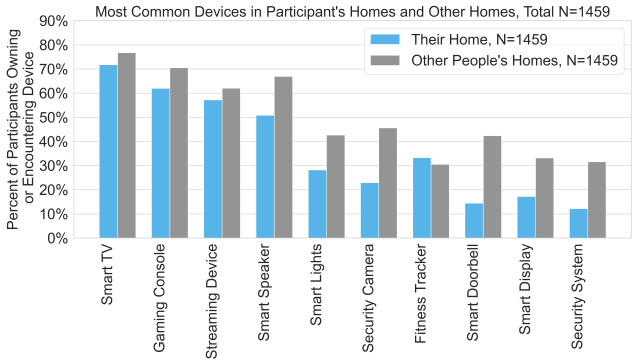

Figure 10: Top ten devices that participants had in their own home and that they encountered in others' homes (top ten for the two contexts combined).

Country	Average Device Types in Own Home	Average Device Types Encountered in Others' Homes
Germany (N=347)	3.8	7.8
Mexico (N=383)	5.1	7.9
UK (N=358)	5.3	6.7
USA (N=371)	5.2	7.3

Table 3: Average number of device types in own home or encountered in others' homes, by country.

Device Adoption

Category	Me	Me with someone else	Someone else in the home	Someone outside the home	Total
Decided to Get					
Female	39%	22%	31%	7%	684
Male	61%	18%	18%	3%	669
Non-binary	38%	25%	34%	3%	32
Less than 25	37%	21%	38%	4%	381
25 to 45	55%	19%	21%	5%	795
45 to 65	54%	22%	16%	8%	184
65 and above	48%	16%	20%	16%	25
Implemented Purchase					
Female	39%	12%	39%	10%	672
Male	63%	9%	23%	5%	670
Non-binary	32%	6%	55%	6%	31
Less than 25	30%	9%	55%	6%	377
25 to 45	57%	11%	24%	8%	791
45 to 65	61%	11%	18%	9%	180
65 and above	63%	17%	4%	17%	24
Owns Device					
Female	44%	25%	28%	2%	682
Male	60%	19%	20%	1%	671
Non-binary	34%	22%	38%	6%	32
Less than 25	41%	19%	39%	1%	380
25 to 45	55%	22%	21%	2%	794
45 to 65	59%	24%	14%	2%	184
65 and above	52%	28%	8%	12%	25

Table 4: Adoption patterns for the Selected Device in the participant's home, by gender and age. ('Other' and 'I don't know' responses not included.)

Decided to Get – Germany ($\chi^2 = 14.1$, $p = 0.00017$, $V = 0.22$*)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	43%	22%	28%	7%	138
Male	67%	18%	13%	2%	162
Non-binary	29%	57%	14%	0%	7
Decided to Get – Mexico ($\chi^2 = 18.5$, $p = 0.00002$, $V = 0.23$ *)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	30%	20%	45%	5%	161
Male	53%	19%	26%	2%	202
Non-binary	31%	15%	46%	8%	13
Decided to Get – UK ($\chi^2 = 5.3$, $p = 0.0211$, $V = 0.13$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	45%	24%	21%	9%	203
Male	64%	16%	13%	6%	140
Non-binary	50%	0%	50%	0%	2
Decided to Get – USA ($\chi^2 = 14.3$, $p = 0.00016$, $V = 0.20$ *)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	39%	20%	32%	8%	182
Male	62%	17%	18%	4%	165
Non-binary	50%	20%	30%	0%	10

Table 5: Involvement in decision to get the Selected Device in participant's home varies by gender in all four countries. ('Other' and 'I don't know' responses not included.)

* Statistical significance and effect sizes are calculated for involvement in decision ("Me" or "Me with someone else") vs. non-involvement ("Someone Else" or "Someone outside the home"), for female vs. male participants.

Implemented Purchase – Germany ($\chi^2 = 11.0, p = 0.00090, V = 0.19$*)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	45%	12%	34%	9%	136
Male	66%	10%	19%	5%	163
Non-binary	43%	14%	43%	0%	7
Implemented Purchase – Mexico ($\chi^2 = 26.6, p < 0.000001, V = 0.27$*)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	22%	10%	60%	9%	161
Male	50%	10%	36%	4%	202
Non-binary	23%	0%	62%	15%	13
Implemented Purchase – UK ($\chi^2 = 9.0, p = 0.00269, V = 0.16$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	47%	16%	24%	14%	197
Male	71%	8%	16%	6%	139
Non-binary	0%	0%	100%	0%	1
Implemented Purchase – USA ($\chi^2 = 25.0, p < 0.000001, V = 0.27$*)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	40%	10%	40%	9%	178
Male	68%	9%	18%	5%	166
Non-binary	40%	10%	50%	0%	10

Table 6: Involvement in implementing the purchase of the Selected Device in participant's home varies by gender in all four countries. ('Other' and 'I don't know' responses not included.)

* Statistical significance and effect sizes are calculated for involvement in purchase ("Me" or "Me with someone else") vs. non-involvement ("Someone Else" or "Someone outside the home"), for female vs. male participants.

Owns Device – Germany ($\chi^2 = 8.4$, $p = 0.00375$, $V = 0.17$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	50%	20%	26%	4%	137
Male	66%	19%	15%	1%	163
Non-binary	29%	29%	43%	0%	7
Owns Device – Mexico ($\chi^2 = 5.2$, $p = 0.0223$, $V = 0.12$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	32%	28%	40%	1%	161
Male	49%	23%	28%	0%	204
Non-binary	31%	23%	38%	8%	13
Owns Device – UK ($\chi^2 = 0.1$, $p = 0.7401$, $V = 0.03$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	50%	31%	16%	3%	202
Male	68%	14%	14%	3%	139
Non-binary	0%	0%	50%	50%	2
Owns Device – USA ($\chi^2 = 7.4$, $p = 0.00638$, $V = 0.15$ – *not statistically significant**)					
	Me	**Me with someone else**	**Someone else in the home**	**Someone outside the home**	**Total**
Female	45%	20%	34%	2%	182
Male	61%	17%	21%	1%	165
Non-binary	50%	20%	30%	0%	10

Table 7: Ownership of the Selected Device in participant's home varies by gender in all four countries. ('Other' and 'I don't know' responses not included.)

