The Skewed Privacy Concerns of Bystanders in Smart Environments

MAXIMILIANE WINDL, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany

Fig. 1. Two interactions between the device owner and a bystander as shown in the survey; a) features a smart home device, i.e., a smart display, b) shows a personal computing device, i.e., a smartphone.

As ubiquitous computing brings sensors and actuators directly into our homes, they introduce privacy concerns for the owners and bystanders. However, privacy concerns may vary among devices and depend on the bystanders' social relation to the owner. In this work, we hypothesize 1) that bystanders assign more privacy concerns to smart home devices than personal computing devices, such as smartphones, even though they have the same capabilities, and 2) that a stronger social relationship mitigates some of the bystanders' privacy concerns. By conducting an online survey (n=170), we found that personal computing devices are perceived as significantly less privacy-concerning than smart home devices while having equal capabilities. By varying the assumed social relationship, we further found that a stronger connection to the owner reduces privacy concerns. Thus, as bystanders underestimate the risk of personal computing devices and are generally concerned about smart home devices, it is essential to alert the user about the presence of both. We argue that bystanders have to be informed about the privacy risks while entering a new space, in the best case, already in the entrance area.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**.

Additional Key Words and Phrases: privacy, smart home, bystanders

ACM Reference Format:
Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (September 2022), 21 pages. https://doi.org/10.1145/3546719

Authors' addresses: Maximiliane Windl, LMU Munich, Munich, 80337, Germany, maximiliane.windl@ifi.lmu.de; Sven Mayer, LMU Munich, Munich, 80337, Germany, info@sven-mayer.com.

2573-0142/2022/9-ART184 $15.00
https://doi.org/10.1145/3546719

1 INTRODUCTION

Smart homes promise great convenience, as they automatically adjust the temperature, control lights, or allow receiving answers to questions just by saying them out loud. To provide such functionalities, smart home devices are equipped with various sensors and processing power of sensitive data. Yet, not only homes are getting smarter with the integration of sensors, voice assistants, and cameras. But also personal computing devices, such as smartphones, laptops, or smartwatches, have the same capabilities [9, 16, 31]. While such devices offer great convenience, they also pose privacy threats, such as detecting sleeping or eating patterns [33], disclosing pin codes [32], or gaining remote control [11]. As even smart home device owners have remaining privacy concerns [24], offering a safe space for bystanders (people merely using the space) is crucial.

In the context of smart homes, research has paid special attention to the privacy of bystanders [1, 29, 42]. In this work, we define the term bystander as people who are neither the owners nor the primary users of a device but are nevertheless exposed to it. In the context of smart home devices, this could, for instance, be guests in a hotel or visitors in private homes. In the context of personal computing devices, this could be a person standing next to someone using their smartphone. Often, bystanders can not choose but are implicitly forced to engage with technology, such as when they visit someone that has smart appliances. Moreover, bystanders do not have the same rights as the device owners, such as turning off devices, removing them, or reviewing and deleting data. They also face strong contextual variations as their role changes depending on their social relationship with the device owner [42]. Therefore, the privacy of bystanders deserves special attention. Moreover, research about privacy concerns towards smart personal computing devices has not experienced the same uptake as research about smart home devices, even though those are equipped with similar sensors and capabilities and thus, pose equal threats to the user's privacy. Interestingly, there seems to be an illogical discrepancy between the perception of smart home devices and personal computing devices. When entering a private space with a smart home device, we often see people getting nervous about the device's presence or even expressing wishes to unplug or deactivate it. In contrast, people only very seldomly report privacy concerns when a person in their vicinity uses their smartphone or smartwatch – even though both are equipped with the same capability: a voice assistant.

Our paper aims to fill this gap in the literature by investigating how privacy concerns of bystanders are affected by the type of device. Here, we investigate personal computing devices (e.g., smartphones) and smart home devices (e.g., smart displays) as they offer the same capabilities in different form factors. In detail, we survey 10 different devices (five from each group). Moreover, since Yao et al. [42] suggested that the social relationship with the owner impacts the privacy concern, we also study five different relationships (family member, friend, colleague, homestay, and hotel as device owner). We conducted an online survey with 170 participants to understand both impact factors.

Our survey results show that bystanders generally have privacy concerns with all types of devices, especially when equipped with cameras and microphones. Further, we could also quantify the subjective perception that bystanders have significantly stronger privacy concerns in the vicinity of smart home devices than personal computing devices, highlighting the skewed perception of privacy. Finally, we show that privacy concerns are affected by social relationships. The general trend is that privacy concerns increase with a lower social relationship. As such, both designers and owners of advanced tracking and processing capabilities need to take care of the owner's privacy and the people in the vicinity of the devices. We summarize that alerting bystanders about smart home devices is similarly important to alerting and educating them about personal computing devices before coming into contact.

2 RELATED WORK

In the following, we first describe why privacy is an important factor to consider in smart home environments and when interacting with personal computing devices. We then explain the special role of bystanders and why their privacy deserves special recognition.

2.1 Privacy Concerns Smart Home Devices

Previous work argued that smart homes require special attention since here, data gets collected in the most intimate spaces, and thus, privacy is subject to societal and legal expectations [5, 25, 45]. Indeed, research has already revealed how data collected from smart homes can be used to reveal identities or retrace user behaviors [3, 35]. For example, Molina-Markham et al. [33] showed how data from smart meters can be used to infer the number of people in a household, their sleeping patterns, or their eating routines. In the context of video surveillance systems, Obermaier and Hutle [35] showed how vulnerabilities can be exploited to blackmail users by denial of service attacks, injecting forged video streams, or gaining access to private video data. By analyzing the encrypted network traffic from four different smart home devices, Apthorpe et al. [3] revealed potentially sensitive user interactions. They showed how the traffic from smart sleep monitors correlated with the times the user was asleep.

Yet, research found that users are often unaware of the possible dangers and vulnerabilities caused by smart home appliances [15]. For example, Malkin et al. [27] found that users are uncertain about the kinds of data collected and used when interacting with SmartTVs. Similarly, in the context of smart speakers, Malkin et al. [28] found that just about half of the 116 people surveyed were aware that their data gets permanently stored, and only very few users reported having ever deleted information. In addition, while many users reported being concerned about data collected by microphones or cameras, users were skeptical about privacy threats of smart home devices without these capabilities [6, 8, 45].

Even though users are often uncertain about the specific kinds of data collected, many still feel uneasy when in the vicinity of smart home devices and can name specific concerns when explicitly asked. For example, Barbosa et al. [5] found that users would mostly deny information flows that allow inferring demographics such as age or gender or allow monitoring communications or habits and lifestyles. Not surprisingly, they were most comfortable with information flows needed for the primary intended purpose of the smart home device. By surveying IoT adopters and non-adopters, Lafontaine et al. [24] found that both groups share similar concerns, primarily that the device might transmit additional data without consent or that there might be security loopholes. Current non-adopters of smart speakers named privacy concerns among the main reasons for not adopting the devices [25]. Specifically, they reported being concerned about the speakers always listening, targeted advertising, and third-party sharing. Besides, they mentioned explicit distrust in the manufacturers. Interestingly, this is in direct contrast to the users of smart devices, whose trust in the manufacturers is one of the main reasons for not having privacy concerns [25, 41, 45].

