# “They Didn’t Buy Their Smart TV to Watch Me with the Kids”: Comparing Nannies’ and Parents’ Privacy Threat Models for Smart Home Devices

RUBA ABU-SALMA, King’s College London, London, UK
JUNGHYUN CHOY, ALISA FRIK, and JULIA BERND, International Computer Science Institute, Berkeley, CA, USA

Smart home devices raise privacy concerns among not only primary users but also bystanders like domestic workers. We conducted 25 qualitative interviews with nannies and 16 with parents who employed nannies, in the U.S., to explore and compare their views on and privacy threat models for smart home devices. We found device-specific purposes of use inspired different perspectives among nanny participants. Most were comfortable with employers’ smart speakers and smart TVs, whose purpose had nothing to do with them. However, with indoor smart cameras, nanny participants were often not just bystanders but targets of monitoring; in such situations, they had a wider range of attitudes. In contrast, parent participants tended to have more similar views across devices. We found notable disconnects regarding disclosure, where nanny participants often hesitated to ask about cameras, but parent participants assumed nannies just didn’t care. We recommend prioritizing interventions supporting disclosure, discussion, and sharing control.

CCS Concepts: • **Security and privacy** → **Social aspects of security and privacy**; Usability in security and privacy; • **Human-centered computing** → *Empirical studies in HCI*; Empirical studies in ubiquitous and mobile computing; • **Social and professional topics** → *Cultural characteristics*;

Additional Key Words and Phrases: Internet of Things (IoT), smart homes, bystanders, domestic workers, multi-user privacy, individual agency

**ACM Reference format:**
Ruba Abu-Salma, Junghyun Choy, Alisa Frik, and Julia Bernd. 2025. “They Didn’t Buy Their Smart TV to Watch Me with the Kids”: Comparing Nannies’ and Parents’ Privacy Threat Models for Smart Home Devices. *ACM Trans. Comput.-Hum. Interact.* 32, 2, Article 12 (April 2025), 53 pages.
https://doi.org/10.1145/3702321

This research was supported in part by grants from the Center for Long-Term Cybersecurity at the University of California, Berkeley, the U.S. National Science Foundation (award CNS-2114229), and the U.S. National Security Agency (contract H98230-18-D-0006).

Authors’ Contact Information: Ruba Abu-Salma (corresponding author), King’s College London, London, UK; e-mail: ruba.abu-salma@kcl.ac.uk; Junghyun Choy, Unaffiliated; e-mail: juchoy99@gmail.com; Alisa Frik, International Computer Science Institute, Berkeley, CA, USA; e-mail: afrik@icsi.berkeley.edu; Julia Bernd, International Computer Science Institute, Berkeley, CA, USA; e-mail: jbernd@icsi.berkeley.edu.

ACM 1557-7325/2025/4-ART12
https://doi.org/10.1145/3702321

## 1 Introduction

With the rise of **Internet of Things (IoT)** technologies and, especially, smart home devices, from surveillance and security cameras to smart speakers and location trackers, the privacy preferences and choices of individuals who own or deploy such devices often impact the privacy and individual agency of those around them.

For example, recent research has explored how the impact of smart home devices plays out in multi-user smart homes (i.e., households where different groups of people—not only device owners and primary users—interact with or are affected by those devices) (overview in [60]). In particular, the privacy and agency of secondary users, incidental users, and bystanders in such homes, as well as surveillance targets, have recently received more focused research attention (see Section 2).[1] Frequently, this work has found that control of devices and of data collection and processing in smart homes are aligned with the social configurations and power dynamics between residents and bystanders.

In this article, we examine a specific privacy-relevant dynamic in smart homes, that between *domestic childcare workers* and *parents who employ domestic childcare workers*. We explore the views of both groups, then compare them to identify disconnects. Because domestic workers are likely to be exposed as bystanders to other people's smart devices in a situation that is at the same time their workplace and their employers' home, the effects on their privacy choices and individual agency regarding those devices are likely to be amplified by power dynamics. In addition to being bystanders to smart home data collection, domestic workers can sometimes be targets of surveillance by their employer [28]. The issue is particularly complex in childcare; although caregiving is a trust-based relationship, it is at the same time subject to the equation of *surveillance-as-care* [45, 68], where surveilling both caregiver and child may be seen as necessary for responsible parenting.

Recent studies conducted in Hong Kong [37], Macao [38], and Jordan [3, 4, 6] have examined in depth how domestic workers'—including childcare workers'—privacy is affected by cameras and other smart home devices in those countries.

We contribute to work on privacy of domestic workers and other bystanders in smart homes by designing and conducting a multi-stakeholder interview study of smart home perspectives, with domestic childcare workers (N = 25) and parents who employ such workers (N = 16) in the U.S. In a previous paper, we analyzed smart cameras' effects on employer-employee relationships, based on the dataset of nanny interviews [16].[2] The present article takes a broader view, comparing views on cameras with views on other smart home devices, as well as adding the parent interview dataset.

This article addresses the following **Research Questions (RQs)**:

(1) What are the experiences with and views of domestic childcare workers on smart home devices in their employers' homes, and what factors influence these views? Do views differ from one smart home device to another and, if so, how and why?
(2) What are the views of parents who employ domestic childcare workers on smart home devices, and why did they deploy them? How do parents view the devices as affecting their own privacy, security, and safety, and that of their workers?

[1] Terminology in this area is still in flux; see Pierce et al. [64, p. 37] for a chart representing some of the myriad schemes. In this article, we use *primary users* and *secondary users* for smart home residents with different levels of control over devices, and *bystanders* for others who are affected by them. (Bystanders may also sometimes be *incidental users*, especially if they are frequently in the home.) People in any of those categories may also be *targets of surveillance* by (other) users.

[2] In this article, we use "nannies" and "nannying" to refer to domestic childcare workers/work, but "nanny" interviews included nannies, au pairs, and professional babysitters. Parent participants included employers of both nannies and au pairs.

(3) How do views of domestic childcare workers and parents who employ such workers about smart home devices align, and how do they differ? Are assumptions these groups make about each other correct?
(4) What types of interventions should be prioritized to balance the privacy needs and preferences of domestic childcare workers with device utility for parents who employ such workers?

In addition to being the first study to focus on domestic childcare workers and parents employing such workers in U.S. smart homes, ours is the first study to take an in-depth comparative look at the factors affecting how both smart home device owners/primary users and domestic workers view *different types* of smart home devices. We found that those device-specific views had different effects on participants' privacy attitudes, behavior, concerns, and choices—as well as on what social and technical privacy protections participants viewed as helpful.

In particular, we show how different purposes of use affected participants' threat models. Nannies' perspectives on different types of devices tended to mainly depend on the uses to which they could be put—most smart speakers and smart TVs could not easily be used by an employer to monitor a nanny (there is no such thing as a "nanny TV"), while most indoor smart cameras could. At the same time, the same type of device used for different purposes (e.g., cameras for monitoring nannies vs. for home security) might inspire quite different attitudes, concerns, and choices. On the other hand, since parents generally were not concerned about consequences of data access by anyone within their household, their perspectives tended to be more similar across device types.

Based on our findings, we recommend prioritizing privacy interventions that support social aspects of multi-stakeholder privacy, particularly around disclosure of, discussions about, and shared control over devices, while mitigating the effects of uneven power dynamics between employers and employees.

## 2 Related Work

Research on IoT and smart home privacy has examined the perspectives of device owners or primary users who choose to deploy the device, other users who share some control over it, and—most relevant to our study—surveillance targets, incidental users, and bystanders who have little to no control.

Many papers mentioned in this section suggest privacy interventions, especially in smart home product design; we discuss some of these interventions in Section 6.3.

### 2.1 Privacy of Smart Home Device Owners and Primary Users

Studies have examined smart home device owners' and primary users' privacy expectations, attitudes, and concerns, especially regarding device manufacturers or service providers collecting and sharing data from smart homes (overviews in [47, 63]). Much of this research has found that primary users have differing views on data collection, processing, and sharing depending on context-specific factors such as what type of data is collected, who receives or sees the data, how the data is used, and what the purposes of collection, processing, and sharing are [e.g., 13, 14, 32, 48, 49, 62]. In particular, researchers have identified a complex interplay between data recipients and device purpose of use [e.g., 1, 12, 29, 92].

Interviews of primary users by Tan et al. [74] found that camera uses related to secondary users and bystanders, e.g., keeping an eye on children or monitoring caregivers—or at least having the ability to do so—were sometimes the motivator for a camera purchase, and sometimes incidental and opportunistic. Concerns about secondary user or bystander privacy have sometimes been raised by primary users, even where it was not the focus of the study. However, as noted by Tabassum and Lipford [72], even device owners who want to protect bystander privacy may not know how to do so. Notably, several participants in a study by Choe et al. [21] commented that they would be less likely to disclose smart devices to domestic workers than to family and friends.

## 2.2 Multi-User Smart Home Privacy

Domestic workers share some similarities with secondary users or “passenger” users in multi-user smart homes, including frequent and long-term exposure to, and sometimes co-use of, devices. (See Meng-Schneider et al. [60] for a recent overview of work on multi-user smart home dynamics.) In other ways, domestic workers are more like incidental users or bystanders (e.g., visitors; see Section 2.4), in that they have little to no ownership or control of the device, and may be seen as having no stake in it.

Most work on multi-user smart homes has neither compared views on specific devices in-depth, nor qualitatively examined privacy attitudes through the lens of contrasting device purposes and data recipients. However, several have described how control of devices—and therefore control of dataflows—can depend on dynamics in relationships between residents, setting the stage for our multi-stakeholder study. For example, an interview and survey study by Apthorpe et al. [11] showed that IoT devices can have positive (e.g., household management or facilitating independence) and negative (e.g., allowing surveillance or causing disagreements over use) effects on relationships. An interview study by Huang et al. [35] found that smart speaker users’ privacy attitudes and coping strategies (avoidance or acceptance) played out differently with respect to other household occupants vs. external recipients such as device service providers. Geeng and Roesner’s [31] interview and experience-sampling study of multi-occupant smart homes found that tensions arose between primary users who drove adoption of the device and other residents, over control of and access to device settings. However, secondary users were generally not very concerned, within the context of cooperative relationships.

Interview studies by Kraemer et al. [42] and Ehrenberg and Keinonen [27] found that often whoever installs the device drives choices about device use, and that attitudes about technology control are closely connected to comfort and power dynamics in the relationship. Surveys by Kraemer et al. [43] found that perceptions about how much control secondary users should have depend on the device location or area of effect, and on the relationship between primary and secondary users.

A survey by Moh et al. [61] examined unauthorized use of devices by their owners’ associates and the factors that influence whether owners perceived it as *misuse*, including the nature of the relationship between owner and unauthorized actor. The interaction between relationship dynamics and control over smart home devices is clearest in explicitly adversarial situations and, at worst, intimate partner violence (overview in [7]), where users may become surveilled subjects.

## 2.3 Surveillant Care in Smart Homes

Several authors have analyzed how IoT devices fit into the “surveillance as care” paradigm, where technology-enabled monitoring is seen as necessary to responsibly care for vulnerable people like children or older adults. For example, Widmer and Albrechtslund’s [81] interviews explored how parents balance surveillant care against children’s privacy and agency in use of location tracking apps. In interviews, Ur et al. [77] found disparities between parents’ and adolescents’ views on data collection from smart doorbells and locks; adolescents preferred to minimize it.

Most relevant to our work, some participants in a scenario-based study by Wong et al. [85] commented that monitoring both children and paid caregivers can be seen as an expression of care—though others discussed how device owners simultaneously incur responsibilities to domestic workers, around disclosure. Stark and Levy [68] provide an analysis of how the surveillance-as-care paradigm convinces consumers that responsible care entails monitoring caregivers along with the person being cared for; our study demonstrates how this concept can play out on each side.