* Statistical significance and effect sizes are calculated for ownership ("Me" or "Me with someone else") vs. non-ownership ("Someone Else" or "Someone outside the home"), for female vs. male participants.

Device Usage

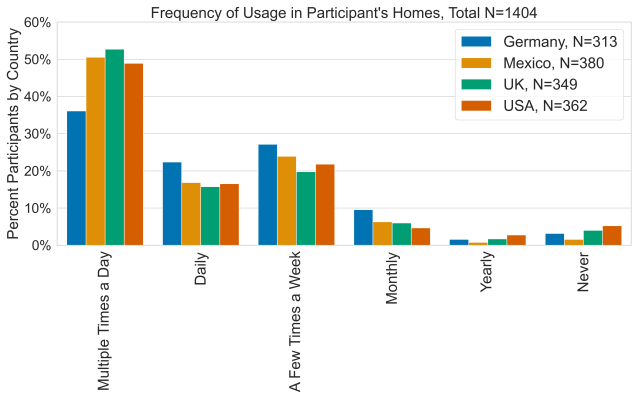

Figure 11: Frequency of use of the Selected Device in their own homes across countries.

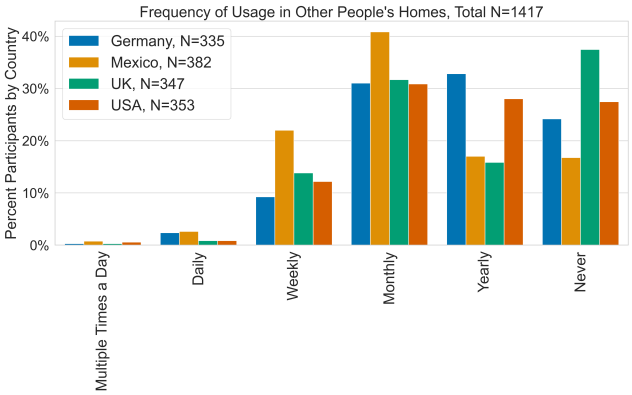

Figure 12: Frequency of use of (any) devices in other people's homes across countries.

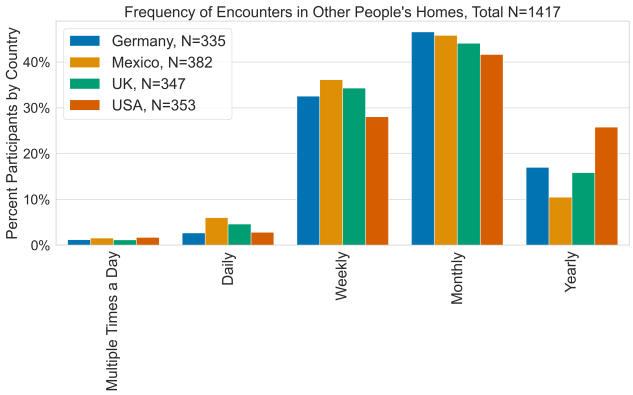

Figure 13: Frequency of encountering (any) devices, without using them, in other people's homes across countries.

Control of Device Configuration and Profiles

	Me and others	Others in the house	I did it	Default settings	Total
Female	14%	31%	50%	2%	679
Male	8%	12%	76%	2%	675
Non-binary	23%	26%	45%	0%	31

Table 8: Involvement in configuring the Selected Device in the participant's own homes, by gender. ('Other' and 'I don't know' responses not included.)

Configuration of Device – Germany ($\chi^2 = 13.9$, $p = 0.00019$, $V = 0.22$*)					
	I did it	**Me and others in the house did it together**	**Others in the house did it**	**Default settings**	**Total**
Female	54%	13%	32%	2%	133
Male	81%	5%	13%	1%	161
Non-binary	43%	29%	29%	0%	7
Configuration of Device – Mexico ($\chi^2 = 15.6$, $p = 0.00008$, $V = 0.21$*)					
	I did it	**Me and others in the house did it together**	**Others in the house did it**	**Default settings**	**Total**
Female	51%	17%	30%	2%	153
Male	70%	14%	12%	3%	202
Non-binary	45%	45%	9%	0%	11
Configuration of Device – UK ($\chi^2 = 14.6$, $p = 0.00013$, $V = 0.21$*)					
	I did it	**Me and others in the house did it together**	**Others in the house did it**	**Default settings**	**Total**
Female	51%	16%	32%	1%	193
Male	82%	4%	13%	1%	137
Non-binary	0%	0%	100%	0%	1
Configuration of Device – USA ($\chi^2 = 26.3$, $p < 0.000001$, $V = 0.28$*)					
	I did it	**Me and others in the house did it together**	**Others in the house did it**	**Default settings**	**Total**
Female	50%	11%	36%	2%	174
Male	79%	8%	12%	1%	165
Non-binary	60%	0%	40%	0%	10

Table 9: Involvement in configuring the Selected Device in the participant's own home varies by gender in all four countries. ('Other' and 'I don't know' responses not included.)

* Statistical significance and effect sizes are calculated for involvement in device configuration ("I did it" or "Me and others did it") vs. non-involvement ("Others did it"), for female vs. male participants.