2.2 Privacy Concerns Personal Computing Devices

Mobile devices are equipped with various sensors that enable a multitude of interactions by inferring aspects of the context of use [31]. Wearable technologies, for example, continuously collect geolocation, habits, activities, and physical and emotional states [16]. Albeit the comfort and functionalities these sensors promise, they also expose users to privacy risks since they can potentially deduce sensitive information [16]. Yet, in the context of smartwatches, users expressed little to no privacy concerns [38]. When asked, they mentioned not believing to fall victim to a privacy attack. The reasons are that many users are unaware of the privacy risks associated with

mobile sensors or that they are generally unfamiliar with the various types of sensors [22, 32]. In fact, the less familiar participants are with a sensor the less risk they associate with it [32]. Nevertheless, such attacks are possible and not unlikely. For example, Mehrnezhad et al. [32] showed how users' PIN codes can be inferred using JavaScript and the mobile and motion sensors of smartphones without requiring any further permissions. In the context of motion sensors, Kirsten Crager [22] found that most users were unaware of privacy threats related to those sensors, except for location tracking. However, by confronting users with videos of attacks that exploited the capabilities of motion sensors, they also showed that users could be educated about privacy threats since they expressed genuine concerns afterward.

Another possible source of privacy concerns are voice assistants that increasingly get integrated into personal computing devices, such as smartphones, smartwatches, and laptops. In the context of smartphones, research has already shown how voice assistants can be exploited for attacks through the phone speaker without requiring any permission from the system. By playing prepared audio files, the malware can forge emails and SMS, transmit sensitive data and gain remote control of smartphones [11]. Cowan et al. [9] showed how infrequent users of voice assistants have privacy concerns regarding the purpose of data collection and storage. They suspected the data to be collected and monetized. Participants also expressed being more concerned about interpersonal data than, e.g., banking or health information.

2.3 Privacy Concerns of Bystanders

Bystanders often can not consciously decide to interact with a smart device but are implicitly forced to do so when visiting someone else's home. For example, if said home is equipped with smart lights or a smart doorbell. Additionally, since guests are not the primary users, they often have to interact with the technology without having the possibility to engage with its privacy policy beforehand [25]. Another factor that makes bystanders unique is their potential to switch social roles in different situations, for example, when visiting a friend versus when being a guest in a holiday home [42]. Yao et al. [42] were the first to explicitly investigate the privacy perceptions of bystanders in smart homes. Though bystanders recognized the benefits of adopting smart home devices, they also expressed several concerns. They were most concerned with temporary resident and playdate scenarios and data captured by microphones and videos. Bystanders also reported ways to mitigate their privacy concerns, including covering security cameras or moving devices to less privacy-sensitive rooms, such as the kitchen. Mare et al. [29] investigated the privacy concerns of guests in Airbnb rentals. They found that guests were most concerned about hosts spying on them, experiencing discrimination based on their behavior that might be captured by the smart devices, and being exposed to security risks as hosts might not take sufficient security measures. Finally, participants also mentioned mistrusting the manufacturers of smart devices. Ahmad et al. [1] argue that tangible privacy mechanisms are needed for bystanders to successfully assess the state (i.e., if a device is off or on) and associated privacy risks of smart devices.

The privacy of bystanders has also been studied in other contexts outside of smart homes. Denning et al. [10] found that bystanders assumed augmented reality glasses were capable of recording, and thus, reacted negatively when being exposed to these devices and expected to be asked for consent. In the context of lifelogging cameras, users reported being concerned about the privacy of bystanders and chose to discard or not share the captured footage [19, 20]. Wang et al. [39] investigated bystanders' concerns towards drones and found that they were concerned about stalking and being surveilled. Yao et al. [43] additionally found that bystanders were concerned about their faces being recognized in drone footage.

3 HYPOTHESES

We aim to quantify the discrepancy in **bystanders' perception of smart home devices compared to personal computing devices**. While bystanders' privacy in smart homes has become prevalent in recent research [1, 29, 42], we do not see equal development concerning personal computing devices. This is intriguing since they share equal capabilities and thus pose similar threats to the users' privacy [11, 16, 22, 31, 32]. Thus, our paper investigates the privacy concerns of bystanders towards personal computing devices and smart home devices. We approach this through five hypotheses:

H1 Prior work found that privacy concerns vary depending on the device. For example, devices with microphones and cameras were generally perceived as more concerning [6, 8, 45], while participants reported very few concerns about smartwatches [38]. Therefore, we set Hypothesis 1 (**H1**): **Different devices pose different privacy concerns.**

H2 Even though users are often uncertain about the specific risks [15, 27, 28, 45], many still feel uneasy when in the vicinity of smart devices [5, 24, 25]. Especially, current non-adopters named privacy concerns as the main reason for not engaging with the technology [25]. We find that the privacy of bystanders has been investigated in several contexts as research recognizes their unique role of often being unwillingly exposed to technology [25]. However, while bystanders' privacy in smart homes has become prevalent in recent research [1, 29, 42], their privacy perceptions of personal computing devices have been neglected. Indeed, research even found that people do not associate privacy concerns with those devices [38], even though they share equal capabilities and thus, pose similar threats to bystanders' privacy [11, 16, 22, 31, 32]. Therefore, we hypothesize that users are less privacy-aware of risks associated with personal computing devices than they are in smart home environments. Thus, we set Hypothesis 2a (**H2a**): **Bystanders perceive smart home devices as generally more privacy-concerning than personal computing devices.**

Even though users are often uncertain about the specific kinds of data collected, they are still able to report concrete concerns when asked explicitly about them [5]. We hypothesize that not only the general concern but also the specific concerns are skewed towards smart home devices. Thus, we set Hypothesis 2b (**H2b**): **Bystanders perceive smart home devices as more privacy-concerning in terms of data access, data processing, data storage, profile building, and data theft than personal computing devices.**

H3 Findings by Yao et al. [42] suggest that "bystanders face strong contextual variations" due to factors such as length of stay and "perceived social relationships with the owners." Thus, we want to understand the impact of the relationship in this first investigation. As stronger social relationships come with a stronger familiarity and trust in the person, we hypothesize that bystanders will associate fewer privacy concerns with a device owned by a family member than with one owned by a stranger. Accordingly, we set our Hypothesis 3 (**H3**): **A stronger social relationship with a device owner reduces privacy concerns.**

H4 Naeini et al. [34] showed that the location influenced participants' level of comfort in the sense that they were more uncomfortable with data being recorded in private spaces. In this regard, Yao et al. [42] found that bystanders felt least comfortable with smart home devices being placed in the bedroom or living room. Motivated by this, we hypothesize that our participants' perceptions differ depending on different locations. Thus, we set Hypothesis 4 (**H4**): **Bystanders' privacy concerns increase the more intimate the usage location is.**

H5 Apthorpe et al. [4] found that owning a smart home device increased participants' acceptance. Therefore, we assume that participants relate fewer privacy concerns to devices they possess. Consequently, we set our Hypothesis 5 (**H5**): **Ownership reduces privacy concerns.**

Fig. 2. All ten Devices as presented in the survey. Pictures a to e show the smart home devices. Specifically, these are a) a smart display, b) a smart speaker, c) a smart doorbell, d) a smart security camera, and e) smart lights. Pictures f to j show the personal computing devices. Those were: f) a laptop, g) a smartwatch, h) a personal computer, i) a smartphone, and j) a tablet.