### 2.4 Privacy of Smart Home Visitors and Bystanders

People may also be exposed to smart home devices in others' homes, as bystanders. Research on smart home visitors has not focused specifically on the kinds of power imbalances that are at play in domestic worker privacy, nor on concerns about specific device purposes. However, similarities between views of visitors and domestic workers can be seen in the importance of the nature of the relationship and assumptions about the device owner's or data recipient's general good intentions, which were highlighted by participants in several studies on smart home visitors.

For example, Marky et al. [53] and Windl and Mayer [82] found in interviews and surveys with visitors to smart environments that levels of privacy concern and data-sharing preferences depended in part on their trust in the device owner as recipient. Participants in a vignette study by Chiang et al. [20] that included spouse, neighbor, short-term tenant, and visiting-worker scenarios mentioned that the type of relationship affected whether they thought consent for using smart devices was necessary—though the direction of effect was highly variable, indicating a need for deeper study.

Windl and Mayer's study [82] also found that devices with cameras and microphones were more concerning than other types; similarly, Wang et al. [80] found that device type was the main factor (amongst those they studied) impacting Airbnb guests' desire to negotiate about smart device privacy. However, the purposes of different device types may underlie some of those findings. An interview study by Ahmad et al. [2] is suggestive in this regard; it focused on comparing non-owners' perceptions of a Nest Cam vs. an Echo Show, finding that participants' mental models of and concerns about the two differed mainly based on the main *functionality* (video recording vs. interaction).

Focus groups conducted by Yao et al. [89] explored different exposure scenarios and devices (cameras in a short-term rental, smart toys at a playdate, a cohabitant's smart speaker), and found that, in all cases, bystanders'/secondary users' perceptions were affected by trust toward device owners and (especially relevant to us) the purpose or perceived utility of the device to the owner (e.g., whether a camera was for home safety) [cf. 29]. We explore the importance of purpose in a different situation, that of in-home childcare.

### 2.5 Comparing User and Bystander Views

Several studies have explicitly compared people's views as smart home users or residents vs. people's views as bystanders. An interview study on smart speakers by Meng et al. [59] found that cohabitants/co-owners have different concerns about the smart speaker of someone they live with, like not wanting to mess with someone else's property, while visitors may focus more on protecting themselves.

Marky et al. [55] compared interviewees' views when presented with a smart home owner scenario vs. a bystander scenario, finding that those in the bystander scenario had more concerns than owners about privacy violation and exerting control over data collection. Participants pointed out that visitors received less benefit from device use, and, thus, their concerns were not mitigated by any convenience tradeoff. Our work explores how these tradeoffs play out in in-home childcare, where potential benefits are often complex and indirect. Mare et al. [51] compared views of Airbnb guests and hosts. Their surveys did not explicitly explore device purposes, but they note that some guests were concerned about spying or discrimination by hosts.

Focus groups and surveys conducted by Cobb et al. [22] also found that participants' concerns as incidental users or bystanders were quite different from their concerns as device owners.

Interestingly, they found that participants felt more positive about devices they encountered in others' homes in the course of their work than other situations; however, it is not clear what type of work or frequency of exposure was involved. Participants had the least positive views of cameras and smart speakers. A survey by Despres et al. [23] similarly found differences in participants' concerns, with video data collection being especially concerning in others' homes as opposed to one's own.

Again, relationships are a key factor in privacy perspectives. Alshehri et al. [8] presented survey participants with owner scenarios involving either trusted friends or visiting (unknown/untrusted) workers, and found differences in owners' willingness to address privacy concerns of trusted vs. untrusted bystanders. Participants in bystander scenarios generally did not expect disclosure by owners, even if they might have preferred it.

In interviews, Marky et al. [52] found that smart device owners were open to guests having some privacy control, as long as it did not impinge on utility or aesthetics. Comparing against surveys with smart home guests, they found that both groups tended to put responsibility for guest privacy largely on the host. A related study found that visitors had impoverished mental models of smart home data flows compared to hosts, indicating a need for more support in privacy control [54]. Both Marky et al. [52] and Thakkar et al. [75] found that visitors were more attentive than owners to the social awkwardness of asking for privacy considerations. Seeing this disconnect in a situation of relative social equality raised the question of whether, in a domestic employment situation, the disconnect would be even more prominent, or whether device owners might be more aware of potential constraints for workers because the imbalance is clearer.

### 2.6 Domestic Work in Smart Homes

As we noted, some studies discussed above included participants' experiences with or as domestic workers [22, 74], but did not focus on these groups, and some studies have included hypothetical domestic-worker scenarios among others [8, 9, 20, 64, 85]. A few prior studies have focused specifically on domestic workers.

In interviews with domestic workers (including childcare and eldercare workers) and employers of domestic workers in Jordan, Albayaydh and Flechais [3] found workers were most concerned about devices that collected audio and/or video, for example, because data were more resharable. The study did not examine the effects of device purposes, but noted that some domestic workers thought they were targets of surveillance by device owners. Some employers disclosed their devices, but some chose not to, or assumed domestic worker participants would notice them—while employees might view non-disclosure as a sign of distrust.

In a follow-up study, Albayaydh and Flechais [4, 6] conducted additional interviews in Jordan, this time including policymakers, activists, and smart home device designers as well as domestic workers and employers. They explored how factors like social norms, customs, religion, and economic status influenced power dynamics in smart homes. They found that workers tended to accept working conditions, including smart devices, due to socioeconomic factors. In these and a further related study [5], Albayaydh and Flechais highlighted design challenges for privacy protection in the context of Jordanian households, where they found that the head of the family—generally the father—made decisions both about devices and about employment of domestic workers, and some families restricted workers' personal activities.

Neither of these studies compared views across different types of devices nor effects of device purposes. Further, Albayaydh and Flechais did not focus specifically on domestic *childcare* workers and how their views compared with employers within the particular constraints of a care situation.

An interview and diary study with Filipina nannies working in Hong Kong by Johnson et al. [37] focused on cameras used for surveillance. Their participants often viewed surveillance as counterproductive to their employers' (presumed) purposes for using the cameras, in that they did not feel they delivered the best care when being watched, and might try to evade cameras. The study highlighted how camera use reinforced power imbalances and reflected social hierarchies based on gender, race, and class. In particular, cameras enabled excessive monitoring and micromanaging, which participants found detrimental to their relationships with their employers. A quantitative analysis by Yang et al. [87] of job satisfaction among domestic workers in China found that video cameras in themselves did not have a direct impact on satisfaction; rather, effects were mediated by whether the worker had experienced discrimination based on their job status.

Ju et al. [38] interviewed Filipino migrant domestic workers in Macao, and found that participants who had a good relationship with their employers were willing to compromise and accept working and even living with nanny cameras in their employers' house. The study did not investigate views on smart home devices in depth, but did note the role camera surveillance played in participants' perceptions about living with their employers, and how live-out workers created a safer and more privacy-preserving space for themselves than live-in workers.

A study by Słupska et al. [67] of various privacy concerns for migrant domestic workers in the UK found that smart-home surveillance by employers was not the highest concern for most participants. However, some participants who had experienced abusive behavior from employers were more worried about smart home devices, because they could be used to enforce control of workers' actions and behaviors even in their off time.

Finally, Foster [28] describes the only prior U.S. study we are aware of on domestic workers and smart home cameras. It did not publish full results, but the surveys did find that disclosure was highly important and impacted trust. Szakolczai [71] examined spycam product reviews and a Reddit thread about spying on domestic workers, and identified tensions between surveillers' and targets' conceptions of privacy.

Studies of cameras have mostly focused on domestic workers as objects of surveillance; a different take is provided by a speculative design study by Bartle et al. [15] about interactive voice assistants to help home health aides track and manage care. Though it mainly focused on feature design, the work notes that participants wanted control of what information about them would be visible to their employers at care agencies.

Although we are focusing on smart *home* devices in this article, it is worth noting that—unsurprisingly, for a case where the home is a workplace—the issues that arose in our interviews echo some concerns raised in prior work about surveillance by IoT devices in the workplace, particularly with regard to care work in institutional settings. For example, in a survey with care facility administrators, Berridge et al. [19] found that many believed in-room cameras would help them deter and detect abuse and keep staff more mindful, but a smaller—but still sizable—minority thought that camera surveillance would lower morale and decrease trust between them and their employees. Caregivers in interviews by Sugihara et al. [69] were concerned about not feeling free to take proper breaks if they were monitored.

These issues also reflect broader concerns about how the proliferation of cameras and similar IoT devices may replicate or intensify existing socio-economic power imbalances and patterns of discrimination (overviews in [24, 79]).

### 2.7 Positioning the Present Article Relative to Prior Work

Although prior work has explored the views of device owners and primary users as well as bystanders (as a broad category) on smart home privacy, our study is the first in the U.S. that qualitatively compares the views of *domestic childcare workers*, as a specific bystander group in multi-user smart homes, with the views of parents who employ domestic childcare workers. At the same time, we explore, compare, and contrast the views of domestic childcare workers and parents who employ such workers on different smart home devices, as well as investigate how different device purposes and uses affect views.

## 3 Methods

We conducted semi-structured interviews with U.S. participants in 2019, including 25 nannies, au pairs, and babysitters, as well as 16 parents who employed nannies or au pairs.

To develop the study design and interview protocols, we surveyed academic literature on user and bystander perspectives on smart homes (see Section 2), and reviewed online content posted by and for nannies (or domestic workers in general) as well as content by and for employers of domestic workers, in particular in the r/Nanny forum on Reddit (a mini-analysis of r/Nanny posts about smart home devices is in Bernd et al. [18]).[3] Before conducting our study, we obtained ethical clearance from the UC Berkeley IRB.

*Relationship to Prior Papers by the Authors.* We previously published brief preliminary findings based on interviewers' notes about both nanny and parent interviews as a work-in-progress paper [17]. We then published a full paper exploring how smart home cameras affect and reflect power dynamics in nannies' relationships with their employers [16], based only on the subset of questions about cameras in the dataset of nanny interviews; additional information on methodology may be found there. The present article adds an analysis of questions about other types of devices in the nanny interviews (using the same set of transcripts, but looking at all devices discussed), as well as adding an analysis of the parent interview dataset for comparison.

### 3.1 Interviews with Nannies

*Recruitment.* We advertised our study targeting nanny-specific or nannies-and-parents communities online, e.g., Reddit and Facebook, distributed flyers in public spaces (e.g., cafes, schools, and playgrounds), and used snowball sampling.

We screened nannies to confirm their job experience and ask whether they had experience working with smart home devices, but did not exclude nannies who did not have such experience. We also checked during screening to make sure none of the nanny and parent participants were each other's employee/employer, so that participants would not feel constrained in their answers nor be concerned about confidentiality breaches. (Recruitment and screening for both participant groups was simultaneous, though interviews were not.)

*Interview Procedure.* We conducted a pilot to pre-test our protocol for clarity and prioritize questions. In total, we interviewed 26 participants: 24 by phone or video chat and 2 in-person. The two interviewers frequently compared notes on the issues and viewpoints arising, and discussed after every few interviews whether data saturation had been reached, or whether to continue. Most interviews took between 60 and 90 minutes, and participants were compensated with $50.

Prior to the interviews, we provided information about the study and obtained informed consent. Then, after asking participants to share some general views on nannying, we asked a series of specific questions about smart home cameras, then parallel series of questions about smart speakers, smart TVs, and other devices they had experienced (including location trackers if we had time). Questions covered experiences working with each type of device, expectations about their use and disclosure, discussions they'd had with employers about devices, privacy attitudes and concerns, and what privacy protections and controls they wanted. If participants had not experienced particular devices or situations (e.g., smart TVs with sensor-based features), we probed their views via hypotheticals.