In Own Home:	**Whether Participant Has an Account/Profile**					**If Yes, What Type**			
	Yes	**No, I share one**	**No, don't have**	**No option**	N	**Admin**	**Regular**	**Guest/temp**	N
Female	51%	38%	9%	2%	605	83%	16%	1%	282
Male	63%	28%	8%	1%	632	89%	10%	1%	387
Non-binary	59%	30%	7%	4%	27	93%	7%	0%	15
Total	*57%*	*33%*	*9%*	*1%*	*1270*	*87%*	*13%*	*1%*	*687*
In Others' Home:	**Whether Participant Has an Account/Profile**					**If Yes, What Type**			
	Yes	**No, I share one**	**No, don't have**	**No option**	N	**Admin**	**Regular**	**Guest/temp**	N
Female	7%	14%	75%	3%	248	59%	35%	6%	17
Male	11%	17%	70%	2%	284	26%	58%	16%	31
Non-binary	8%	25%	67%	0%	12	0%	100%	0%	1
Total	*9%*	*16%*	*72%*	*2%*	*547*	*37%*	*51%*	*12%*	*49*

Table 10: Whether participant has their own individual account or profile on the Selected Device in their own home and (if they use it) on the Selected Device in someone else's home, and if so, what type of account or profile. ('Other' and 'I'm not sure'/'I don't know' responses not included.) Gender has a small effect on whether someone has an account/profile on the Selected Device in their own home ($\chi^2 = 18.0$, $p = 0.0001$, $V = 0.12$ for female vs. male), but not on what type of profile, and no significant effect in others' homes.

Control of Privacy Configuration

	I did, for my account	I did, for everybody	Me and others for everybody	Others in the house for everybody	Default settings	Total
<25	20%	32%	6%	27%	14.5%	359
25-45	20%	44%	6%	17%	12.4%	765
45-65	21%	41%	6%	20%	11.6%	164
65+	10%	43%	19%	14%	14%	21

Table 11: Control over configuring privacy settings in participants' own homes, by age. ('Other' and 'I don't know' responses not included.)

Configuration of Privacy Settings – Germany ($\chi^2 = 12.3$, $p = 0.00047$, $V = 0.22$*)						
	I did for my account	**I did, for everybody**	**Me and others for everybody**	**Others in the house for everybody**	**Default settings**	**Total**
Female	24%	24%	12%	27%	13%	119
Male	27%	50%	3%	11%	10%	157
Non-binary	29%	43%	0%	29%	0%	7
Configuration of Privacy Settings – Mexico ($\chi^2 = 12.4$, $p = 0.00044$, $V = 0.20$*)						
	I did for my account	**I did, for everybody**	**Me and others for everybody**	**Others in the house for everybody**	**Default settings**	**Total**
Female	15%	32%	10%	30%	14%	154
Male	25%	41%	7%	14%	13%	202
Non-binary	9%	27%	27%	27%	9%	11
Configuration of Privacy Settings – UK ($\chi^2 = 26.8$, $p < 0.000001$, $V = 0.31$*)						
	I did for my account	**I did, for everybody**	**Me and others for everybody**	**Others in the house for everybody**	**Default settings**	**Total**
Female	15%	32%	9%	28%	16%	186
Male	22%	58%	3%	6%	11%	132
Non-binary	0%	0%	0%	50%	50%	2
Configuration of Privacy Settings – USA ($\chi^2 = 18.2$, $p = 0.00002$, $V = 0.25$*)						
	I did for my account	**I did, for everybody**	**Me and others for everybody**	**Others in the house for everybody**	**Default settings**	**Total**
Female	16%	34%	8%	30%	13%	166
Male	16%	58%	2%	11%	12%	164
Non-binary	22%	33%	0%	33%	11%	9

Table 12: Involvement in choosing the privacy settings for the Selected Device in the participant's own home varies by gender in all four countries. ('Other' and 'I don't know' responses not included.)

* Statistical significance and effect sizes are calculated for involvement in choosing privacy settings ("I did, for my account", "I did, for everybody" or "Me and others") vs. non-involvement ("Others in the house"), for female vs. male participants.

B Additional Data and Analysis on Concerns, Conflicts, and Privacy Perspectives (RQ2)

Concerns

	In Own Home			In Others' Homes		
Country	**% Concerns**	**% No Concerns**	N	**% Concerns**	**% No Concerns**	N
Germany	49%	48%	(N=291)	36%	62%	(N=308)
Mexico	59%	40%	(N=351)	39%	61%	(N=335)
UK	42%	56%	(N=332)	24%	75%	(N=328)
USA	53%	46%	(N=343)	32%	67%	(N=336)

Table 13: Percentages of participants who mentioned concerns or said they had none, by country.[a]

[a] Percentages do not add up to 100% because some responses were generally usable (i.e. clear and on-topic) but difficult to classify as concerns vs. no concerns, for example those containing hypothetical comparisons, or concerns that did not cause worry.

Comfort

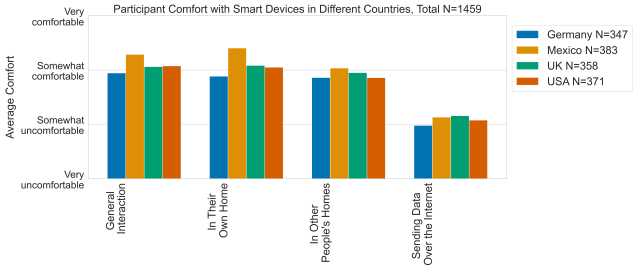

Figure 14: Participants' average level of comfort interacting with smart devices in different contexts, and with their data practices, by country. Participant's comfort with general interaction ($\chi^2 = 25.4$, $p < 0.0001$, $V = 0.13$) and comfort with devices in their own home ($\chi^2 = 42.2$, $p < 0.00001$, $V = 0.17$) varied significantly by country, with a small effect size (responses binarized to comfortable/not comfortable for all statistical tests).

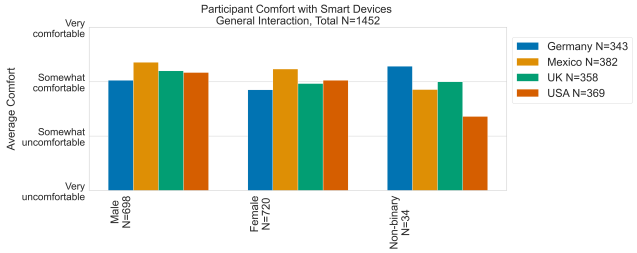

Figure 15: Participants' average level of comfort interacting with smart devices in general, by country and gender. No effects were statistically significant.