4 SURVEY

Framed by our five hypotheses, we wanted to investigate whether bystanders perceive smart home devices as more privacy-concerning than personal computing devices and whether their concern is affected by the type of computing device and the relation to the device owner. Therefore, we conducted an online survey on Prolific and our university to reach a comprehensive and diverse sample. We wanted to clarify the devices' capabilities and make the situations feel more realistic and graspable by using videos to showcase interactions with five personal computing devices and five smart home devices. We used an iterative process to create the questions for the survey: We first generated an initial set of questions, conducted a pilot study with colleagues, conducted a second pilot study with 10 participants from Prolific, and used these insights to build the final survey and resolve ambiguities.

This resulted in a questionnaire containing four main blocks: 1) demographic questions, 2) general questions about the participants' privacy perception and affinity for technology using the IUIPC questionnaire [26] and the ATI scale [12], 3) for each device: how familiar participants were with the device, whether they owned such a device, whether they perceived the device as privacy-concerning and which specific concerns they had with the device, and 4) final questions about the influence of specific sensors and locations on their privacy concerns. We provide the complete questionnaire in the Appendix A.

All participants rated all ten Devices in a randomized order as the within-subjects variable. We grouped them into *Smart Home Devices* and *Personal Computing Devices* (Group). We used a between-subjects design for the third block of the questionnaire with the Social context (relation to the device owner) as the independent variable.

4.1 Videos

We used videos to illustrate the interactions with the devices. Each video featured a bystander that was either entering a situation where the device was present, currently used by the owner, or where the bystander was implicitly forced to interact with the device (e.g., in the case of a smart doorbell or smart light bulbs). In the first iteration, we planned on using photos to illustrate interactions with the devices. However, this proved to be unsuitable as the capabilities of some devices can not be conveyed using images, for example, for motion-activated light bulbs. Additionally, videos helped make the situation feel more realistic and natural, which is especially important since we

can not guarantee that the participants have experienced such a situation before. We filmed each interaction with the same actors and in the same room to reduce biases. Further, we instructed the actors to engage in a friendly conversation so that the situation itself did not seem unpleasant. Only the interaction with the smart doorbell had to be filmed in another room, i.e., in front of a front door. Additionally, the interaction with the smart security camera required the device owner to be in another room to showcase being notified about movements.

To clarify that the situation should be judged from the bystander's perspective, we added the following description before the videos: *"In the following, we will show you a video. Please turn on the sound and watch the video until the end. Please judge the situation as if you were the person in the yellow shirt, i.e., as if you were joining the situation. This means that you are not the owner of the presented device but perceive the situation from a bystander's perspective."* We muted the videos to not introduce biases from the content of the actors' conversations. However, we dubbed each video with a voice-over to explain the situation, device capabilities, and social relationship. An example is the following text for smart doorbells in the friend scenario: *"You are visiting a friend that has a smart doorbell. The doorbell allows you to communicate via video and audio; thus, your friend can verify who you are before letting you enter."* Even though we instructed the participants to turn on their audio, we additionally provided these descriptions in text form before each video. Figure 2 shows a picture of each video used in the survey. We provide access to all videos licensed under Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) via https://maximiliane-windl.com/skewed-bystanders/.

4.2 Questionnaire Construction

The following explains how we inquired about privacy concerns and which devices and social groups we compared. Further, we describe the final questions about different sensors and locations. We presented each question as a statement to which the participants had to state their agreement using a slider ranging from *Strongly disagree* to *Strongly agree* on a 100-point scale without ticks to prevent the responses from converging around the ticks, cf. [30]. We decided to use visual analog scales instead of Likert scales since they have been shown to lead to more precise responses and thus a higher data quality [13]. In addition, since they collect continuous data, they allow for more statistical tests [37]. To further ensure the quality of the data, we saved a timestamp after each section. Additionally, we had an attention check item after each device, asking randomly to either set a slider all the way to the right or the left.

Privacy Concerns. To assess the privacy concern towards each device, we asked participants to rate the following statement: *"I am strongly concerned when I am in the vicinity of a [friends'] [smartphone]."* In addition to this general concern question, we also asked about eight different specific concerns. We constructed these by conducting six open expert interviews with HCI researchers (five male and one female) and asking for specific concerns about smart home devices and personal computing devices. Their ages ranged from 27 to 31 years ($M = 29.67, SD = 1.37$). We took notes during the interviews. If experts were too generic in their answers, we asked follow-up questions to understand their specific concerns clearly. Next, we analyzed them by coding the statements and using Affinity Diagramming to form groups of related codes [17]. We then integrated all concerns that at least two different experts mentioned. This resulted in the following concerns: local and global data storing, local and global data processing, 1st and 3rd party sharing, profile building, and stolen data.

Devices. We selected five different personal computing devices and five different smart home devices (ten Devices in two Groups). Since we wanted to investigate if smart home devices were perceived as more privacy-concerning, even though they have similar capabilities as personal

Table 1. All devices used in the survey with their respective sensors relevant for bystanders.

Device	Microphone	Camera	Motion
Personal Computer	✓	✗	✗
Laptop	✓	✓	✗
Smartphone	✓	✓	✗
Smartwatch	✓	✗	✗
Tablet	✓	✓	✗
Smart Lights	✗	✗	✓
Smart Speaker	✓	✗	✗
Smart Display	✓	✓	✗
Smart Security Camera	✗	✓	✓
Smart Doorbell	✓	✓	✓

computing devices, we required each selected device to have at least one sensor that can be found in both. We also picked devices that are readily available and have penetrated the consumer market significantly since we wanted to exclude biases that might be caused by people not knowing the device and thus being unsure about its capabilities. That is why we, for example, excluded smart glasses, as they currently are not widely adopted. Therefore, we chose as personal computing devices: a personal computer, a laptop, a smartphone, a smartwatch, and a tablet. For the smart home devices: we selected smart lights, a smart speaker, a smart display, a smart security camera, and a smart doorbell. See Table 1 for an overview of all selected devices and their respective sensors.

Social Groups. Yao et al. [42] found that bystanders' privacy concerns regarding smart home devices varied depending on the social context and that their expectations and information needs were significantly affected by their relationship with the device owner. Specifically, participants in Yao et al.'s [42] study reported that they would prefer using smart home devices that belong to a close friend or family member (i.e., their wife). Another important social context is hotels since they are increasingly integrating smart home appliances, such as Marriott International adopting Amazon Echo speakers[1]. Unlike major hotel chains, private accommodations are a special case since they are not subject to strict control structures as shown by a media outrage about hidden cameras in Airbnb apartments [14]. Therefore, we examined these five Social contexts in our survey: *family*, *friends*, *colleagues*, *homestays*, and *hotels*.

Final Questions. Smart home and personal computing devices are equipped with various sensors that allow for conclusions about peoples' identities to varying degrees. Research showed that users feel more comfortable about anonymously collected data, for example, by temperature or presence sensors [34] and are most concerned about data captured by video cameras or microphones. Therefore, we asked our participants to rate their level of comfort regarding different sensors. Specifically, we asked about motion and temperature sensors, microphones, and video cameras.