[3] Materials for both sets of interviews, including recruitment flyers, screeners, interview protocols, and exit questionnaires, can be found at: https://bit.ly/3VhAyIM

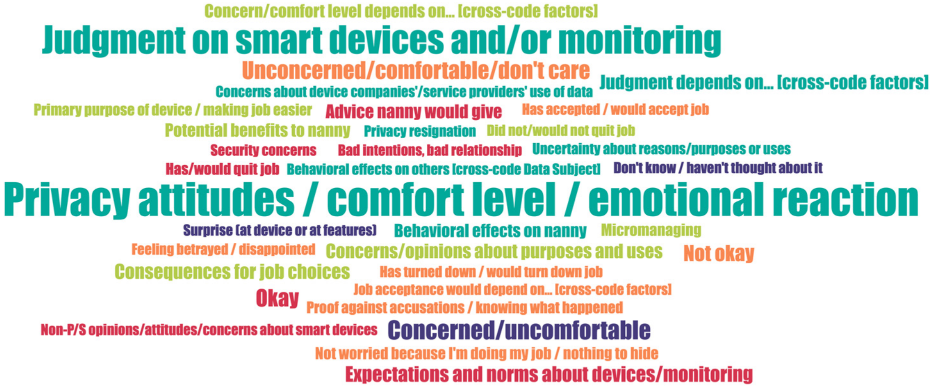

Fig. 1. Word cloud of some codes and subcodes in the "Nannies' Perspectives on Devices/Monitoring" theme group in our codebook, with larger text indicating more frequently applied codes. (Cloud generated by MaxQDA.)

Finally, participants provided information about their demographics, technical background, current employment status, career trajectories, and exposure to smart home devices (i.e., what devices they and their employers owned), by filling out an online exit questionnaire.

*Data Analysis.* Interviews were professionally transcribed. One transcript was discarded, as a language barrier made it difficult to interpret, leaving 25 in the dataset.

To analyze, first, three researchers inductively coded one test transcript each (three in total). Each researcher developed their own coding frame. The researchers then met to discuss our frames, develop code definitions, and merge the frames into one. An additional researcher then joined the team. Using the merged frame, the four researchers independently coded two additional transcripts (the same ones as each other). They then met to resolve disagreements and adjust coding policy.[4] We then divided all 25 transcripts into batches, and each transcript was coded by two researchers. As we coded the first few transcripts, we continued discussions to resolve remaining disagreements and confirm code saturation, then finalized the coding frame for the remainder (see Figure 1 for a subset of codes).[5]

After finishing coding, all researchers discussed and refined the overarching themes based on the coded excerpts, examining relationships between themes to develop a picture of what factors influenced nannies' views on different devices.

### 3.2 Interviews with Parents Who Employ Nannies

As the parent interviews were intended as a point of comparison with nannies' views, and a cross-check on nannies' perceptions about their employers' device use and views, we conducted shorter interviews, and approached analysis differently.

*Recruitment.* We began with similar recruitment methods to the nanny interviews, along with mailing lists, but did not get enough potential participants; we therefore expanded our pool using the Prolific recruitment platform.

[4] We calculated agreement rates while testing the codebooks for both participant groups, to ensure that the four researchers applied codes similarly. However, these numbers were used only for testing, as our findings do not make quantitative claims [see 57].

[5] Codebooks for the thematic analysis for both studies can be found at: https://bit.ly/4cCz6HS.

Screening was also similar, but (as we were interested mainly in cross-checking perceptions) we excluded potential participants who did not have any smart home devices.

*Interview Procedure.* All parent participants were interviewed by phone or video chat. Piloting and approach to data saturation were similar to nanny interviews. However, both because the interview protocol was shorter *a priori*, and because parent participants were less likely to expand at length on their opinions (often having thought about it less), parent interviews were shorter, lasting between 30 and 45 minutes. We therefore reached data saturation with only 16 participants. Parent participants were compensated $25.

Interview procedures and topics were similar to those for nannies. We asked participants some general questions about having a nanny, then asked sets of questions about smart home cameras and other devices. Questions about each device type covered adoption processes, privacy attitudes and concerns, and (at least for cameras) privacy protections. We explored parents' approaches to device disclosure, discussions, and use with respect to their nanny, as well as their expectations about and views on use and disclosure of devices in other situations.

*Data Analysis.* We took a deductive approach to the parent interviews, structuring analysis around areas for comparison we identified after completing our inductive analysis of the nanny interviews. We therefore began with the coding frame we had used for the nanny interviews, modified codes to reflect the different point of view, and simplified and reorganized the codebook to capture answers to our RQs about parents.

Two researchers tested the new coding frame on one transcript. After modifying the codebook and coding policies to better reflect the particularities of the parent interviews, we tested it on two more transcripts and then finalized the coding frame. Then all 16 transcripts were divided among three researchers, with two researchers coding each transcript.

We then discussed and developed answers to our RQs comparing parents' views to those of nannies and cross-checking nannies' assumptions about employers' views and device use.

### 3.3 Limitations

We did not enquire about our participants' immigration status; for a study of this size, we did not believe it was worth the potential discomfort to any undocumented participants. We may therefore have missed potential comparisons between nannies (or parents) with different immigration status. Future quantitative work (see Section 6.4) should investigate this dimension, employing focused strategies to recruit participants (especially domestic workers) with varying immigration statuses, while considering all ethical aspects and mitigating harms.

In addition, recruiting and interviewing only in English may have limited the demographic diversity of the sample (including by immigration status), and/or caused us to miss views and issues specific to non–English fluent participants. Future study materials should include additional languages.

Combining online recruitment (including in some groups specific to big-tech cities) with flyering in the San Francisco Bay Area may have attracted a disproportionately tech-savvy sample, and, for nannies, a sample whose employers were more likely to have smart home devices. Finally, richer context might have been provided by interviewing employers and employees of each other, were it possible to do so without incurring the scientific and ethical risks mentioned in Section 3.1.

## 4 Participants

*Nanny Participant Demographics.* All nanny participants were female, aged between 19 and 55; the median age was 30. At the time of our interviews, 76% were nannies or combined nannying with household management, 12% were professional babysitters, and 8% were au pairs. The au pairs lived with their employers, but none of the other participants did at the time of the interviews. In our sample, 64% were full-time employees and 32% worked part-time as nannies (usually with another job, or they were students).

More information about nanny participants' demographic characteristics, job situations, career trajectory, and device exposure can be found in Appendix A.1, which also shows how our sample is representative of domestic childcare workers in the U.S.

*Parent Participant Demographics.* Among our parent participants, 44% were female and 56% were male. Their ages ranged from 25 to 40, with a median of 33. At the time of our interviews, 94% employed nannies and 6% (one participant) employed an au pair. Most had one or two children being taken care of by the nanny; one had three.

More information about parent participants' demographic characteristics, childcare situation, and device ownership can be found in Appendix A.2.

## 5 Findings

This section presents and compares participants' experiences with several different types of smart home devices in nanny workplaces, views on how those devices affect privacy, and factors that influence those views. In Section 5.1, we cover views on nannying. We describe participants' experiences with and views on *smart home cameras* in Section 5.2; *location trackers* in Section 5.3; and *smart speakers, smart TVs, and other smart home devices* in Section 5.4.[6] Section 5.5 compares participants' views on the different devices. Within each subsection, we describe perspectives from nanny participants and parent participants separately, then Sections 5.2.9 and 5.4.5 compare the two groups.

### 5.1 Views on Nannying

*Nannies' Perspectives.* We began interviews by asking our nanny participants about general pros and cons of the job. Many mentioned that nannying provided more autonomy than other jobs, and most found it rewarding.[7] Nanny participants said that good employer–employee relationships required trust, respect, and willingness to communicate (e.g., about employment terms or how children should be raised):

> Both for me and for the family, we both have to trust each other. And that's not as important in a lot of other positions. (N20)

Several pointed out that nannies may have trouble maintaining professional boundaries when working in someone's home and taking care of their child. Some found it difficult to advocate for themselves:

> All of the different characteristics of fair employment are really on you, and it's a very vulnerable position to be in, especially because you're in somebody else's house. The power dynamics are really different. (N4)

At the same time, some nanny participants believed that nannying was not always valued by society:

[6] We present participants' views on smart home devices other than cameras in one combined subsection because participants had quite similar views on them, based on their having a narrow range of purposes of use, whereas cameras had a greater range of purposes, and thus inspired a greater range of views.

[7] We did not attempt to count the number of participants who expressed a given view in this qualitative study. We instead use words like *most*, *many*, *some*, or *a few* when presenting such findings, to provide a rough idea of prevalence [see 56].

> The most frustrating part about being a nanny is other people not taking it seriously. This is my current career. (N3)

*Parents' Perspectives.* Like nanny participants, most parent participants said that they found open, direct, and frequent communication, as well as mutual trust and respect, key to a good parent–nanny relationship:

> I think communication and being transparent with your needs and what specifically you're looking for from her is something that is crucial in maintaining a good relationship. (P14)

## 5.2 Views on Smart Home Cameras

Here we describe participants' experiences with and attitudes toward smart home cameras, and identify factors that affected their perspectives, behaviors, and choices.

### *5.2.1 Camera Exposure and Expectations.*

*Nannies' Perspectives.* Of 25 nanny participants, 22 had worked with some sort of camera inside an employer's home at some point, and usually more than one per dwelling.[8] In most cases, the cameras had been deployed before the nannies started working there. Some of the cameras collected audio as well as video, but several nanny participants were uncertain about audio collection. All nanny participants had worked mostly with cameras that produced a live feed (usually over the Internet) that could be accessed by employers in real time, often using another device (regardless of whether that feed was recorded). A few had worked with cameras that recorded as well (either to a hard drive or the cloud), but again, many were not sure. Most cameras collected data continuously, but some were motion-triggered.

Nanny participants rarely knew how frequently their employers actually checked the feed, but their guesses ranged from occasional spot checks to continuous watching. Some nanny participants themselves had access to the feed, especially in the case of baby monitors, to check in on kids during their nap time.

Most nanny participants viewed the presence and use of cameras in their employers' houses as normal and, as a result, a reasonable expectation:

> Probably on the first day, I would assume that people have cameras now. I haven't worked in a home probably in at least eight years that didn't have a camera in the nursery. It's highly unusual to work for families without cameras. (N4)

*Employers' Perspectives.* Out of 16 parent participants, all had at least one camera outside their home, and 15 had at least one inside.[9] Most cameras collected both video and audio. Most parent participants had at least one Internet-connected camera providing a continuous live feed. Some also recorded, either to a hard drive/memory card, to a cloud service, or both. Some parent participants were not sure whether or for how long companies retained data.

The frequency with which parent participants checked camera footage when nannies were there varied from several times a day to once a week, and often depended on the reasoning behind installing cameras (discussed further in Section 5.2.4). While it was common for parent participants to have cameras on all the time, some turned them off when they themselves were home. Some gave their nanny temporary access to the feed to check in on children; a few also gave access to others outside the household, such as their own parents.

[8] More information about nanny participants' camera exposure, in both their employers' homes and their own, can be found in Appendix A.1.

[9] More information about parent participants' camera devices can be found in Appendix A.2.