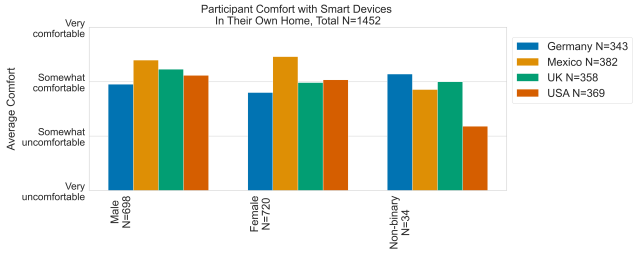

Figure 16: Participants' average level of comfort interacting with smart devices in their own homes, by country and gender. No effects were statistically significant.

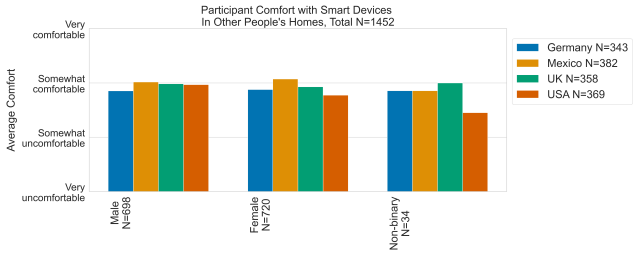

Figure 17: Participants' average level of comfort interacting with smart devices in other people's homes, by country and gender. No effects were statistically significant.

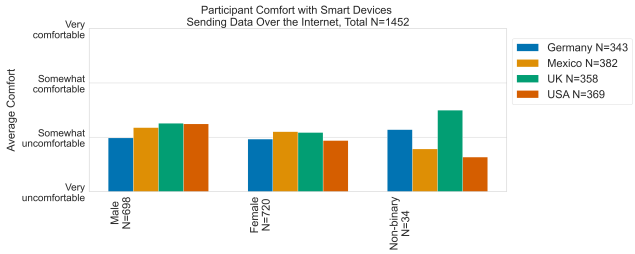

Figure 18: Participants' average level of comfort interacting with smart devices sending data over the internet, by country and gender. No effects were statistically significant.

Privacy Impacts

	In Own Home			In Others' Homes		
Country	**% Impacts**	**% No impact**	N	**% Impacts**	**% No impact**	N
Germany	58%	31%	(N=319)	58%	37%	(N=312)
Mexico	75%	19%	(N=339)	56%	39%	(N=316)
UK	60%	34%	(N=337)	57%	40%	(N=331)
USA	70%	24%	(N=340)	63%	32%	(N=341)

Table 14: Percentages of participants who mentioned privacy impacts or said they did not perceive any, by country.[a]

[a] Percentages do not add up to 100% because some responses were generally usable (i.e. clear and on-topic) but difficult to classify as impacts vs. no impact, for example those containing hypothetical comparisons or dependency factors.

Devices With Highest Privacy Impact

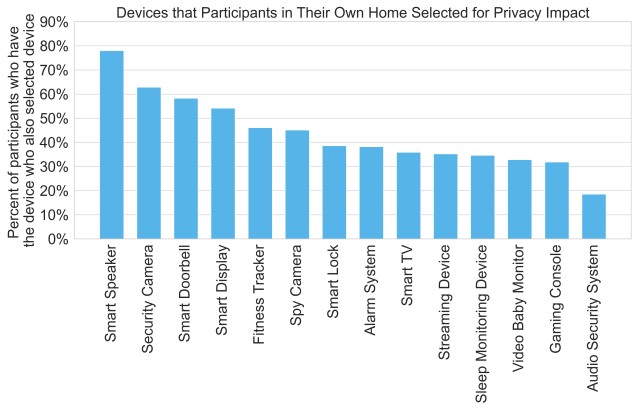

Figure 19: Frequency of participants choosing devices as having the largest impact on their privacy in their own home (up to three choices, all included here).

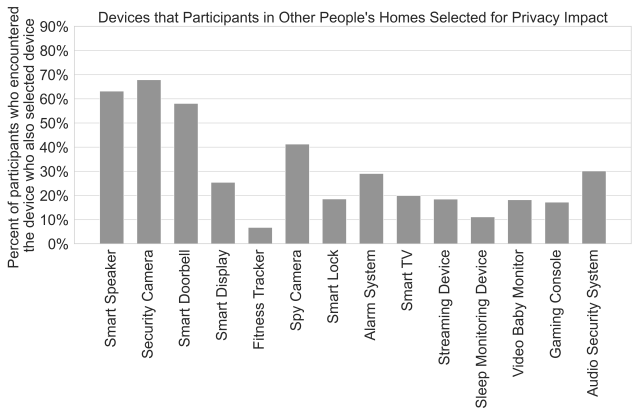

Figure 20: Frequency of participants choosing devices as having the largest impact on their privacy in other people's homes (up to three choices, all included here).

C Additional Data and Analysis on Privacy Protection (RQ3)

Actual Protective Behaviors and Mechanisms

Device	% No Protections in Own Home	% No Protections in Others' Homes
Smart Speaker	50% (N=323)	66% (N=332)
Smart TV	62% (N=177)	67% (N=113)
Streaming Device	49% (N=133)	74% (N=70)
Security Camera	44% (N=96)	62% (N=212)
Smart Doorbell	55% (N=42)	72% (N=160)

Table 15: The percent of participants who said they do not take measures to protect their privacy in each context, for the five most frequently presented Selected Devices.