Naeini et al. [34] showed that the location influenced participants' comfort level in the sense that they were more uncomfortable with data recorded in private spaces. Yao et al. [42] found that bystanders felt least comfortable with smart home devices being placed in the bedroom or living room. Motivated by this, we additionally asked our participants how concerned they were with

[1] https://www.forbes.com/sites/andriacheng/2018/06/19/amazons-marriott-deal-is-way-beyond-alexa-as-your-new-hotel-butler/

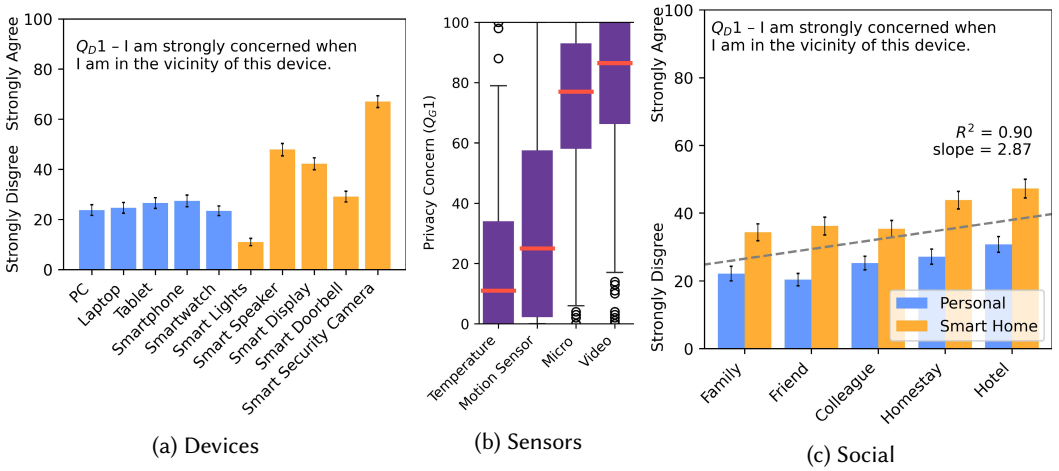


Fig. 3. a) Shows the mean privacy concern for the general concern question (Q_D1) for all ten Devices, whereby the color represents the device Group. The error bars show the standard error. b) Shows box plots of the privacy concern for the different sensor types. c) Shows the mean privacy concern over all devices for the general concern question (Q_D1) grouped by Social context and Group. The trendline represents the change in relation to the social distance with its R^2 fitness and slope. The error bars show the standard error.

data being captured in different rooms. Specifically, we asked about the bedroom, living room, bathroom, kitchen, office, entrance hall, balcony, front door, garage, and nursery.

4.3 Participants

We recruited most (135) participants on Prolific. We also advertised the study via mailing lists of our institution and convenience sampling, aiming to reach an even more diverse participant pool. In total, we recruited 170 people (90 female, 79 male, and one non-binary), which we distributed equally to each of the five Social groups so that each between-subject condition had 34 participants. We recruited our participants in several batches to counterbalance the data set in terms of age, gender, occupation, and country of residence. Their ages ranged from 19 to 62 years (M = 31.1, SD = 9.6). The participants resided on three continents, including Europe, America, and Africa. The five most frequent countries were Germany with 35 participants, the UK (20), Portugal (19), Poland (16), and Greece (14). 113 were full-time and seven part-time employed, 41 were students, and nine were unemployed. Their mean technical affinity according to the ATI scale [12] was 3.9 (SD = 1.0). We used the IUIPC questionnaire [26] to understand participants' general perception of privacy measured on a 7-point Likert scale (higher scores = more private). Thereby we found that they rated their *Awareness* on average with 6.1 (SD = .9), *Control* with 5.4 (SD = 1.2), and *Collection* with 5.5 (SD = 1.4), which indicates a rather high level of privacy concerns across all three areas (using the same interpretation as Hoyle et al. [18]).

The study took on average 22 minutes to complete, and we compensated participants with 3.13£. Students could choose between course credits[2] or monetary compensation.

[2]Students at our institution have to earn a certain amount of study credits towards the completion of their degree, where one hour equals one course credit. The participation is anonymous, and the students receive the same amount of compensation, no matter their responses.

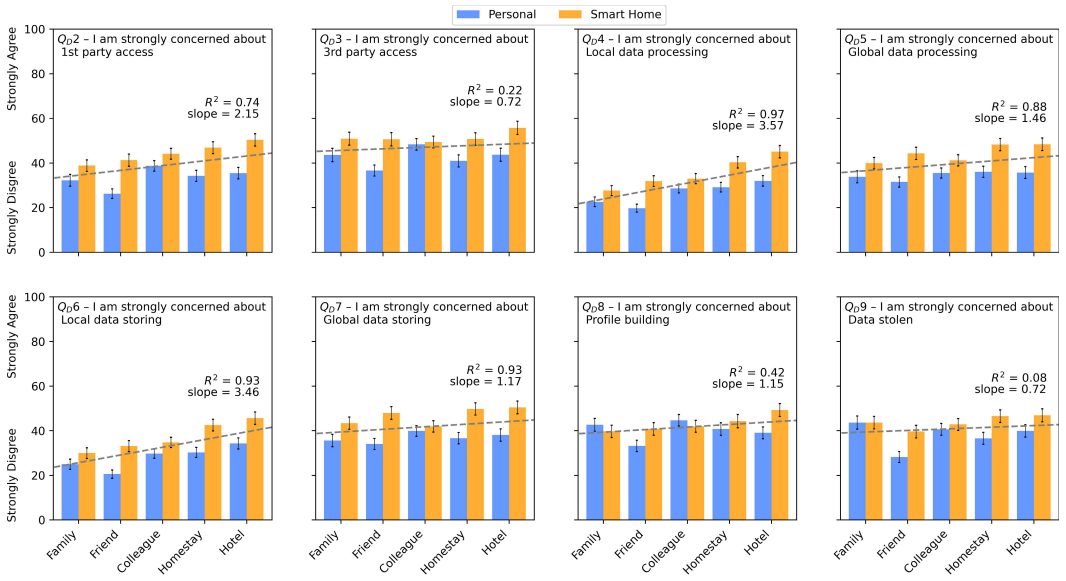


Fig. 4. The mean privacy concern over all devices grouped by Social context and device Group (blue is *Personal* and orange is *Smart Home*) for each of the eight specific concern questions ($Q_D2 - Q_D9$, Section A.3). The trendline represents the change in relation to the social distance with its R^2 fitness and slope. The error bars show the standard error.

5 RESULTS

We used Python and R to analyze the data. To ensure the quality of our data, we performed various sanity checks. First, we excluded all participants that had failed the attention checks. Second, we analyzed the timestamps and excluded all participants who took less than 30 seconds to go through one device as this was the minimum time required to watch the video in full and answer the questions. Third, we excluded all participants with strange patterns in their responses, such as consistently rating every device as 0 or 100. Finally, we excluded all participants with mismatched demographics between Prolific and our survey.