The majority of parent participants viewed use of cameras as common generally, and as a typical or at least reasonable work condition for nannies. Even the participant who did not himself have an indoor camera viewed it as expectable:

> They're probably gonna be recorded at some point wherever they're at, and they should be prepared for that. (P18)

Most parents who owned cameras indoors said they did not mind cameras at their own workplaces, and a few described it as a normal workplace expectation:

> There's always cameras. You know, [my employers] are not doing anything illegal, we're all working. (P17)

#### *5.2.2 Disclosure of and Discussions about Cameras.*

*Nannies' Perspectives.* Although many nanny participants expected cameras in their workplace, most viewed it as desirable (or even ethically imperative) for employers to inform nannies about the existence of cameras, especially inside the house—and preferably to initiate the discussion, either at time of hire or when any new cameras were deployed. To many nanny participants, lack of disclosure was perceived as breaching trust or signaling a lack of respect—which was especially problematic for a high-trust, in-home caregiving job (see Section 5.1), leading to a feeling of unsafety and job insecurity as well as privacy invasion. (See Bernd et al. [16] for a detailed discussion of relationship implications of camera disclosure.)

However, nanny participants had mixed expectations about whether employers were *likely* to disclose cameras. Some nanny participants sympathized with why first-time parents or employers who had had a negative experience with previous nannies felt a need to hide cameras—even if they would have preferred disclosure:

> I also understand why some families feel nervous about care providers, and probably feel justified at not saying something. [...] I do think that everybody should disclose if they had a camera. [...] [But] if they've had previous abuse from a care provider, absolutely, I can understand why they wouldn't want to tell somebody. (N4)

Although nannies did not expect to influence whether a given employer would use cameras, several participants believed they had the right to initiate the discussion and ask employers about the presence and use of cameras, especially before accepting a job offer. However, some felt uncomfortable doing so, either out of general hesitancy to jeopardize harmony by advocating for themselves (see Section 5.1), or specifically out of fear that parents would find such a question suspicious:

> I feel like it's kind of sensitive. I don't want to make it seem like I don't want to be videotaped, like I'm scared. (N26)

A few nanny participants said it did not matter whether employers disclosed cameras because a good nanny should behave the same either way (see Section 5.2.6); others said they always assumed there might be cameras even if none were disclosed.

Several nanny participants discovered indoor cameras *during their employment* that their employers had not informed them about (due to either intentionally withholding the information, forgetting to mention it, or assuming they were obvious). In such cases, some nanny participants would ask employers about the reasons for non-disclosure; some would consider leaving their job (see Section 5.2.6).

A couple of nanny participants felt that employers did not need to disclose cameras if they were very obvious, but most said they would still prefer an explicit acknowledgment. Some nanny participants also mentioned that they would prefer their employers to initiate discussions about not only the presence, use, and location of cameras but also their purpose of use and frequency of checking the feed, preferably before they started the job. However, few had employers who had done so:

> I was almost more comfortable with the cameras in Family [1], because they, like, from the get-go [...] let me know that they used nanny cams and they would check in pretty regularly [...]. But with Family [2], [...] I don't really know if they check in on me, or if it's like just at night when the kids are sleeping. I'm not sure. So, that's what kind of makes me uncomfortable is when I'm unsure. (N26)

Several nanny participants also mentioned they would want to know whether a camera recorded audio, for example, so they would know to avoid private phone conversations, though at least one held the opposing view:

> I don't want to know [about audio], because I don't want to be self-conscious. I want to do my job without thought of the camera. (N12)

Most nanny participants were less concerned about disclosure of details such as data sharing, storage, and deletion, but some did say they would like to know.

*Employers' Perspectives.* Most parent participants believed they should disclose cameras to the nanny, at least if they were inside the house, though fewer had actually done so. Those who did commonly cited a desire to respect the nanny's privacy and trust:

> For respecting her as a professional, the fact that she deserves to know that there are cameras around the house. (P5)

Some were concerned about legal consequences:

> You'd probably want to alert them because otherwise they might be able to get a court case against you for spying on them, even. (P6)

When asked about cameras in their own workplaces, several parent participants emphasized this aspect as well:

> If, obviously, we weren't informed, then that's not ethically and I don't believe legally allowed. (P16)

Only one parent participant had specifically decided to not disclose cameras, to avoid compromising her child's safety. More believed that disclosing cameras was the best way to prevent abuse:

> I would much rather detour [sic] something nefarious happening than being able to review the camera later and find out that it happened after the fact. (P2)

However, while very few deliberately hid their cameras, a number of parent participants had not actually disclosed cameras. In some cases, they thought the cameras were in a visible enough location. In others, they assumed the nanny was already comfortable with cameras, and therefore would not consider them a breach of privacy whether disclosed or not. In particular, parents who already had cameras assumed nannies would not care about additional ones:

> Since she was already fine with having the first [camera], we did install the second one without even notifying her. [...] She did not raise any concerns about it. So it seemed fine to me. (P14)

Several parent participants mentioned they would be less likely to disclose cameras to an occasional babysitter, either because they didn't consider it important for a brief exposure, or deliberately because they did not have an established trust relationship.

Even when they disclosed, not many parent participants had discussed any aspects of camera use with their nannies beyond their existence and location. Many said that their nannies did not ask any further questions when camera usage was disclosed, and therefore they assumed that nannies did not have any. When parent participants did receive questions, for example, about camera configuration or function, they did not consider it to be cause for suspicion, and most did not have qualms about answering.

However, even if they said they were willing to answer questions, parent participants commonly felt nannies should not have influence on parents' decision whether to use cameras in the first place, as their right to know what was going on in their own house came before any privacy concerns the nanny might have.

#### *5.2.3 Perceived Benefits of Cameras to Nannies.*

*Nannies' Perspectives.* Most nanny participants balanced any concerns they had about cameras against potential benefits. Some endorsed cameras' usefulness in home security (see Section 5.2.4). Some believed that cameras could encourage better performance (see Section 5.2.6), or demonstrate to parents that the nanny was good at the job:

> They could know what you are doing, and if you are doing a good job, well, they will know that too. (N5)

Further, many nanny participants believed that if something went wrong and that they were not at fault (e.g., a child getting injured), cameras could "give, like, the whole context of anything that was happening" (N36) and serve as proof against potential accusations. This protection could be traded off against comfort working with cameras, as in this comparison between jobs with and without cameras:

> I definitely feel more relaxed in Family [X]'s house, but in Family [Y]'s house, I do feel more protected if something were to happen to the little ones. (N35)

In particular, a few nannies opined that the potential for audio data to clarify what happened could be worth the privacy downsides of capturing the additional data stream.

Some nanny participants also mentioned how cameras could aid them in their job if they had access to check in on children—and some opined that cameras were not particularly beneficial if the nanny couldn't use them:

> If they're not giving me a baby monitor to look at, and there's a video camera in there just, like, recording and seeing everything, and none of it is to aid me as the child carer, then [...] that's not helpful, that's not productive. It's just spying. (N7)

*Employers' Perspectives.* For the most part, parent participants listed the same potential benefits that nanny participants did, such as increased motivation to perform better on the job, demonstrating that the nanny is taking good care of the children, or providing evidence against accusations of negligence or wrongdoing:

> I would hate to be a nanny for someone and their seven-year-old said, you know, that I touched them inappropriately, and I have no way of defending myself because it's my word against theirs. But with the nanny cam, I think it protects the nanny just as much as it protects the child. (P7)

One parent participant said the camera could benefit the nanny by facilitating reminders and instructions:

> [If] I saw her maybe not cutting up the grapes or something, I could communicate through that and say, "Oh, don't forget to cut up the grapes." And so that could maybe be a helpful reminder to her. (P2)

While some also gave nannies access to check in on children, none of the parent participants had thought about this benefit when deciding to buy the camera.

*5.2.4 Attitudes about Cameras and Factors Affecting Attitudes, with a Focus on Purposes of Use. Nannies' Perspectives.* Nanny participants' acceptance of and privacy attitudes toward cameras ranged widely and were influenced by a number of factors, including expectations and social norms (see Section 5.2.1), disclosure (see Section 5.2.2), purpose of use, when and where employers installed cameras, and frequency of checking feeds.

In some cases, there was a difference between how nanny participants judged the existence and use of cameras and their personal feelings of (dis)comfort. For example, to some nannies, cameras were okay in theory, but they were uncomfortable with cameras in practice:

> I understand what they're there for. I understand it's a safety thing, I get it. So, I'm not anti-camera. I just know I wouldn't like to be recorded. (N33)

Conversely, other nanny participants did not approve of cameras in principle, but were comfortable with them in practice because they did not anticipate negative consequences—or due to privacy resignation.

As we noted above, many nanny participants were more accepting of cameras if employers disclosed them, building trust and rapport:

> If the parents are honest and upfront about the cameras, generally, I forget about them. [...] It feels like, Oh, you know, we're both on the same page about this. (N7)

To some nanny participants, cameras were more acceptable in the beginning of the employer–employee relationship, but less so when employers decided to install them after the nanny had been working for them for a while, due to a perceived lack or breach of trust.

Nanny participants noted that cameras were multi-purpose devices, and their attitudes tended to be closely tied to purpose of use—and could change if that use changed. For example, many nanny participants thought their employers used their cameras mainly to ensure the safety and security of the household (e.g., against external threats like burglary), which most viewed as unproblematic. A number of nanny participants mentioned employers using cameras to check in on household members, including their children and pets:

> Originally they got it to check on their dog during the day, and watch what he was doing while they were at work. And then when they had a child, they decided to keep it and use it to monitor their child. (N3)

Nanny participants tended to be sympathetic to employers using cameras as a way of capturing memories of their kids, or as a way of feeling connected with their kids and being involved in parenting:

> If [...] the parents miss the kid's first steps or the kid's saying whatever, they should be able to have that milestone, right? That's why you should have [cameras]. (N16)

Some nanny participants mentioned that employers used cameras to communicate with or manage nannies:

> Most families like having [the Nest camera]. They can see if their kid is sleeping, they can sign in remotely and kind of and check in, see how the day is going, and also make sure their schedule is sort of being kept. (N4)

However, a number of nanny participants found that employers could overuse that function of cameras (see Section 5.2.5):

> She was just kinda constantly viewing the feed, and trying to tell me how to, you know, care for her child while she was still in the same house, but supposedly working at the same time. It just was like, you have that much time to sit and stare, come on. (N7)

Location was another important factor. Even nanny participants who accepted cameras (including hidden ones) had some common limits; e.g., cameras in private places like bathrooms or nannies' bedrooms were universally unacceptable. (However, none of the nannies in our sample had experienced this, that they knew of.)

Expectations about and attitudes toward cameras in other locations generally depended on the purpose associated with that location. They most frequently noticed—and expected—cameras in kids' rooms or playrooms, to check on the children. Nanny participants believed cameras in entryways or porches were primarily for home security—i.e., for monitoring outsiders, not nannies. In combination with their limited exposure (only when exiting or entering the house), porch and doorbell cameras therefore did not tend to evoke the same levels of discomfort as indoor cameras. In fact, many nanny participants seemed to think about outdoor cameras more similarly to how they thought about other types of smart home devices, and less similarly to indoor cameras (see Section 5.5.1).

Cameras in common living spaces like kitchens were also frequent. Nanny participants' attitudes about such cameras were more varied, largely depending on whether the location was relevant to the employers' stated purpose for them—and if employers had not told them the purpose of the camera, they were less able to infer it than with cameras in other locations, so felt more uncertain.

Interestingly, some nanny participants had rather different attitudes about initial camera data collection (with parents having access) vs. data re-sharing, especially on social media:

> *[I: If you found out that the family has actually shared something with you only [without the kids in the video], would you consider leaving the job?]* [...] I just feel like that's really kind of an invasion of privacy. Again, I really don't mind being on camera just so they can make sure their kids are safe and happy. But that's just like a weird way of using their home and like, you know, I just would not feel comfortable working there anymore. (N26)

*Employers' Perspectives.* As mentioned above, many parent participants assumed nannies did not have privacy concerns about cameras because they hadn't mentioned any (Section 5.2.2), or because the parents saw it as very normal for nannies to be monitored at work (Section 5.2.1).