Device	N	Protection 1	Protection 2	Protection 3
Smart Speaker	162	Power off device	Limit use or info	Settings
Smart TV	68	Limit use or info	Settings	Software & network security
Streaming Device	68	Settings	Limit use or info	Access control
Gaming Console	64	Limit use or info	Settings	Access control
Security Camera	55	Access control	Settings	Choose location

Table 16: Most common privacy-protective behaviors or mechanisms participants used in their own home, for the most common Selected Devices

Device	N	Protection 1	Protection 2	Protection 3
Smart Speaker	115	Change speaking behavior	Limit use or info	Avoid use
Security Camera	81	Avoid devices	Other behavior change	Cover themselves
Smart Doorbell	45	Change speaking behavior	Other behavior change	Avoid devices
Smart TV	37	Limit use or info	Avoid linking accounts	Access control
Gaming Console	36	Access Control	Limit use or info	Avoid linking accounts

Table 17: Most common privacy-protective behaviors or mechanisms participants used in other people's homes, for the most common Selected Devices

Country	% No Protections in Own Home	% No Protections in Others' Homes
Germany	59% (N=282)	71% (N=293)
Mexico	49% (N=348)	64% (N=318)
UK	60% (N=302)	74% (N=305)
USA	45% (N=319)	57% (N=304)

Table 18: The percent of participants who said they do not take measures to protect their privacy around the Selected Devices in each context, by country.

Desired Privacy Options

Device	% No Desired Options in Own Home	% No Desired Options in Others' Homes
Smart Speaker	8% (N=319)	7% (N=335)
Smart TV	8% (N=178)	18% (N=108)
Streaming Device	11% (N=132)	14% (N=67)
Security Camera	15% (N=98)	10% (N=216)
Smart Doorbell	23% (N=48)	16% (N=165)

Table 19: The percent of participants who did not suggest any desired privacy options in each context, for the five most frequently presented Selected Devices.

Device	N	Option 1	Option 2	Option 3
Smart Speaker	295	Data collection & storage control	Data flow & usage control	Disable microphone
Smart TV	164	Data flow & usage control	Restrict activity tracking	Data collection & storage control
Streaming Device	118	Data collection & storage control	Data flow & usage control	Access control
Gaming Console	109	Data flow & usage control	Access control	Data collection & storage control
Fitness Tracker	103	Data flow & usage control	Data collection & storage control	Restrict activity tracking

Table 20: Most common privacy options participants proposed for their own home, for the most common Selected Devices

Device	N	Option 1	Option 2	Option 3
Smart Speaker	316	Data collection & storage control	Disable microphone	Data flow & usage control
Security Camera	199	Data collection & storage control	Access control	Data flow & usage control
Smart Doorbell	142	Data collection & storage control	Access control	Data flow & usage control
Smart TV	92	Data collection & storage control	Data flow & usage control	Restrict activity tracking
Gaming Console	64	Access control	Data collection & storage control	Share accounts

Table 21: Most common privacy options participants proposed for other people's homes, for the most common Selected Devices

Country	% No Desired Options in Own Home	% No Desired Options in Others' Homes
Germany	8% (N=266)	10% (N=284)
Mexico	9% (N=340)	10% (N=326)
UK	15% (N=322)	16% (N=310)
USA	12% (N=324)	15% (N=313)

Table 22: The percent of participants who did not suggest any desired privacy options for the Selected Devices in each context, by country.

D Participant Characteristics

This appendix gives a picture of the demographics and life experiences of participants in our dataset. The full set of questions and answer options can be found within the survey instrument at https://bit.ly/3Vlfn82. This data was also used to support findings about demographic and socioeconomic correlations in Section 4.

Notes, Explanations, and Caveats: Here we provide information pertinent to all or most tables in this appendix. Additional information is provided below each table.

- The row labels in the table below reflect specific answer options offered to participants where feasible, but are abbreviated where answer options were longer or more complex in nature.
- For some questions, participants were invited to check all options that applied; in such cases, breakdowns may not add up to 100%.
- In all cases, breakdowns may not add up to 100% due to rounding.
- For some questions where "Other (please explain)" was offered as an option, we recategorized some of the answers as belonging to existing answer options.
  - For gender, we only recategorized where the self-description was identical to a listed option, as the choice of specific labels has its own significance. (In the similar case of race/ethnicity, no self-descriptions matched the given options.)
  - For the remaining questions, where the choice of label is not especially significant, we recategorized some self-descriptions where they were basically equivalent to or encompassed by one of the given answer options. E.G., for who the participant lives with, we recategorized an answer of "Grandparents" as "Other family member(s)".
- For the remaining questions with an "Other (please explain)" option, if we noticed clusters of similar self-descriptions, we broke these out as a separate line in the tables below. These should not necessarily be taken as truly separate categories; for example, under employment status, a number of people who picked "Other" described themselves as "Self-employed"—but of course, many people who chose given options, e.g. "Full-time employment", may also have been self-employed.
- For the most part, the answer options offered for each question were the same across countries, and translated directly between the two languages. Exceptions are noted in the tables below.
- For most of our questions covered here, we offered a "Prefer not to answer" option; Ns for each question therefore vary, as we dropped those responses from the analysis. (N=1459 for questions answered by everyone.)