In the following, we present our survey results through our five hypotheses. We describe whether different devices pose different concerns, whether personal computing devices are perceived as more concerning than smart home devices, and how location and ownership influence privacy concerns. Finally, we report qualitative results collected after each situation via a free text field.

5.1 Privacy Concerns of Different Devices

To address **H1**, we analyzed the impact of the ten different devices (Devices) on the general privacy concern (Q_D1). As the data was not normally distributed ($W = .871$, $p < .001$), we conducted a Friedman test which showed that the devices are indeed rated differently ($\chi^2(9) = 513.81$, $p < .001$, *Kendall's* $W = .336$). The mean concerns and the associated standard errors are shown in Figure 3a.

As not all devices have every sensor, we looked at the concerns assigned to the individual sensors (Q_G1) next. Due to normality violations ($W = .885$, $p < .001$), we conducted a Friedman test which showed that the different sensors have significantly different privacy concerns ($\chi^2(2) = 346.734$, $p < .001$, *Kendall's* $W = .680$), see Figure 3b. Pairwise post-hoc tests using Wilcoxon signed rank tests showed that all sensors are rated significantly different (for all $p < .001$).

Table 2. The two-way F-statistics for the nine questionnaire measures ($Q_D1 - Q_D9$) for Group × Social.

	Group		Social		G × S	
	$F_{1,165}$	p	$F_{4,165}$	p	$F_{4,165}$	p
Concern (Q_D1)	114.32	<.001	1.768	.137	1.079	.367
1st party access (Q_D2)	55.330	<.001	0.871	.482	1.583	.181
3rd party access (Q_D3)	23.964	<.001	0.308	.873	1.676	.158
Local processing (Q_D4)	52.234	<.001	2.76	.029	1.861	.2
Global processing (Q_D5)	44.96	<.001	0.335	.854	1.078	.369
Local storage (Q_D6)	50.977	<.001	2.37	.054	1.390	.24
Global storage (Q_D7)	40.698	<.001	0.169	.954	3.226	.081
Profile building (Q_D8)	6.706	.01	0.457	.767	2.77	.028
Stolen data (Q_D9)	21.003	<.001	0.821	.513	1.527	.197

5.2 Privacy Concerns of Personal Versus Smart Home Devices

To investigate **H2a** and **H2b**, we conducted a MANOVA with the between-subjects variable Social and the within-subject variable Group. We found a statistically significant effect on Social ($F_{(4,640)} = 1.503$, $p < .032$, Pillai's trace = .0312, $\eta^2 = .040$). Further, we found a statistically significant effect on Group ($F_{(1,157)} = 13.743$, $p < 0.001$, Pillai's trace = .0.441, $\eta^2 = .070$). Additionally, the two-way interaction Social × Group was not statistically significant ($F_{(4,640)} = .212$, $p = .212$, Pillai's trace = .251, $\eta^2 = .017$). Thus, *Smart Home Devices* are significantly rated more privacy-concerning than *Personal Devices*. See all individual concerns ($Q_D1 - Q_D9$) that are contributing to the understanding of the general concern in Figure 3c and 4. Thus, we can confirm **H2a**.

Based on the findings of the MANOVA, we conducted nine two-way ANOVAs (or non-paramedic equivalents using ARTool [40]) for the questionnaire measures ($Q_D1 - Q_D9$). The individual rankings of the nine concerning factors are shown in Figure 3c and 4. The F-statistics of the nine ANOVAs are presented in Table 2. The analyses showed that there is a significant difference for all measures for the main effect Group. In detail, we found that as a bystander, the average concern for *Personal Devices* is statistically significantly lower than for *Smart Home Devices*. Thus, we can confirm **H2b**. On the other hand, the between-subject variable Social was only statistically significant for local processing (Q_D4). However, pairwise post-hoc tests using Wilcoxon signed rank tests with Bonferroni correction could not reveal differences.

To investigate **H3**, we assumed equidistant distribution between the social groups. Then we fitted a line to all mean concern ratings individually ($Q_D1 - Q_D9$), see Figure 3c and 4. We found that the slopes of all trendlines are positive. As such, we confirm that overall, a stronger social relationship with the device owner reduces privacy concerns. Thus, we accept **H3**.

5.3 Impact of the Locations on Privacy Concerns

To address **H4**, we analyzed the impact of the ten different locations on the privacy concern. As the data was not normally distributed ($W = .892$, $p < .001$), we conducted a Friedman test which showed that the privacy concern is affected by the location ($\chi^2(9) = 568.92$, $p < .001$, *Kendall's W* = .372), see Figure 5a. Therefore, we conducted pairwise post-hoc comparisons using Wilcoxon signed rank tests with Bonferroni correction applied, see Table 3.

5.4 Impact of Ownership on Privacy Concerns

Next, we look at how the ownership influences the general privacy concern (Q_D1) to investigate **H5**. Since all participants owned a smartphone, we had to account for the missing values. Thus,

Table 3. The p-values for the pairwise post-hoc comparisons of the privacy concerns about different locations using Wilcoxon signed rank tests with Bonferroni corrections.

Locations	Garage	Balcony	Outside	Entrance Hall	Kitchen	Home Office	Nursery	Livingroom	Bathroom
Balcony	.099								
Outside	.029	1.							
Entrance Hall	<.001	1.	1.						
Kitchen	<.001	.108	1.	1.					
Home Office	<.001	<.001	<.001	<.001	<.001				
Nursery	<.001	<.001	<.001	<.001	<.001	1.			
Livingroom	<.001	<.001	<.001	<.001	<.001	1.	1.		
Bathroom	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	
Bedroom	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	1.

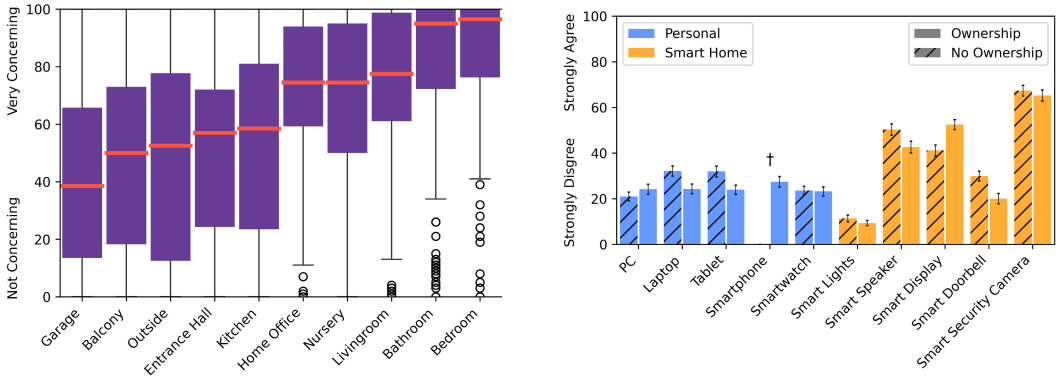
instead of running a Friedman test, we used a Skillings–Mack test [7]. We found that the privacy concern is statistically significant affected by the ownership (*Skillings-Mack* = 241.39, $p < .001$, $df = 169$) with a average rating of 27.0 ($SD = 24.6$) when the devices is owned versus an average concern of 36.5 ($SD = 21.4$) when the device is not owned, see Figure 5b.