Most parent participants themselves did not have concerns about nannies' privacy, and many said they had not considered it in their decision to use cameras. When they had thought about it, some thought cameras had little or no impact on nannies' privacy; others viewed it as a reasonable tradeoff for having a high-trust job:

> Since she would be, you know, occupying my home for the time she's employed, her privacy is, she basically agrees to temporarily suspend that [...] during working hours. (P5)

Our parent participants' reasons for having cameras generally aligned with our nanny participants' assumptions about their own employers' reasons, though parent participants tended to draw a stronger distinction between checking on the children vs. the nanny. Many parents said they used cameras for checking in on their children or pets—but several parents emphasized that they did *not* view checking on children as synonymous with monitoring the nanny:

> Because my main purpose in having it is more just my ability to check in on my daughter, and not really to watch what the nanny is doing. (P4)

However, several parent participants said they installed cameras at least in part to manage the nanny, and to see for themselves that she was "doing her job" (P14). In such cases, participants often checked cameras daily or almost daily—though few had ever discussed with nannies anything they saw on camera. Beyond supervision, a few parent participants said they installed cameras to deter, or at least discover, misbehavior or abuse (see Section 5.2.2):

> I don't think every person is bad. However, the reality is, you are still a stranger to me and to my daughter, and I just always want to make sure that she is safe. (P7)

Meanwhile, many parent participants used cameras for home safety and security, especially outdoor cameras. Some such participants also used the cameras to monitor the nanny, but others were at pains to point out that they did not, relying rather on their judgment of the nanny's trustworthiness:

> I want to clarify that these devices were not installed for the purpose of checking in on the nanny. I was technically able to do that, but I also really trusted her completely. And if I didn't have those devices, I wouldn't be nervous. (P19)

No parent participant had ever installed a camera in a bathroom, and the general consensus was that doing so would be very inappropriate.

When it came to their own privacy or that of their children, most parent participants who had cameras were not especially concerned. However, some said their views depended on whether data were recorded (as opposed to only live-streamed), whether data were stored in the cloud, and camera location (exterior cameras and cameras in children's rooms raised less concern than cameras in adults' bedrooms). Even parents who expressed some concern might not find it very pressing where the data recipient was abstract or unknown:

> I'm always kind of wary just about [...] the data that our devices in general are always collecting on us. [But] it's hard for me to [...] put a face to someone, I guess, that would be using this data or stealing this data for some nefarious reason. (P9)

Some viewed the privacy downsides for themselves as a necessary cost in exchange for peace of mind: "I like being able to check in, and so that's sort of the trade-off I'm willing to make." (P4) A few parent participants mentioned being less concerned about data of their children because they viewed it as particularly low-value or low-risk: "It's kids in a crib. [...] A, who would want that footage, and B, what could possibly go wrong?" (P17)

#### 5.2.5 Privacy Concerns about Cameras.

*Nannies' Perspectives.* We found that most nanny participants had much stronger privacy concerns about cameras, at least indoor cameras, than other smart home devices. Although many participants were concerned about being watched, they often felt they could not challenge the current state of affairs, due mainly to social norms and power imbalances (see Section 5.1).

*Concerns about Hidden Cameras or Incomplete Knowledge.* Most nanny participants were concerned about hidden cameras (see Section 5.2.2); this was one of the most frequently mentioned concerns. For those who had the strongest privacy concerns about cameras, undisclosed cameras could lead to feelings of being betrayed, violated, untrusted, hurt, upset, and/or disrespected (see Section 5.2.2). Nanny participants were also concerned about hidden cameras because they would have no means of controlling what cameras captured, especially embarrassing behaviors or private calls. Some worried that their lack of knowledge could facilitate creepy behavior or abuse (see Bernd et al. [16]).

*Concerns about Hidden or Uncertain Purposes and Uses.* Concerns about cameras most often arose specifically from being uncertain about purposes and uses:

> There was a time where I took a leave from work, and I came back. And that's when one of the cameras [was] there. So I did find myself wondering, you know, are they checking in more because I took time off, and now I'm back. (N37)

Even if employers disclosed cameras to nanny participants, a mismatch between what employers said about why they had cameras and how cameras appeared to be actually used prompted concerns, and some said they might assume parents had deliberately hidden their main purpose in having cameras:

> I almost feel like if someone has cameras for security, but then they kind of use it to spy on you, I almost feel like that's worse just because it's not completely honest. (N26)

At worst, hidden cameras, or incomplete disclosures of cameras' capabilities, could be used by employers to help "catch out" or "frame" nannies:

> *[I: Do [nannies] need to know whether the devices are collecting audio only, video only? Or, like, when the device is on, when the device is off, for example?]* Yeah, I think they should know [...] anything possible to know about it, I think you should be aware. Just seems tricky to me. Just seems shady to me, [...] it's almost like you're trying to catch someone in something. (N34)

*Concerns about Micromanagement.* Many nanny participants' privacy concerns about cameras revolved around how cameras reflected or impacted their work relationships with their employers (see Bernd et al. [16] for detailed discussion of cameras and relationships). In particular, they could be used to closely supervise and micromanage nannies:

> That's actually a reason why I left my previous nanny family. They would constantly check the cameras and text me on, like, certain things that they would do differently or things I was doing wrong in their eyes. (N35)

Micromanaging also made some nanny participants feel they were not seen as subjects in their own right:

> Parents who micromanage are awful, and that parents who use cameras improperly often see nannies as human robots. (N3)

*Concerns about Job Insecurity.* Many nanny participants linked cameras with their job security, e.g., if a camera captured their mistakes. In fact, a few nanny participants either had been fired, or a nanny they knew was fired, because of what employers said they had seen on camera:

> They fired me because they said that I used my phone too much. They said, "We looked at the cameras and saw that you used your phone for about ten minutes while [child] was playing on the floor." (N27)

However, N27 believed the real reason was religious discrimination, and the camera footage was an excuse.

*Concerns about Data Sharing by Employers.* Nanny participants had varied opinions regarding parents sharing camera footage on social media, mainly depending on employers' intentions and purposes in sharing:

> I think if it was footage of me or audio of me that they were sharing, I would want to know about it. And again, I think I would want to know their reasoning. If it's like malicious, like, "Oh my god, look. [N37]'s face is weird." (N37)

A few nanny participants found even benign social media sharing to be "super crossing the line" (N18).

*Concerns about Camera Manufacturers.* Some nanny participants expressed concerns about what manufacturers might do with camera data, especially of children, including whether they would sell it to third parties. Some were concerned that manufacturers were not transparent about data handling and did not like being unsure of what data could be used for:

> I think companies should be more transparent. Yeah. Companies in general are just profit, like, mongrels. You know, like they're just here trying to eat everything. (N8)

Yet, camera data handling by manufacturers and third parties was often viewed as a secondary concern among nanny participants, compared with data handling by employers:

> I would wanna know what type of camera it is, who has access to it, where is it being streamed to. But the main thing I wanna know is: Do you have cameras and where. [...] The other things are secondary. (N7)

Only a couple of nanny participants had worked with smart home assistants that had integrated cameras (Facebook Portals). In both cases, their employers also had cameras that they used for checking on the kids and nanny, which those participants were comfortable with—so those participants were less comfortable with the Portals, citing their uncertainty about what they captured, who had access, and how data could be used:

> [The Portal] just felt, like, more invasive to me cause I feel like maybe someone other than the family is watching me. (N37)

*Employers' Perspectives.* As we noted in Section 5.2.4, most parent participants did not have strong concerns about data collected by smart cameras, and many had not thought about it, either on their own behalf or that of their children or nanny.

*Concerns about Nannies' Concerns.* Some parent participants recognized nannies' potential privacy concerns; while this did not influence their choices about *whether* to get a device or what privacy protections to use, in some cases this recognition did spur conversations around cameras.

With the exception of a few, most parent participants found deliberately hidden cameras unacceptable. Some commented that hidden cameras would be a violation of the nanny's privacy or (as discussed in Section 5.2.2) a sign of disrespect, and acknowledged that nannies could worry about hidden cameras:

> Her privacy, like we wanted to care about that. [...] We're not camouflaging the cameras, just like out there, it will be visible, so it's fine. But then before she feels like privacy is not being considered for such decision, we wanted to bring up the topic. (P14)

Several parent participants acknowledged that the nanny could worry about the cameras being used to spy or micromanage, and said they had tried to forestall such concerns:

> We talked over it, like, if our nanny feels comfortable, and she was okay with it. We just wanted to make sure that it didn't feel intrusive. [...] We don't want to spy on any conversations or anything like that she might have. (P16)

Most parent participants stated that they would not consider sharing camera footage that had the nanny in it on social media, citing not being able to control or know exactly who would access the data. However, many thought it was more acceptable to share footage with specific people they knew, such as close relatives.

*General Privacy Concerns.* When asked, most parent participants said they had not considered household members' privacy, or had not considered it extensively, when deciding to get a camera. A few did mention concerns about manufacturers'/service providers' handling and use of data, or (usually stronger) concerns about hackers. The parent participant who did not have an indoor camera cited security as a serious concern, including the manufacturer's security practices:

> I don't know where [the data storage facility] is located, what kind of rules and regulations they have there, what kind of policies they have for security. (P18)

A few parent participants had considered privacy and data protection in their purchases, and said they were not very concerned because they'd chosen brands where the data were under their control:

> Since the data is stored and monitored and controlled by us in the camera chip, it was not such a big issue for me. (P14)

One participant explicitly acknowledged the asymmetry in making decisions about others' privacy, but did not consider it very concerning because, in her judgment, the privacy risk was not large:

> *[I: Did you think about privacy? Your privacy, your child's privacy, and the nanny's privacy? [...]]* A little bit, yeah, but it's my house, so, that's my decision to do that, and I take that privacy risk, I guess. But I don't feel like it's a lot. Because I don't have the whole house rigged for outsiders to look at. (P15)

*(Lack of) Concerns about Nannies' Effects on Parents' Privacy.* Parent participants who had given nannies access to their cameras did not tend to be concerned about impacts on their own privacy, especially if the feed could not be accessed from outside the house. Parent participants who had *not* given nannies data access did not tend to cite privacy concerns for why they hadn't done so (except in one case where camera access was tied to their whole Google account); they simply did not think it was necessary/useful.

#### *5.2.6 Cameras' Impact on Behavior.*

*Nannies' Perspectives.* We found that cameras affected the behavior of our nanny participants in different ways. Many employed strategies to avoid being observed by cameras in common areas. Nanny participants particularly tried to avoid cameras during non-work related activities (e.g., taking a break) or while doing personal things (e.g., changing clothes):

> I might go off camera if I want to, like, lift a bag of potato chips and just pour the last little bits into my mouth. Or just do something really stupid. (N12)

Some were self-conscious of their behavior even when interacting with the kids:

> I just find it harder to like be silly or, you know, just be and play with the kids in a normal way. I just kind of feel a little bit tense and like my attention is focused on the fact that I'm being watched. (N6)

Some referred to this feeling of awkwardness as "being on stage" (N27) or "putting on a show" (N16).