Participant Characteristics: Descriptive Statistics

Demographic Characteristics (Part 1)	**Total**	Germany	Mexico	UK	USA
Age*	*(N=1459)*	*(N=347)*	*(N=383)*	*(N=358)*	*(N=371)*
Median	30 y.o.	28 y.o.	25 y.o.	36 y.o.	31 y.o.
Range	18–79 y.o.	18–71 y.o.	19–68 y.o.	18–79 y.o.	18–79 y.o.
Gender[a]	*(N=1454)*	*(N=344)*	*(N=383)*	*(N=358)*	*(N=369)*
Female	50%	46%	42%	60%	51%
Male	48%	52%	54%	40%	46%
Non-binary	2%	2%	4%	1%	3%
Other descriptions	< 0.5%	< 0.5%	< 0.5%	0%	0%
Household Income Quintile[b]	*(N=1326)*	*(N=306)*	*(N=332)*	*(N=340)*	*(N=348)*
Lowest	14%	24%	16%	9%	9%
Second	17%	19%	24%	9%	16%
Third	17%	13%	19%	16%	18%
Fourth	23%	19%	27%	22%	23%
Highest	29%	25%	14%	44%	33%
Educational Attainment‡◊	*(N=1452)*	*(N=345)*	*(N=382)*	*(N=358)*	*(N=367)*
Middle school/junior high (level 1) or less	-	< 0.5%	< 0.5%	1%	1%
Comprehensive secondary (grade 10; level 2)	-	8%	-	16%	-
High school (4yr); sixth form/trade school	-	35%	29%	28%	34%
Community/technical college (2yr); Associates	-	-	5%	-	20%
University (4yr); Bachelor/professional degree	-	32%	58%	36%	31%
(Post)Graduate school; Masters	-	22%	7%	17%	10%
Doctorate or higher	-	4%	1%	3%	3%
Other: Some college	-	0%	0%	0%	2%
Employment Status‡◊[c]	*(N=1435)*	*(N=347)*	*(N=375)*	*(N=356)*	*(N=359)*
Full-time employment	44%	41%	39%	55%	39%
Full-time student	13%	22%	17%	3%	9%
Part-time employment, part-time student	11%	17%	17%	5%	6%
Part-time employment (only)	13%	10%	9%	16%	15%
Not employed, but seeking work	9%	4%	13%	5%	14%
Not employed; not seeking work	8%	3%	2%	14%	13%
Other: Self-employed/freelance	1%	2%	< 0.5%	1%	2%
Other: Full-time student, also employed	1%	1%	< 0.5%	0%	1%
Other descriptions	1%	1%	2%	1%	1%

Table 23: Selected demographic characteristics of survey participants. Except where noted, data are from questions asked in our survey.

Notes:
* Data from Prolific (not part of our exit survey).
‡ Participants' self-descriptions under "Other (please explain)" may have been recategorized if they were similar to a given answer choice, or a recognizable subcategory thereof.
◊ Participants' self-descriptions under "Other (please explain)" are broken out according to clusters of common answers.
[a] One participant's self-description under "Other (please explain)" was recategorized as it was identical to one of the given answer choices.
[b] Answer options for income differed by country. For each, we presented income ranges based on household income decile thresholds from the World Inequality Database [146] (combined into quintiles).
[c] Options for educational attainment followed the structures of the education system in each country, which are quite different between Europe and North America. The row labels here do not reflect the full descriptions that were given for each country.
In addition, unlike other questions, answer options differed between languages. For example, for the Spanish version distributed in the U.S., we included approximate equivalents from both the U.S. and Mexican education systems within each option, on the logic that a Spanish speaker in the U.S. might likely have been educated in either place—but for the U.S. English version, we referenced only the U.S. system.

Demographic Characteristics (Part 2)[a]			
Ethnicity/Race—Germany[†◊] *(N=339)*		**Ethnicity/Race—Mexico**[†◊c] *(N=361)*	
Arab, Middle Eastern, North African	4%	Asian, Pacific Islander (including Native Hawaiian)	0%
Asian	6%	Black, Afro-Mexican, African descent	3%
Black	1%	Indigenous (including Alaska Native)	3%
Pacific Islander (including Native Hawaiian)	0%	White, European descent	21%
Romani/Traveller	0%	Other: Latino(a), Hispanic, Mexican, Mestizo(a)[d]	76%
White	87%	Other: Arab	< 0.5%
Other: Latin(o)(a), Hispanic	3%	Other descriptions	1%
Other: Mestizo(e)[b]	1%		
Other: Details of other mixed ethnicity/race	1%		
Other descriptions	2%		
Ethnicity/Race—UK[†◊] *(N=356)*		**Ethnicity/Race—USA**[†◊] *(N=369)*	
Arab, Middle Eastern, North African	1%	Asian, Asian-American	12%
Asian, Asian British	4%	Black, African-American	10%
Black, Black British, Caribbean, African	7%	Hispanic/Latino/Latinx	20%
White	87%	Middle Eastern, North African	< 0.5%
Other: Latino(a)	1%	Native American, Alaska Native	3%
Other: Mixed (no further details)	< 0.5%	Pacific Islander (including Native Hawaiian)	1%
Other: Details of other mixed ethnicity/race	1%	White	65%
		Other: Romani	< 0.5%
		Other: Multiracial/mixed (no further details)	1%
		Other: Details of other mixed ethnicity/race	< 0.5%

Table 24: Ethnicity and/or race of survey participants. Data is from a question asked in our survey, which differed by country.

Notes:
† Participants were invited to check all options that applied.
◊ Participants' self-descriptions under "Other (please explain)" are broken out according to clusters of common answers.
[a] Options given for ethnicity or race were different between countries, as ideas about the relevant categories and what they mean vary greatly. For the UK, we used categories the UK national censuses. For the U.S., we used census categories with a couple of additions commonly broken out in survey research; we did similarly for Mexico, with nuances noted below. As Germany does not include ethnicity in any national census, we used categories gleaned from survey research.
[b] As participants describing themselves as "Mestizo" in Germany were born in a variety of countries with different ideas about ethnic labels, we did not view it as appropriate to combine it with "Latino" in this case. (Unlike with Mexico; see below.)
[c] The Mexican census intentionally only asks whether someone is a member of certain minority ethnic groups, with the intent of blurring racial, ethnic, or regional differences amongst the majority of the population, in favor of a unified Mexican identity. However, there is no agreed-upon term to cover this concept; terms like *Latino* and *Hispanico* are primarily used outside Mexico, and *Mexicano* is ambiguous in scope. We therefore left the matter open to self-description for those who did not fit into the limited categories we offered.
[d] This group combines answers including (in order of frequency): Latino/Latina, Hispano/Hispana, Mexicano/Mexicana/Mexican, Mestizo, Hispanic/Hispanico, Latinoamericano/Latina americana, Latin, Mixto, Latinx, or combinations of those terms. We consider these answers together as they all may be used to express a similar concept of broadly Mexican or Latin American identity. (We assume the prevalence of terms like *Latino* and *Hispanic* is due to Prolific participants' being accustomed to seeing them in surveys.)