5.5 Feedback

After every situation, we asked participants for additional feedback via a free text field. This feedback field was optional. Nevertheless, we received 97 individual feedback statements for specific situations and 14 general feedback statements. We analyzed our participants' responses by coding them and forming groups of related codes using Affinity Diagramming [17]. This process led to the following four themes: *Sensors*, *Influencing Factors*, *Bystander Perspective*, and *Mitigation Strategies*.

Sensors. In line with our quantitative analysis (see Figure 3b), participants mentioned that their privacy concerns strongly depended on the sensors. While they reported being comfortable with data collected by motion sensors, they were concerned about data captured by microphones and cameras. For example, P30 stated not being worried about smart lights because of their inability to record video and audio: *"Since there is no camera/microphone visible I kinda feel safer."* However, several participants mentioned being worried about cameras recording them without their consent or devices always listening and recording audio data. Here, P135 reported in the context of the smart speaker: *"I am concerned that the device is constantly recording without anyone knowing."*

Influencing Factors. Participants elaborated on the various factors such as the location of the device, the social context, the familiarity with the device, and the perceived benefit, that influenced their privacy concerns. In line with our quantitative analysis that showed clear differences in privacy concerns depending on the location (see Figure 5a), several participants mentioned being more comfortable with data being recorded outside. Here, P92 explains regarding the smart security camera: *"I might be able to accept a smart camera placed at the building entrance."* Interestingly, regarding the social context, there were explanations in both directions. While some participants did not consider their conversations with friends sensitive (*"usually, when I am hanging out with friends we do not talk about something that sensitive"* (P27)), others considered their conversations with friends particularly privacy-relevant, e.g., *"when I am at friends and we are having a conversation, I do not like the fact the smart speaker can record this."* (P115). Multiple participants reported not being concerned about a device only because it was so familiar. Here P104 stated *"being around smartphones is so natural these days I would not think about these concerns."* The last factor explicitly mentioned by participants is that often the benefit (increased security) outweighed possible privacy concerns, especially regarding the smart security camera and the smart doorbell.



(a) Locations (b) Ownership

Fig. 5. (a) Shows boxplots of the privacy concerns in different locations, whereby the red horizontal line indicates the mean. b) Shows the mean privacy concerns for all ten DEVICES grouped by ownership (stripes) and device GROUP (color). The error bars show the standard error.

Bystander Perspective. Participants also explained how their unique role as bystanders influenced their privacy concerns in both directions. While some felt that being the bystander and not the primary user reduced privacy threats, others thought the lack of control made them more exposed. P117 elaborated regarding the smart lights: *"I guess these lights could identify some patterns of life, but as it's not in my house, I don't really see the issue."* However, P157 was concerned about the lack of control: *"I can't really control whether the smart speaker is 'listening' or not, and as a visitor, I might not have the 'right' to turn it off."* P92 explained how they use smart devices in their own homes since they can track where the data is sent to but avoid smart devices in Airbnbs since here, they do not have the same control option.

Mitigation Strategies. Several participants reported mitigating their privacy concerns by adjusting their behavior around smart devices. Participants reported being careful to not talk about sensitive information, such as banking data (P27) around smart speakers, or being careful not to be captured by a device's camera, for example, by observing how the owner holds their phone (P60) or if they are in the laptop camera's field of view (P5).

6 DISCUSSION

To the best of our knowledge, this paper is the first to explicitly quantify the discrepancy between the perception of smart home devices and personal computing devices. Thereby we found that bystanders perceive smart home devices as significantly more privacy-concerning than personal computing devices even though they share the same capabilities. In the following, we will outline our findings in detail, along with our five hypotheses.

Our results validate our hypothesis **H1** that different devices pose significantly different privacy concerns. In line with previous work [6, 8, 45], we found that devices with microphones and cameras were perceived as especially privacy-concerning. In contrast, smart lights raised the least privacy concerns, probably because they are only equipped with motion sensors which are perceived as least privacy-relevant, as shown in our data and by previous work [45]. In contrast, by far, the most concerns were raised by the smart security camera, followed by the smart speaker. Our qualitative findings provide reasoning. Here, several participants mentioned feeling surveilled by both devices, either by constantly being watched or listened to without consenting to either. In line with previous

work that already called to notify bystanders about the presence of devices with sensors in the context of assistive devices for visually impaired people [2], we conclude that **bystanders should be notified about the presence of devices, especially those with microphones and cameras.** Before intervening, notifying is the first necessary step to help bystanders reflect on possible concerns. Yet, we see it as an important challenge for future work to hand bystanders the necessary tools to handle these concerns.

We could also validate our hypotheses **H2a** and **H2b** that smart home devices are perceived significantly more privacy-concerning than personal computing devices. Here again, the qualitative data hints at possible explanations. Several participants mentioned not being concerned about smartphones anymore because they are so familiar. Participants also indicated why they were less concerned about voice assistants in smartphones or laptops. For example, P115 mentioned, *"the voice-enabled part isn't as prominent as, say, in a smart speaker."* Thus, we suspect participants underestimate the privacy threats of personal computing devices because they have already been using them for several years before they even had such capabilities. Therefore, they do not relate them as immediately with voice assistants and, thus, privacy threats, as they do with devices where this is the core feature, such as smart speakers. We see that, even though smart home devices are generally perceived as more privacy-concerning, personal computing devices also raise privacy concerns of bystanders. Thus, we conclude that **bystanders should not only be notified about the presence of smart home devices but also of personal computing devices.** This continues to be important as current strategies to inform bystanders, such as the LED light in laptops to indicate an active webcam, have proven to be ineffective [36].

We further verified our third hypothesis (**H3**): In line with Yao et al. [42], we found a general trend that a stronger social relationship reduced privacy concerns. However, this trend is not as clear as suggested by Yao et al. [42]. We find additional possible reasoning in our qualitative data. While some participants considered their conversations with friends especially privacy-relevant, others felt these conversations were not very sensitive. Worthy et al. [41] provides additional explanations. They suggest people might be less drawn to confide in the people closest to them since they are most likely to draw conclusions from their behaviors. They explain this with the *mosaic effect* [21] stating that the people closest to us already have more pieces of our puzzles, which might make us wish to exert even greater control over the information we share with them. However, the privacy concern generally increases the more unfamiliar the other party is. Therefore, notifying bystanders about the presence of devices is especially relevant in unknown spaces, such as hotels or Airbnbs. However, since individual preferences differ for closer relationships, **we call for notifying bystanders about the presence of devices in all social contexts.**

In line with Naeini et al. [34] and Yao et al. [44], we could also validate our fourth hypothesis (**H4**) that privacy concerns increased with the space's intimacy. Accordingly, our participants rated all three locations outside the home (garage, balcony, and outside) as least concerning and the bedroom and bathroom as most concerning. Inside the house, the entrance hall was assessed as least privacy-relevant. Therefore, we argue that **bystanders should be notified about devices before entering intimate spaces, for example, already in the entrance hall.** This relevance of timing was also already emphasized by previous work in the context of body-worn cameras as a pre-requisite to giving bystanders the option to consent before being exposed to possibly privacy-invading procedures [23].