Several nanny participants thought that being conscious of cameras helped them control their emotions and could result in better job performance, but many said that they would deliver the best care possible without the need for cameras:

> I'm the same always, you know. I'm treat the girls just in the same way when [the cameras] are present. (N15)

*Employers' Perspectives.* Several parent participants speculated that cameras could encourage nannies to self-monitor and improve their job performance:

> They can sort of subconsciously correct their behavior now that they know they have the potential for being recorded [or] being watched. (P9)

However, most parent participants—including some of those who said hypothetically the nanny's behavior could change—did not actually notice substantial impacts in practice. Several said they felt the nanny's behavior *should* remain consistent whether or not they could be monitored:

> If it does affect the behavior then there would be other questions as well. I mean I ideally would want [a] relationship with somebody who would feel totally comfortable with our son. (P19)

In terms of their own behavior, some noted that they took protective measures such as turning indoor cameras off when they themselves were at home.

#### 5.2.7 Employment Choices Related to Cameras.

*Nannies' Perspectives.* Views on cameras often affected nannies' job acceptance or quitting.

*Quitting a Job.* Some nanny participants had quit, or said they would quit, their job due to various reasons related to cameras, including micromanaging:

> That's actually a reason why I left my previous nanny family. They would constantly check the cameras and text me on, like, certain things that they would do differently or things I was doing wrong in their eyes. (N35)

Further, most nanny participants would quit if they found a hidden camera, or found out that their employers had shared recordings on social media with malicious intent (see Section 5.2.5):

> If it was just an embarrassing video of me, like we all kind of do stuff like blow our nose or eat unattractively, you know, if it was something like that, I think I would just immediately quit. (N26)

Due to feelings of privacy resignation, social norms, or need for employment, a few believed cameras were unavoidable, and they needed to accept working with them, even if they discovered an undisclosed one:

> A lot of different factors are coming to play. One is pay. You know, if they're paying me twenty-five bucks an hour, film me all you want. If you're paying me fifteen bucks an hour, and you're gonna lie about the cameras, then I'm less likely to work for them again. [...] It

> bums me out to say that because I really am genuinely bothered by the use of cameras in homes, but it's become so prevalent, I feel that it's almost taboo to question it. (N7)

*Declining a Job Offer.* A few nanny participants had turned down a job offer because of undisclosed cameras, and several others said they would do so in such a situation:

> One family, I was offered a job [...] and she hadn't been upfront with me about cameras, so I declined because of that. (N7)

But usually camera surveillance was perceived as a catalyst or signal rather than the sole reason for turning down an offer:

> There were cameras in [...] all the shared living areas and I knew I would never feel comfortable, or able to relax, and [...] it felt like starting from a place of distrust. (N6)

(See Bernd et al. [16] for more about camera use and (non)disclosure as an indicator.) Some participants noted they would have different tolerances for short-term babysitting—either more likely to turn down, because it wasn't much money anyway, or more likely to accept, because they didn't have to deal with the family long-term:

> *[I: Would you turn down a one-time babysitting job because parents did not decide to tell you there is a camera inside the house? [...]]* I would probably do one day, but I probably would not return to that family. (N29)

Conversely, a live-in or au pair position occasions more caution, even for someone generally comfortable with cameras:

> *[I: Being offered a position, would [camera] audio be enough to make you reconsider it, or?]* Well, if I don't live there, I don't care. But, I'm going to live, like an au pair, like a nanny, then yeah. [...] I prefer just, like, something video. (N24)

*Employers' Perspectives.* None of the parent participants mentioned a prospective nanny declining or quitting a job because of cameras, that they knew of.

However, most parent participants said that if a prospective nanny objected to being recorded via camera while working, they would not be inclined to offer them the job. They commonly cited reasons such as incompatible views on monitoring, uncertainty about the nanny's reliability, or wondering what the nanny was trying to get away with. A few said they might be open to modifying conditions, but they still had reservations:

> She could cover [the camera] up while she was in the living room [...] But I think it might have been a red flag if she truly didn't want us to see what she was doing. (P19)

No parent participants mentioned having fired a nanny due to something they'd seen on camera.

#### *5.2.8 Camera Protections and Controls.*

*Nannies' Perspectives.* The most common protective measures nannies took were avoiding cameras or modifying their behavior, as mentioned in Section 5.2.6. A few took further measures; most had not, but we asked about what protections they *would like* to implement, or have implemented on their behalf. Most viewed disclosure of cameras (see Section 5.2.2) as a protection, and if so, generally the most important one; other measures are discussed here.

*Device Feedback.* Many nanny participants wanted (non-tamperable) indicators such as lights signaling when cameras were on, and whether they were recording or livestreaming:

> Cameras [...] have settings that can alert you if they're turned on, but the parents are able to turn that off if they'd like to. There's a colored light indicator that shows when they're on, but also that light blinks whenever the cameras are being actively watched somewhere. (N4)

Some mentioned that indicators would make them feel comfortable and allow them to avoid embarrassing behaviors (see Section 5.2.6).

*Device Controls.* Most nanny participants did not have access to cameras' privacy settings and controls nor the ability to view camera data, let alone delete it. Nannies who had access to camera feeds felt more confident, especially being able to use it in their work (see Section 5.2.3). A couple mentioned that they would like their employers to give them access to a shared online account or have their own account, at least with limited capabilities:

> Giving a password and giving agency to nannies over their data and over their information would be amazing. (N7)

Nanny participants viewed it as socially unacceptable and potentially harmful to them to delete or edit data themselves. However, a few suggested that they would like to negotiate with employers about retention policies—but for the most part, nanny participants did not have strong preferences about what privacy settings their employers' cameras should have.

Some nanny participants opined that manufacturers should invest in strong encryption, require strong passwords, or just generally make cameras more secure.

*Contracts.* Many nanny participants had employment contracts, but most did not mention the presence of cameras, let alone other details like number, location, and purposes. Yet (especially after talking with us), most nanny participants wanted their contracts to mention cameras, including number and location, and stipulate that employers were required to disclose them. Some even wanted more details such as data format, retention, and who has access to the data.

*Agencies.* The majority of nanny participants did not work with a nanny agency. Among those who did, few had received any information about or advice on working with cameras, negotiating their inclusion in contacts, nor legal privacy rights—and even fewer thought their employers had received information. Some nanny participants believed that agencies prioritized what employers wanted over nannies' needs:

> I think agencies sometimes do not work well for nanny. They don't tell us a lot of our rights and a lot of the things that we should be entitled to. They cater more to the parent than the nannies. (N10)

Several nanny participants opined that agencies should be more helpful in helping nannies and employers to negotiate expectations and rights around cameras.

*Legal Rights.* Most nanny participants were not aware of their rights with regards to cameras, though some believed there were state-specific laws in the U.S. about consent to audio recording. However, almost all nanny participants believed that there *should* be laws protecting workers' privacy rights and requiring consent to using cameras.

*Employers' Perspectives.* Most parent participants had not done much to protect their own privacy or that of their nannies from smart cameras. However, some mentioned protections they would like for themselves, and what they thought would be appropriate to protect their nannies' privacy (beyond disclosure, discussed in Section 5.2.2).

*Device Feedback.* Most parent participants' cameras had "on" indicators that anyone could see. Some mentioned that it would be useful to also have an indicator for whether the camera was recording or live-streaming data, as well as whether someone was viewing the stream.

*Device Controls.* Some parent participants were more willing than others to give their nanny access to the camera feed to help with childcare, though they were more willing if the camera was in the nursery than in common space. Parents were not willing to let nannies edit nor delete data.

*Contracts.* Only a couple of parent participants had a formal written contract with their nanny, and only one was certain it mentioned cameras.

*Agencies.* No parent participants had ever hired a nanny through an agency. When asked hypothetically, many stated that agencies should facilitate discussions about cameras. Suggestions included informing both parties about camera-related laws, encouraging transparency on the part of employers, and providing demos to nannies explaining how cameras work.

*Legal Rights.* Most parent participants were not aware of their rights nor nannies' rights with regard to cameras, though one mentioned that recordings obtained without consent would be inadmissible in court.

Asked for opinions, many believed it would be unacceptable if a privacy law prohibited people from deploying cameras in their own homes:

> These type of arrangements are just one family that does not have to hire a certain person if they don't want to work with them, and so I think it would be unfair and it would be shortsighted if they have laws that prevented homeowners from having these types of cameras in their home. (P1)

A handful of parent participants said disclosure of cameras to domestic employees should be legally required, but it was less common to opine that consent should be given too. A few also said laws against misuse of camera data could be beneficial, although they did not specify examples of misuse beyond noting that cameras in bathrooms should be illegal.

*5.2.9 Comparison of Nanny and Parent Participants' Views on Cameras.* Here we compare views of nanny and parent participants, and discuss topics where we noticed disagreements or disconnects between views common in each group. Some of these disconnects serve as potential points of intervention (see Section 6.3), especially where members of one group have misconceptions about the likely views of the other.

*Expectations and Preferences about Cameras and Disclosure.* Both nanny and parent participants generally believed that cameras are normal and expectable in homes where nannies work, and that nannies should not have a say in whether cameras were deployed. However, nannies put more emphasis on disclosure as enabling consent, including for new cameras added during their employment.

Most participants in both groups believed that employers *should* disclose cameras, especially indoors. And at the same time, nannies' perception that employers often didn't bother disclosing (even if they weren't intentionally hiding cameras) was matched by the self-reported behavior of our parent sample, many of whom believed employers should disclose but hadn't explicitly done so in practice. However, while there were both nannies and parents who didn't think it necessary to mention reasonably obvious cameras, that position was more common among parent participants.

*Why Nannies Don't Ask about Cameras.* Some parent participants assumed that if nannies did not ask about cameras before beginning a job, they must either expect them as a matter of course or just not care. However, many nannies said they would prefer cameras be disclosed whether or not they were expectable or even obviously placed, as a matter of respect. Their lack of asking was often driven by not wanting to seem suspicious, i.e., worrying that a question about *whether* there were cameras would be interpreted as *fear* that there were. When we asked, most parent participants said they wouldn't find such a question suspicious (though sometimes they expressed uncertainty or mixed feelings), but few had considered that nannies might be concerned about appearing so.

Similarly, parent participants tended to assume that if nannies didn't ask for details about cameras, it's because they didn't care—but instead, again some nannies said it was a fear of seeming suspicious. Many nanny participants wanted at least to know whether the cameras were there to check on them and how often they would be checked—not because they would necessarily object in either case, they simply wanted to know. Most parents said they wouldn't have found questions about details problematic or suspicious, though a couple said they wouldn't want to reveal frequency of checking or whether data were recorded.

*Framing Purposes and Uses.* There was a disconnect in how nannies and parents thought about *checking in* vs. *monitoring*. Some parent participants made a big distinction between using cameras to check in on the kids and make sure they're okay, vs. to see what the nanny was doing. However, nanny participants did not tend to see "making sure the kids are okay" and "making sure the nanny is doing her job" as so distinct, unless their employers were very explicit that they were motivated by missing their kids while at work.

We also found clear disconnects in what nanny vs. parent participants thought of as *communication* vs. *micromanaging* by parents. Some parents had considered this potential issue. But unsurprisingly, parent participants did not tend to judge their own behavior as unnecessarily intrusive or micromanaging, whether or not they specifically made efforts to avoid such behavior. In particular, most parents who had given nannies feedback based on what they saw on camera did not think it was a big deal, framing it as "giving reminders" or, at worst, "correcting mistakes." However, nanny participants tended to view such behavior as nitpicking or micromanaging if done frequently, and often became concerned that parents were looking for excuses to fire them.

*Psychological Effects of Being Watched.* Many nanny participants expressed a general feeling that it was burdensome to be on camera and potentially watched all day [cf. 74]; some emphasized needing a non-monitored space to take breaks. However, few parent participants recognized that a nanny might want to be out of the camera's view unless they were doing something specifically private (like making a personal call or changing clothes)—or unless they were doing something nefarious. While some nannies mentioned feeling self-conscious because of cameras, or even finding it more difficult to bond with the children [cf. 37], it did not seem to occur to most parents that such self-awareness might be negative. Generally, both the nanny and parent groups had mixed views on whether cameras might help job performance (vs. having no effect), but the issue was more in focus for parents.