Demographic Characteristics (Part 3)	**Total**	Germany	Mexico	UK	USA
Type of Locality	*(N=1448)*	*(N=342)*	*(N=382)*	*(N=356)*	*(N=368)*
Rural	12%	14%	2%	14%	18%
Suburban	38%	29%	19%	55%	51%
Urban	50%	57%	79%	31%	30%
Other descriptions	< 0.5%	0%	0%	1%	0%
Immigration Status[*a]	*(N=1459)*	*(N=347)*	*(N=383)*	*(N=358)*	*(N=371)*
Born in current country of residence	88%	78%	98%	85%	90%
Not born in current country of residence	12%	22%	2%	15%	10%
First Language[*b]					
Out of those who took survey in English:	*(N=990)*	*(N=320)*	*(N=22)*	*(N=333)*	*(N=315)*
English	62%	1%	0%	95%	93%
German	27%	83%	0%	1%	0%
Spanish	3%	1%	100%	< 0.5%	3%
Other	8%	16%	0%	4%	4%
Out of those who took survey in Spanish:	*(N=463)*	*(N=26)*	*(N=358)*	*(N=24)*	*(N=55)*
English	9%	0%	1%	50%	49%
German	2%	27%	0%	0%	0%
Spanish	87%	62%	99%	33%	49%
Other	2%	12%	< 0.5%	17%	2%

Table 25: Selected demographic characteristics of survey participants. Except where noted, data are from questions asked in our survey.

Notes:
* Data from Prolific (not part of our exit survey).
[a] Immigration status was inferred by comparing Prolific data on participants' country of residence and country of birth.
[b] Language data does not include 6 participants who took the Spanish version of the survey but responded to free-answer questions in English.

Personal and Work Situations	**Total**	Germany	Mexico	UK	USA
Housing Situation[‡◊]	*(N=1438)*	*(N=344)*	*(N=380)*	*(N=350)*	*(N=364)*
Owns their home	33%	16%	29%	55%	32%
Rents from someone who also lives there	7%	11%	5%	4%	10%
Rents from someone who doesn't live there	32%	55%	17%	32%	28%
Lives with someone without paying rent	24%	14%	46%	7%	28%
Lives in hotel/Airbnb/other temporary housing	< 0.5%	0%	< 0.5%	0%	1%
Lives in dorm/long-term care/institutional housing	2%	4%	1%	1%	1%
Other: Living with parents/family	1%	< 0.5%	2%	1%	< 0.5%
Other descriptions	1%	1%	1%	0%	< 0.5%
Who Participant Lives With[†‡◊]	*(N=1436)*	*(N=338)*	*(N=380)*	*(N=355)*	*(N=363)*
Spouse(s)/partner(s)	40%	40%	23%	61%	39%
Friend(s)	7%	13%	5%	6%	6%
Child(ren)	22%	10%	17%	42%	19%
Parent(s)	33%	20%	60%	13%	34%
Sibling(s)	16%	7%	36%	3%	15%
Other family member(s)	6%	4%	9%	2%	9%
Lives alone	14%	24%	5%	12%	17%
Other: Housemate(s)/flatmate(s)/roommate(s)	2%	2%	0%	1%	0%
Other descriptions	< 0.5%	< 0.5%	< 0.5%	1%	< 0.5%
Experiences with Visitors to Home—Past 2 Yrs[†]	*(N=1459)*	*(N=347)*	*(N=383)*	*(N=358)*	*(N=371)*
Had someone they know visit (not overnight)	90%	92%	89%	92%	86%
Had someone visit and stay overnight	63%	74%	63%	60%	56%
Held a group meeting/event inside their home	40%	42%	66%	25%	24%
Had someone working inside their home	41%	41%	35%	45%	42%
Had someone working outside close to the home	27%	22%	22%	26%	37%
Experiences Visiting Others' Homes—Past 2 Yrs[†]	*(N=1459)*	*(N=347)*	*(N=383)*	*(N=358)*	*(N=371)*
Visited someone they know (not overnight)	93%	96%	91%	94%	91%
Stayed overnight in someone's home	71%	87%	73%	65%	59%
Attended a group meeting/event at someone's home	61%	70%	85%	42%	48%
Been inside someone's home for work	22%	31%	25%	16%	17%
Worked outside close to someone's home	13%	15%	14%	7%	16%

Table 26: Selected aspects of survey participants' housing, personal, and work situations. Data are from questions asked in our survey.

Notes:
[†] Participants were invited to check all options that applied.
[‡] Participants' self-descriptions under "Other (please explain)" may have been recategorized if they were similar to a given answer choice, or a recognizable subcategory thereof.
[◊] Participants' self-descriptions under "Other (please explain)" are broken out according to clusters of common answers.

Technology Experience	**Total**	Germany	Mexico	UK	USA
Technology Background					
Has educational background in CS, CE, or IT *(N=1403)*	21%	27%	22%	15%	19%
Has worked in CS, CE, or IT *(N=1420)*	20%	28%	19%	15%	18%
Has written a computer program *(N=1452)*	27%	35%	32%	16%	25%
Has ≥ 1 digital security requirement at work *(N=1073)*[a]	72%	73%	70%	77%	66%
Has ≥ 3 digital security requirements at work *(N=1073)*[a]	20%	25%	19%	20%	16%
Frequency of Being Asked for Help with Technology	*(N=1459)*				
Rarely	26%	24%	20%	36%	25%
Sometimes	50%	53%	52%	48%	49%
Frequently	24%	24%	27%	16%	27%

Table 27: Selected aspects of survey participants' technology experience. Data are from questions asked in our survey. Most questions borrowed with modifications from Tan et al. 2017 [128], except digital security requirements at work borrowed with modifications from Abu-Salma and Livshits 2020 [3].