Finally, as already suggested by Apthorpe et al. [4], we could also confirm our fifth hypothesis (**H5**), that participants assign fewer privacy concerns to devices they own, i.e., devices they are already experienced with. This leads us to believe that some of the current privacy concerns might decrease over time as devices penetrate households even more and, thus, get more familiar.

7 LIMITATIONS AND FUTURE WORK

We acknowledge that our work is prone to certain limitations. First, our sample is skewed towards Europe. As previous work already showed that the country of residence [24] influences users' privacy concerns, it might be interesting to repeat the survey with a more diverse sample, especially including countries outside of Europe. Second, while we aimed at making the scenarios as realistic as possible by creating videos, it might still be difficult to put oneself in the position of a bystander and the specific social context, especially since those social relationships vary in themselves. For example, a social relationship with a "family member" could vary depending on which family member it is and, thus, how close the relationship is. However, since we could already observe significant effects in this first investigation, we expect more natural environments to yield even more robust results. Therefore, we see it as an avenue for future research to replicate our findings in the wild.

Further, as we showed that bystanders perceive some sensors as significantly more privacy-concerning than others, future work should investigate how to accommodate such concerns. A possible approach is to allow deactivating sensors independently from one another. Here, device manufacturers should also support such efforts by allowing control at the individual sensor level, for example, by providing an API.

Finally, while in the digital world, providers are forced by law to inform users about their privacy practices through the GDPR and privacy policies, there is no comparable system in the real world. However, as our survey showed that privacy concerns are prevalent in everyday life, we see a need to provide users with notice and choice in the real world – just as it is done online through privacy policies.

8 CONCLUSION

We investigated whether bystanders associate more privacy concerns with smart home devices than personal computing devices, even though both have equal capabilities. In addition, we surveyed the influence of the social relationship on this perception. We found that smart home devices are perceived as significantly more concerning than personal computing devices and that a stronger social relationship mitigates some of the concerns. We further found several factors that influenced the severity of privacy concerns: cameras and microphones were assessed as especially privacy-threatening, and privacy concerns increased with greater intimacy of the location and decreased with greater familiarity through ownership. We thus call for informing bystanders about the presence of smart home devices and personal computing devices in all social contexts and before entering intimate spaces.

ACKNOWLEDGMENTS

This work has been funded by the German Federal Ministry of Education and Research (BMBF) under Grant No. 01IS18036A. The authors of this work take full responsibilities for its content.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a Limit? Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 89 (sep 2018), 27 pages. https://doi.org/10.1145/3264899

[3] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *Workshop on Data and Algorithmic Transparency* (2016).

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 59 (jul 2018), 23 pages. https://doi.org/10.1145/3214262

[5] Natã M Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 211–231. https://doi.org/10.2478/popets-2019-0066

[6] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC, 16)*. IEEE, 172–175. https://doi.org/10.1109/EISIC.2016.044

[7] Mark Chatfield and Adrian Mander. 2009. The Skillings-Mack test (Friedman test when there are missing data). *The Stata journal* 9, 2 (01 Apr 2009), 299–305. https://pubmed.ncbi.nlm.nih.gov/19829764

[8] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/2370216.2370226

[9] Benjamin R. Cowan, Nadia Pantidi, David Coyle, Kellie Morrissey, Peter Clarke, Sara Al-Shehri, David Earley, and Natasha Bandeira. 2017. "What Can i Help You with?": Infrequent Users' Experiences of Intelligent Personal Assistants. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Vienna, Austria) *(MobileHCI '17)*. Association for Computing Machinery, New York, NY, USA, Article 43, 12 pages. https://doi.org/10.1145/3098279.3098539

[10] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352

[11] Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang. 2014. Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices* (Scottsdale, Arizona, USA) *(SPSM '14)*. Association for Computing Machinery, New York, NY, USA, 63–74. https://doi.org/10.1145/2666620.2666623

[12] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150

[13] Frederik Funke and Ulf-Dietrich Reips. 2012. Why Semantic Differentials in Web-Based Research Should Be Made from Visual Analogue Scales and Not from 5-Point Scales. *Field Methods* 24, 3 (2012), 310–327. https://doi.org/10.1177/1525822X12444061

[14] Sidney Fussell. 2019. Airbnb Has a Hidden-Camera Problem. https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/

[15] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2018. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. In *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP)*. USENIX, Baltimore, MD, USA. https://doi.org/10.5445/IR/1000083578

[16] Loni Hagen. 2017. Overcoming the Privacy Challenges of Wearable Devices: A Study on the Role of Digital Literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research* (Staten Island, NY, USA) *(dg.o '17)*. Association for Computing Machinery, New York, NY, USA, 598–599. https://doi.org/10.1145/3085228.3085254

[17] Gunnar Harboe and Elaine M. Huang. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proc. 33rd Annual ACM Conf. Human Factors in Computing Systems*. ACM, New York, NY, USA, 95–104. https://doi.org/10.1145/2702123.2702561

[18] Roberto Hoyle, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. 2020. Privacy Norms and Preferences for Photos Posted Online. *ACM Trans. Comput.-Hum. Interact.* 27, 4, Article 30 (aug 2020), 27 pages. https://doi.org/10.1145/3380960

[19] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1645–1648. https://doi.org/10.1145/2702123.2702183

[20] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 571–582. https://doi.org/10.1145/2632048.2632079

[21] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B. Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, Nicolas Roussel, and Björn Eiderbäck. 2003. Technology Probes: Inspiring Design for and with Families. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 17–24. https://doi.org/10.1145/642611.642616

[22] Anindya Maiti Kirsten Crager. 2017. Information Leakage through Mobile Motion Sensors: User Awareness and Concerns. *Proceedings of the European Workshop on Usable Security (EuroUSEC)* (2017). http://dx.doi.org/10.14722/eurousec.2017.23013

[23] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-Worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction* (Stockholm, Sweden) *(TEI '18)*. Association for Computing Machinery, New York, NY, USA, 177–187. https://doi.org/10.1145/3173225.3173234

[24] 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'21)*. Association for Computing Machinery, New York, NY, USA, Article 307, 10 pages. https://doi.org/10.1145/3411763.3451633

[25] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (nov 2018), 31 pages. https://doi.org/10.1145/3274371

[26] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. http://www.jstor.org/stable/23015787

[27] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK*. https://doi.org/10.14722/eurousec.2018.23016

[28] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019). https://doi.org/10.2478/popets-2019-0068

[29] 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* 2020, 2 (2020), 436–458. https://doi.org/doi:10.2478/popets-2020-0035

[30] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. 2016. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5421–5432. https://doi.org/10.1145/2858036.2858063

[31] Maryam Mehrnezhad, Ehsan Toreini, and Sami Alajrami. 2018. Making Sense of Sensors: Mobile Sensor Security Awareness and Education. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust* (Orlando, Florida, USA) *(STAST '17)*. Association for Computing Machinery, New York, NY, USA, 40–52. https://doi.org/10.1145/3167996.3168001

[32] Maryam Mehrnezhad, Ehsan Toreini, Siamak F Shahandashti, and Feng Hao. 2018. Stealing PINs via mobile sensors: actual risk versus user perception. *International Journal of Information Security* 17, 3 (2018), 291–313. https://doi.org/10.1007/s10207-017-0369-x