*Nannies' Access to Data.* Several nanny participants mentioned that they would have liked to have access to cameras in children's bedrooms, to use as a baby monitor; those who had access found it helpful. For the most part, when we asked parent participants whose nannies did not have nursery camera access why not, it wasn't that they had any objections (as long as they didn't have to share account credentials); they simply didn't think it would be useful.

*Privacy Threat Models.* Most of the parents in our sample were not very concerned about their or their children's privacy regarding cameras, either due to protections they'd implemented or to baseline attitudes. They therefore weren't especially concerned about nannies' privacy either, and assumed nannies would feel similarly. As regards privacy from outside parties, this was often true; most nannies in our sample were not very concerned about device manufacturers, hackers, and so on accessing data about them. However, as a few pointed out, this lack of concern was relative, as their employers' access to data about them was of much more immediate potential consequence.

Even nannies who felt positive about cameras tended to recognize parents' data access as a significant privacy impact, while most parents did not frame their own access to nannies' data in terms of the nannies' privacy at all. This blind spot was particularly notable amongst parents who did not use cameras to monitor nannies; they did not think of the *possibility* of monitoring as a threat in itself.

*Protections.* For the most part, the two sets of participants agreed about what privacy protections were desirable and appropriate in homes where nannies work. In particular, both sets agreed that nanny agencies should facilitate discussions about cameras and educate everyone about the legalities; however, most participants had not worked with agencies so this was a moot point for them personally. Nanny and parent participants also agreed that nannies having edit and deletion access would likely be too problematic, but some nannies pointed out that automatically limiting retention via settings could help their privacy without raising such problems. For the most part, both groups agreed it would be unreasonable to completely outlaw cameras in homes where domestic workers are employed, but nanny participants were more likely to suggest that disclosure and consent should be legally required.

## 5.3 Views on GPS Location Trackers

Companies market technologies for that can track nannies' and children's locations via GPS beacons, key finders, phone apps, or onboard devices in cars. Though these are not smart home devices *per se*, we include them as another way the IoT can affect domestic work.[10]

### 5.3.1 *Experiences with Location Tracking.*

*Nannies' Perspectives.* Though we asked most of our nanny participants, only one had ever experienced GPS tracking (that they knew of), and only when she first arrived in a foreign country as an au pair:

> It was almost more like a safety for me thing, more like if I had gotten lost or something. [...] Once I kind of like knew the way and stuff, they were fine with me not putting my location on [on my phone]. (N26)

A more frequent means of keeping track of where nannies and children were was to ask nannies to send texts and photos, e.g., when they were going to a playground: "They don't have any tracking devices or anything like that. I just text them." (N20) For the most part, nanny participants who had experienced this approach did not frame it as "monitoring" or "tracking" the nanny; rather, they explained parents' motives as wanting to know where their children were or being able to find them in an emergency.

*Employers' Perspectives.* None of the parent participants we asked had tracked their nannies using GPS. If they monitored location at all, they did so through phone calls or texts from the nanny [cf. 81].

*5.3.2 Attitudes and Concerns about Location Tracking.* Because most participants had not experienced it, we probed views on GPS tracking largely via hypothetical scenarios.

[10] As questions about GPS tracking were at the end of the interviews, we sometimes had to omit them when short on time. Findings in this subsection are therefore based on data from only a subset of participants.

*Nannies' Perspectives.* As with cameras, purposes of use or motives could be important in determining whether nanny participants would be comfortable with location tracking (amongst those who would accept it at all):

> *[I: What kind of questions would you ask the parents?]* What's motivating that. If there's a lack of trust, if it is worried about emergency situations, I would ask if they do that with one another. (N4)

The quality of the employer–employee relationship could determine whether nannies assumed good faith:

> I feel like when I'm working, they should have the right to track me when I'm with their child. [...] This all comes from a place of privilege though, you know? Because I've never really had anyone distrust me in a way that I think a lot of other caregivers have been distrusted. (N32)

As with cameras, undisclosed monitoring was of especial concern, because it related to trust between employer and employee:

> If I knew about it, it would be fine. But if I, like, found it, I would be probably pretty upset. [...] It would feel like a violation of my trust. (N20)

The most frequently mentioned concern was that location tracking might happen during nannies' off hours; even nanny participants who generally found location tracking acceptable were concerned about the boundary between work time and personal time:

> If I'm in my working hours, [...] and they want to know where I'm going, [...] it's okay for me. But, not in my personal life. [...] I would feel really bad and pissed off. (N24)

Even if employers did not intentionally cross that line, nannies would be worried they might forget to turn off the app.

*Employers' Perspectives.* As well as considering it unnecessary, a couple of parent participants explicitly mentioned that GPS tracking would be "too intrusive" (P5).

#### 5.3.3 Location Protections.

*Nannies' Perspectives.* We did not explicitly ask either participant group about location privacy protections, but one nanny participant mentioned that concerns about (accidental or intentional) tracking in her off time—whether by employers or third parties—could be mitigated by using a separate GPS device (instead of a phone app):

> I told them that I'd feel better if they just got a GPS device, and I would just keep it with me. Rather than have it on my own personal phone as an app. Because my privacy when I'm not on the clock is my own thing. [...] I don't keep my location services on. I don't prefer to. (N12)

### 5.4 Views on Other Smart Home Devices

Besides cameras (Section 5.2) and GPS location trackers (Section 5.3), we asked participants about their experiences with and attitudes toward other smart home devices. As smart speakers and smart TVs were by far the most common non-camera smart home devices owned by parents or encountered by nannies, the findings below focus on them.

#### 5.4.1 Device Types and Purposes.

*Nannies' Perspectives.* Many of the nanny participants' employers owned at least one smart home device besides cameras. Amongst our 25 nanny participants, 16 were currently working in homes with smart speakers and 13 in homes with smart TVs, usually in common living spaces like the kitchen or living room. Some households also had smart locks, lights, or thermostats, sometimes connected by smart home hubs, as well as smart toys.[11]

These smart devices typically served informational, entertainment, and/or convenience (e.g., home control) purposes, for employers, children, and nannies. Smart locks were used for security, including being able to let the nanny in during certain times. To nanny participants' knowledge, none of these devices were there specifically to monitor them, though in a few cases their employers had looked at usage histories (watch history for TVs, entry logs for locks) that happened to include data from the nanny. In the case of smart TVs, participants were often uncertain whether they had sensor-based features or were only "smart" in the sense of being Internet-enabled.

*Employers' Perspectives.* Amongst 16 parent participants, 13 had smart speakers and 12 had Internet-enabled smart TVs.[12] Most participants used these for information, entertainment, or home control, as did other members of their households, often including their nanny. About half the TVs had voice-recognition features, and a couple had gesture recognition. However, some parent participants were unsure what "smart" sensors their TVs had.

Few parent participants had seen their nannies' request or watch histories, and none had deliberately monitored them. (In fact, in the case of smart speakers, several participants had not known about the history feature.)

#### 5.4.2 Disclosure of Other Smart Home Devices.

*Nannies' Perspectives.* It was uncommon for nanny participants' employers to disclose the presence of non-camera smart devices; most of their employers had not done so. However, nanny participants were generally not particularly upset by the absence of disclosure.

Several factors likely came into play. Smart devices were usually placed in obvious, common locations and easily identifiable by employees. Visibility, combined with a tendency to perceive non-camera smart home devices as at most only a minimal threat to the nanny (as opposed to smart home cameras; see Section 5.2), led to overall nonchalant attitudes about device disclosure.

When employers *had* disclosed presence of non-camera smart home devices, they commonly did so to show the nanny how to use those devices, and not for privacy- or transparency-related reasons:

> *[I: When did they mention to you that it was there?]* Since I started working. The parent told me, "Hey, here is Alexa. You can use her whenever you want. You can play music. You can just come at the side [...] like that." (N15)

When prompted, more often than not, nanny participants stated that ideally they would like employers to disclose all smart home devices; however, very few participants brought it up unprompted. Most nanny participants did not *expect* their employers to disclose the presence of smart home devices other than cameras, nor did they think employers should be obligated to do so:

> I think they're so normalized nowadays that it's just a given sometimes. (N10)

[11] More information about which non-camera smart devices nanny participants owned or had worked with can be found in Appendix A.1.

[12] More information about parent participants' devices can be found in Appendix A.2.

One nanny participant said she would want disclosure if she had reason to believe such devices had implications for her privacy *with respect to her employers*:

> *[I: Do you think parents need to disclose to nannies if they had an Alexa, or a smart speaker, inside their house?]* I don't think so unless Alexa had a way to record our conversations and the parents were listening to it.[13] (N26)

*Employers' Perspectives.* Some parent participants had disclosed to their nannies that they had smart speakers or smart TVs, though they tended to frame it as a matter of telling nannies they were welcome to use the devices. Some believed there was no need to disclose them to nannies nor guests, for example, because the devices were conspicuous anyway:

> I didn't think that conversation needed to explicitly happen because she sees us every morning, talks to the device and asks what the weather is, and to play music. (P1)

In the case of smart TVs, disclosure about sensor data collection was a moot point if the TVs didn't have sensors, or if one had to push a button on the remote to activate them (so it wouldn't otherwise be collecting data—as far as they knew).

#### 5.4.3 Privacy Attitudes and Concerns about Other Smart Home Devices.

*Nannies' Perspectives.* As with cameras, nanny participants had a range of attitudes and concerns about smart speakers and smart TVs, depending on factors such as device capabilities, purpose of use, manufacturer reputation, and privacy resignation.

Nanny participants who were unaware or unsure of smart home device listening or recording capabilities were more likely to feel relatively comfortable around such devices than nanny participants who were aware of such capabilities:

> I've never thought about [the smart speaker] being able to record me. [...] So, unless I knew that it happens, I don't think it would bother me that it was there. (N33)

A few nanny participants, despite believing that smart home devices could collect and retain user data, explicitly noted that they viewed any potential privacy threats as comparatively unimportant, given that parents did not obtain these devices to monitor nannies:

> [The smart speaker] doesn't make me as uncomfortable as the nanny cameras and stuff, but I definitely have read about all the privacy issues that people hate. But, I feel it's not necessarily there to judge me specifically. *[Later]* I don't like them personally, but if you feel, like, you know, it's not necessarily targeted towards me either. (N19)

These nanny participants reasoned that even if devices were listening in on conversations and the data were accessible to developers, it was not targeted and not as consequential as access by employers:

> When it's by the parents, [...] it's much more intimate and it's much more personal. When it's by a corporation, it's kind of a fact of life. (N27)

However, many other nanny participants knew of smart home devices' listening and recording capabilities, and found them discomfiting. Aware that smart home devices were capable of listening in on conversations and recording audio, they worried about the implications of data collection and expressed concern over who could access their recorded data, and what they could do with it:

[13] Though it is technically possible for the owner of a smart speaker to use it to spy remotely on someone, none of our participants had actually experienced this, that they knew of.