Notes:
[a] The question about digital requirements at work did not ask for a number. Rather, it offered five options plus "Other (please explain)", and we counted how many each person checked.
We also offered an option for "not currently working"; the N for digital security requirements questions includes only participants who are currently working.

E Codes for Qualitative Analysis of Free-Answer Questions

This appendix lists the codes used for thematic analysis of free-answer data. A full codebook with coding rubrics can be found at https://bit.ly/3Vlfn82

Concerns

Questions coded:

- In participants' own homes: "Have you ever had any concerns regarding IoT devices in your home? If so, what device(s) and why?" / «¿Alguna vez ha tenido alguna inquietud con respecto a los dispositivos IoT en su hogar? Si es así, ¿con qué aparato y por qué?» *(Asked all participants.)*
- In other people's homes: "Have you ever had any concerns regarding IoT devices in other people's homes? If so, what device(s) and why?" / «¿Alguna vez ha tenido alguna inquietud con respecto a los dispositivos IoT en los hogares de otras personas? Si es así, ¿con qué aparato y por qué?» *(Asked participants who had encountered devices in others' homes.)*

Types or causes of concern:[15]

- Access control
- Audio
- Child use/exposure
- Data collection/storage
- Data use/misuse
- Elder use
- Energy use
- Functionality
- Hacking
- High cost
- Information sharing
- Listening to/recording conversations
- Network connection
- No control in others' homes *[used only for others' homes]*
- Power imbalance
- Privacy
- Security
- Surveillance by user
- Surveillance/monitoring (general)
- Tracking
- Usability
- Video

Other/meta:

- Other concerns
- No concerns
- Off topic/unclear

Privacy Impacts

Questions coded:[16]

- In participants' own homes: "What is the impact of IoT devices in your home on your privacy? " / «¿Cuál es el impacto de los dispositivos IoT en su hogar en su privacidad?» *(Asked all participants.)*
- In other people's homes: "What is the impact of IoT devices in other people's homes on your privacy?" / «¿Cuál es el impacto de los dispositivos IoT en los hogares de otros en su privacidad?» *(Asked all participants.)*

Degree of privacy impact:

- Large privacy impact
- Small privacy impact
- No impact

Factors that affect degree of impact:

- Being careful/self aware*
- Configuration dependent
- Nothing to hide
- Usage/device dependent

Polarity of privacy impact:

- Negative privacy/security impact
- Positive privacy/security impact

Sources of privacy impact (how devices cause impact):

- Audio
- Consent/disclosure/privacy rights*
- Data collection/storage
- Data use or sharing
- Hacking/security
- Listening to/recording conversations
- Location privacy*
- No control in others' homes *[used only for others' homes]*
- Surveillance by user
- Surveillance/monitoring/tracking (general)*
- Video

Effects of privacy impact (what kinds of impacts are enabled/allowed):

- Being careful/self aware*
- Consent/disclosure/privacy rights*
- Corporate control/monetization
- Location privacy*
- Normalization/resignation
- Safety under threat
- Surveillance/monitoring/tracking (general)*

Other/meta:

- Other impacts
- Uncertain or unconcerned
- Off topic/unclear

Actual Protective Behaviors and Mechanisms

Questions coded:

- In participants' own homes: "How do you protect your privacy around the *<insert Selected Device>* in your home? Are there specific actions you take or strategies you use?" / «¿Cómo protege su privacidad en torno a *<insert Selected Device>* en su hogar? ¿Hay acciones específicas que toma o estrategias que usa?» *(Asked participants who had devices in their homes.)*

[15] Groupings are post hoc, to provide structure to the findings. They were not part of the coding process, and are not intended as an analysis of, e.g., how people think about privacy impact.

* indicates code could be viewed as belonging to multiple groups.

[16] We did not provide a definition of "privacy" anywhere in the survey, but rather left it open to participants' interpretations.

- In other people's homes: "How do you protect your privacy around the *<insert Selected Device>* in someone else's home? Are there specific actions you take or strategies you use?" / «¿Cómo protege su privacidad en torno a *<insert Selected Device>* en la casa de otra persona? ¿Hay acciones específicas que toma o estrategias que usa?» *(Asked participants who had encountered devices in others' homes.)*

Technical protections:

- Access control
- Cover or disable sensor
- Power off device
- Settings
- Software and network security

Behavioral strategies:

- Alternative information
- Ask owner for info/protections
- Avoid devices
- Avoid linking accounts
- Avoid use
- Change speaking behavior
- Choose location of device
- Cover themselves
- Educate self or others
- Find devices
- Limit time in home
- Limit use or info given
- Other behavior change

Other/meta:

- Other protections
- None
- Uncertain/off topic/unclear

Desired Privacy Options

Questions coded:

- In participants' own homes: "If you could have any privacy options that you can imagine, what privacy settings would you pick for the *<insert Selected Device>* in your home?" / «Si pudiera tener cualquier opción de privacidad que pueda imaginar, ¿qué configuración de privacidad elegiría para *<insert Selected Device>* en su hogar?» *(Asked participants who had devices in their homes.)*
- In other people's homes: "If you could have any privacy options that you can imagine, what privacy settings would you pick for the *<insert Selected Device>* in someone else's home?" / «Si pudiera tener cualquier opción de privacidad que pueda imaginar, ¿qué configuración de privacidad elegiría para *<insert Selected Device>* en la casa de otra persona?» *(Asked participants who had encountered devices in others' homes.)*

Types of privacy settings or controls:

- Access control
- Activation control
- Consent
- Content control
- Control automatic recognition
- Data collection/storage control
- Data flow/usage control
- Disable camera/video
- Disable microphone/listening
- Network control
- Power off
- Private browsing
- Restrict activity tracking
- Share accounts/multiple profiles
- Spatial constraints
- Use indicator

Other/meta:

- Other options
- Something stricter (vague)
- None
- Their home their choice *[used only for others' homes]*
- Uncertain or unconcerned
- Off topic/unclear