[33] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. 2010. Private Memoirs of a Smart Meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (Zurich, Switzerland) *(BuildSys '10)*. Association for Computing Machinery, New York, NY, USA, 61–66. https://doi.org/10.1145/1878431.1878446

[34] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[35] Johannes Obermaier and Martin Hutle. 2016. Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (Xi'an, China) *(IoTPTS '16)*. Association for Computing Machinery, New York, NY, USA, 22–28. https://doi.org/10.1145/2899007.2899008

[36] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1649–1658. https://doi.org/10.1145/2702123.2702164

[37] Ulf-Dietrich Reips and Frederik Funke. 2008. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior Research Methods* 40, 3 (01 Aug 2008), 699–704. https://doi.org/10.3758/BRM.40.3.699
[38] Emmanuel Sebastian Udoh and Abdulwahab Alkharashi. 2016. Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. In *2016 Future Technologies Conference (FTC)*. IEEE, 926–931. https://doi.org/10.1109/FTC.2016.7821714
[39] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. *Proc. Priv. Enhancing Technol.* 2016, 3 (2016), 172–190. https://doi.org/10.1515/popets-2016-0022
[40] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. 2011. The Aligned Rank Transform for Nonparametric Factorial Analyses Using Only Anova Procedures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 143–146. https://doi.org/10.1145/1978942.1978963
[41] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890
[42] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (nov 2019), 24 pages. https://doi.org/10.1145/3359161
[43] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6789–6793. https://doi.org/10.1145/3025453.3026049
[44] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 6777–6788. https://doi.org/10.1145/3025453.3025907
[45] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469

A SURVEY

A.1 Demographics

(1) In which country do you currently reside? (drop-down list)
(2) Which gender do you most identify with?
- Male
- Female
- Non-binary
- Self-described

(3) How old are you? (number field)
(4) What is the highest degree you have received?
- Less than high school degree
- High school graduate
- Some college but no degree
- Bachelor's degree
- Master's degree
- Doctoral degree
- Vocational education

(5) What is your current primary occupation? (free text)

A.2 Privacy Perception & Affinity For Technology

IUIPC. Many people spend a lot of time online, for example on their smartphones, tablets, or computers. During this time online, people also share data, for example when signing up for online shopping, posting on social media, or using GPS in navigation apps. In the following

questions, we are interested in your personal experience and perception when sharing your personal information online. Please indicate the degree to which you agree/disagree with the following statements. (7-point Likert scale ranging from strongly disagree to strongly agree)

(1) I have been the victim of what I felt was an improper invasion of privacy.
(2) I am very concerned about the privacy of my data.
(3) I always falsify personal information needed to register with some websites.
(4) It usually bothers me when online companies ask me for personal information.
(5) When online companies ask me for personal information, I sometimes think twice before providing it.
(6) It bothers me to give personal information to so many online companies.
(7) I'm concerned that online companies collect too much personal information.
(8) Your online privacy is really a matter of your right to exercise control and autonomy over decisions about how your information is collected, used, and shared.
(9) Your control of your personal information lies at the heart of your privacy.
(10) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
(11) Companies seeking information online should disclose the way the data are collected, processed, and used.
(12) A good consumer online privacy policy should have a clear and conspicuous disclosure.
(13) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

ATI. On this page, we are interested in how you deal with technology. Please indicate the degree to which you agree/disagree with the following statements. (6-point Likert scale ranging from completely disagree to completely agree)

(1) I like to occupy myself in greater detail with technical systems.
(2) I like testing the functions of new technical systems.
(3) I predominantly deal with technical systems because I have to.
(4) When I have a new technical system in front of me, I try it out intensively.
(5) I enjoy spending time becoming acquainted with a new technical system.
(6) It is enough for me that a technical system works; I don't care how or why.
(7) I try to understand how a technical system exactly works.
(8) It is enough for me to know the basic functions of a technical system.
(9) I try to make full use of the capabilities of a technical system.

A.3 Questions Per Device

In the following, we will show you a video. Please turn on the sound and watch the video until the end. Please judge the situation as if you were the person in the yellow shirt, i.e., as if you were joining the situation. This means that you are not the owner of the presented device but perceive the situation from a **bystander perspective.** Please evaluate this situation as if you were visiting [social group] (sliders from strongly disagree to strongly agree)

(1) I am very familiar with [device].
(2) Do you currently own or have you ever owned [device]?
    - Yes
    - No
(3) For how long have you owned [device]? [in years] (free text)
(4) I am strongly concerned when I am in the vicinity of a [social group's] [device].

(5) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **local data processing** (the data is processed locally in your home network).
(6) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **global data processing** (the data is processed remotely - it gets sent to servers outside of your home network).
(7) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **local data storing** (your data is stored locally on the device in your home network).
(8) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **global data storing** (your data gets sent and stored on remote servers).
(9) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **1st party data access** (the manufacturer has access to your data).
(10) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **3rd party data access** (entities outside of the device manufacturer have access to your data).
(11) When I am in the vicinity of a [social group's] [device], I am strongly concerned about **profile building**, e.g., for targeted ads (your data gets analyzed to draw conclusions about your person).
(12) When I am in the vicinity of a [social group's] [device], I am strongly concerned about my **data getting stolen**.
(13) Use this field if you have any additional feedback regarding this situation (free text).
(14) Put the slider all the way to the [right/left] (attention check item).

A.4 Final Questions

Concern Sensors (sliders from strongly disagree to strongly agree)

(1) I am very concerned about data captured by **motion sensors**.
(2) I am very concerned about data captured by **microphones**.
(3) I am very concerned about data captured by **video cameras**.
(4) I am very concerned about data captured by **temperature sensors**.

Concern Rooms (sliders from strongly disagree to strongly agree)

(1) I am very concerned when data is captured in the **entrance hall**.
(2) I am very concerned when data is captured in the **bedroom**.
(3) I am very concerned when data is captured in the **kitchen**.
(4) I am very concerned when data is captured in the **bathroom**.
(5) I am very concerned when data is captured in the **livingroom**.
(6) I am very concerned when data is captured on the **balcony**.
(7) I am very concerned when data is captured outside of the **front door**.
(8) I am very concerned when data is captured in the **garage**.
(9) I am very concerned when data is captured in the **home office**.
(10) I am very concerned when data is captured in the **nursery**.

Concern Companies (sliders from strongly disagree to strongly agree with option *I do not know this company.*)

(1) I think **Samsung** is very trustworthy.
(2) I think **Apple** is very trustworthy.
(3) I think **Xiaomi** is very trustworthy.
(4) I think **Lenovo** is very trustworthy.
(5) I think **HP** is very trustworthy.
(6) I think **Dell** is very trustworthy.
(7) I think **Amazon** is very trustworthy.

(8) I think **Google** is very trustworthy.
(9) I think **Baidu** is very trustworthy.
(10) I think **Huawei** is very trustworthy.
(11) I think **Nest** is very trustworthy.
(12) I think **Ring** is very trustworthy.
(13) I think **Arlo** is very trustworthy.
(14) I think **Ecobee** is very trustworthy.
(15) I think **Wyze** is very trustworthy.

A.5 Feedback

If you have any further feedback you can let us know here. (free text)