> The idea of it constantly monitoring, recording visual and audio is a little, it's off-putting. Because it's like, who is recording this, and why, and where is it going. [...] It's just a general discomfort. (N37)

For some nanny participants, unfavorable views on smart home devices were tied to negative opinions about their developers or service providers, especially for smart speakers:

> They record audio constantly, you can access that audio forever on Amazon. I wouldn't trust Amazon at all with my data. [...] They're not a very trustworthy company. (N4)

A few nanny participants who were concerned about working near smart home devices mentioned feeling resigned to privacy intrusions while working, especially given that smart home devices are nearly ubiquitous:

> I feel like there's cameras everywhere and so much data's being collected on me already, and if it's not a camera, it's an Alexa. [...] So, I think, at this point, I'm a little bit desensitized to it because it feels so common. (N36)

Nannies might therefore have to ignore personal discomfort and accept working in an environment with such devices—and, as one participant pointed out, accept losing their agency over their privacy choices:

> If I'm working in a nanny house, and they've consented to the research of their searches and stuff and I haven't, I definitely feel like that's a little bit of a privacy issue as well. (N35)

*Employers' Perspectives.* Parent participants were not aware of their nannies or babysitters having any privacy concerns about smart speakers, smart TVs, or other (non-camera) smart devices. To the extent that any of them knew their nannies' attitudes toward the devices, they seemed to be positive:

> She loves [the Echo]. She used it more than I did. (P7)

Many assumed that their nannies were comfortable with the devices, because they are common and/or because the nanny used the device themself. However, parents had not specifically asked nannies about their concerns:

> *[I: Do you know if the nanny has any concerns about whether [the TV's voice controller] is recorded, or?]* Not that she's ever expressed, and I've certainly never asked. (P8)

The majority of parent participants who had devices were themselves comfortable with them. If they had privacy concerns for themselves, their children, or their nannies, they tended to view them as minor. In some cases, this was because they didn't think the devices captured anything other than commands, or didn't save them:

> I don't think it actually records anything unless I specifically tell it too. (P5)

In other cases, they thought devices—or third parties—might be continuously listening, but weren't bothered by it:

> I don't feel uncomfortable with those. I mean, I understand that the FBI or whatever can use them to listen to you, but my life is pretty boring. If you would like to hear me sing songs about eating peas to my baby, then really, have at it. (P2)

Some parent participants were uncertain, and a couple had more serious privacy concerns. In one case, the participant projected his own concern onto his nanny:

> *[I: Did she have any questions or concerns about it, or do you know whether she knows about it?]* I'm not sure if she does or doesn't, but that really is a good question. I'm sure, um, I would guess, I'd say she does. But that's a good question because that brings up another privacy issue, because those things don't turn off. [...] I don't like that thing. It's not allowed in my bedroom, my bathroom, it's not allowed near me. (P18)

However, most did not bring up concerns about their nannies' privacy unless we asked.

In particular, since none had deliberately monitored their nannies' usage history on such devices, parent participants mostly had not considered how their own access to data might affect nannies' privacy. When asked, they tended to view any impact as negligible and expectable:

> If they're not aware that what they look up [on YouTube] is there, then, well, I don't know what to tell them on that, because you're using someone else's device. (P6)

#### *5.4.4 Protections and Controls for Other Smart Home Devices.*

*Nannies' Perspectives.* For the most part, nanny participants did not take many protective measures around non-camera devices in their employers' homes, and most were not much concerned about whether their employers took protective measures on their behalf.

*Device Feedback.* The most common privacy mechanism nanny participants had access to was status indicators such as lights. However, nanny participants did not always notice such feedback, or weren't certain what it meant:

> I think the light would change red or green or it would, like, make colors. [...] Like, why's it doing that? So, I don't know. I didn't even ask. (N40)

*Ability to Unplug or Power Off Device.* Very few nanny participants had their employers' permission to unplug or power off any of their employer's smart home devices—or even necessarily knew how to turn them off, given the ambiguity between "off" and "standby" and unclear feedback from the device. Nanny participants noted that unplugging someone else's device would break social norms:

> I'd be like, excuse me. You know, don't unplug my electronics, please. [...] It'd be like somebody like coming in and unplugging my TV. (N27)

Some nanny participants said they would feel comfortable asking for permission if they wanted to turn off a device, but a couple said they would hesitate to broach the topic in someone else's home.

*Device Controls.* Nanny participants generally had little knowledge of or control over smart home device privacy controls and settings. However, few nanny participants had strong or specific opinions on what device controls they would like to exercise in their employers' homes, even if they could, though a couple would have preferred less data retention:

> I mean, I would probably set [the smart TV] so that it didn't store any data other than what was necessary for its functioning. (N14)

If nanny participants *had* had particular ideas about stronger privacy controls that they really wanted, most said they would feel comfortable asking their employers, but they wouldn't necessarily feel comfortable pushing it:

> I feel like I would definitely talk to the parents about [Alexa] [...] and if they could change the privacy setting a little bit, that would be great. But if they said no, I think I would pretty much just ignore it and move on. (N35)

*Contracts, Agency Guidelines, and Legal Protections.* Aligning with the perception of minimal threat from their employer to their privacy, nanny participants did not tend to think non-camera smart home devices needed to be mentioned in contracts:

> *[I: Would you specify in your contract whether it's permissible to use smart home devices other than cameras? [...]]* I would not, mostly because I wouldn't think of them as having data accessible to my employers in a situation that would be uncomfortable for me. (N14)

Most nanny participants either were not sure whether there are laws about disclosing non-camera smart home devices to domestic employees or thought there weren't any. Most did not think there needed to be. Of those who had worked with agencies, none had been given advice about non-camera devices, but they didn't think it necessary.

*Employers' Perspectives.* A few parent participants mentioned protective measures they had taken or might like to have, for their own sake or their nannies', but most did not have strong opinions.

*Device Controls and Ability to Unplug/Power Off.* Most parent participants had not interacted with the privacy settings on their non-camera smart devices at all, and none had discussed preferred settings with their nanny, nor offered them access to such controls. A few parent participants mentioned having told their nanny or babysitter they could turn off or unplug the device if they weren't comfortable. Others whom we asked said they wouldn't mind if their nanny did so.

*Contracts and Legal Protections.* When laws about disclosing non-camera smart devices to domestic employees came up, participants either weren't sure or thought there weren't any; none thought there *should* be laws specific to that situation.[14] Since most parent participants did not have written contracts with their nanny, device provisions were a moot point.

*5.4.5 Comparison of Nanny and Parent Participants' Views on Other Smart Home Devices.* We did not observe so many significant disconnects between nanny and parent participants' views on other devices as we did with cameras—nor in their assumptions about each other's views. The two groups' threat models were much more similar.

*Expectations and Preferences about Disclosure.* Nanny and parent participants tended to agree that explicit disclosure of non-camera devices just for the sake of disclosure was rare and largely unnecessary, especially as compared to cameras. (Even among those who thought cameras should be disclosed.) Both cited the commonness of smart home devices and the fact that, especially for smart speakers, they tend to be conspicuous.

However, nannies were more likely to explicitly point out that non-camera devices were far less likely than cameras to be used to monitor them, and that parents often did not access data about them at all. Only a couple of parents cited having less access to nannies' data in explaining why they did not disclose non-cameras—but as mentioned in Section 5.2.9, most parents didn't even think about the privacy impact of their access to camera data of nannies in the first place.

*Privacy Threat Models and Attitudes.* Nanny participants' assumptions that their employers used their non-camera devices for their advertised purposes and not to monitor them were borne out (at least in our small sample) by parents' self-report of their behavior. The two groups' threat models for these devices were therefore much more similar than their respective threat models for cameras, with both concentrating on external actors. Nannies were more likely to explicitly highlight the difference from cameras in terms of who might access their data.

[14] We asked all parent participants whether they had disclosed non-camera smart devices, but did not always probe further if they said they'd never even thought about it.

The two groups had similar ranges of variation between participants' levels of concern about their own data. There was more of a skew toward being comfortable among the parent participants, but this is not necessarily meaningful, since we recruited only parents who had smart home devices of some kind. Perhaps more interestingly, some nanny participants drew more of a distinction between unconcern and resignation, for example, because they did not expect to control devices or be able to fully protect their privacy in others' homes. However, overall, differences in attitudes were not as striking as for cameras.

*What's Worth Discussing.* However, the similarity in range of attitudes does highlight a potential disconnect, in that parent participants assumed that their nannies simply did not have privacy concerns because they did not mention them, or because they used the devices themselves. The range of concerns in our nanny sample suggests that parents participants' assumptions may sometimes have been inaccurate; rather, their nannies may just not have been concerned enough to make a fuss about it with their employers.

*Protections and Discussions about Protections.* Most participants in both groups had not thought much about privacy settings for smart speakers, smart TVs, and other non-camera devices, and therefore had not discussed it with their employers or employees, respectively. The one discrepancy was with regard to turning off or unplugging the device, where parent participants tended to say they would have no problem with either, while nanny participants were not necessarily ready to make that assumption about their employers.

### 5.5 Comparing Views and Threat Models for Different Types of Smart Home Devices

In this subsection, we systematically describe differences between participants' views about and threat models for different types of smart home devices. We include some quotes in which participants explicitly compared multiple device types (at least for nannies, who more often made explicit comparisons); however, the analysis was based on a higher-level look at all of the data. We compare nannies' perspectives on different devices in Section 5.5.1 and parents' in Section 5.5.2. We compare the two participant groups' differentiation among devices in Section 6.1.

*5.5.1 Comparing Nannies' Perspectives by Device.* The differences between nanny participants' experiences of and concerns about different types of devices were quite pronounced. For example, for most nanny participants, indoor cameras could (if misused) change their perception of a job drastically, by blunting their autonomy and causing problems in their relationship with their employers. Smart speakers and smart TVs had no such power. Some possible causes and consequences of this distinction are outlined below.

*Targeted vs. Shared Purposes.* Compared to other smart home devices, cameras enabled a wide range of purposes and use cases, ranging from home security to checking in on kids and monitoring and micromanaging nannies. In some households, nannies might share in at least some of the purposes (security, monitoring children) and use or benefit from cameras. However, cameras often had additional—or sole—purposes that nannies did not share in, that might not benefit them, and that sometimes even ran counter to nannies' own interests:

> I feel like a smart TV is different because they [...] didn't buy their smart TV to watch me with the kids. [...] Whereas a camera, like, the purpose is to record me with their kids. (N26)

On the other hand, devices like smart speakers and TVs were generally used by both employers and nannies for the same purposes, e.g., entertainment. Even if nannies did not use smart speakers and TVs, unlike cameras, at least they didn't believe their employers used them for targeted monitoring of nannies.

Thus, nanny participants had a wider range of comfort levels with cameras, depending on their purposes of use, compared to smart speakers and TVs. However, on the whole, most found non-camera devices less invasive than cameras (at least indoor cameras) or location trackers, which their employers at least *could* use to monitor nannies specifically:

> I'm not all that worried about [Alexa listening], because I just don't have the mental effort to do that right now, you know. It's just, like, so nebulous. And to me, it doesn't seem like it's the parents recording it. It's a third-party system. [...] They're less threatening than the in-home security cameras. *[Later]* I would put [Alexa] under a different category, because it's not the parents that are saving the data. (N7)

Nanny participants' views on location trackers (whether phone apps or GPS tags) tended to be more similar to their views on cameras than their views on other devices. In particular, given the narrow set of reasons one might want to track someone's location, views were most similar to cameras used for checking on or monitoring the nanny with the kids (with similar equivocation around whether "checking on" and "monitoring" are truly different).

*Use-Based Threat Models.* Some types of cameras couldn't be effectively used to monitor the nanny with the children, such as doorbell or porch cameras, closed-circuit baby monitors (that couldn't be accessed by parents outside the house), or security cameras that were clearly disarmed when anyone was home. Nanny participants' threat models and privacy attitudes about such cameras tended to be more similar to their threat models and attitudes regarding other types of smart home devices than they were to threat models and attitudes about cameras that could be used for monitoring. In effect, device *type* could be less determinative of nannies' attitudes than device *purpose*.

Those nannies who found smart speakers equally concerning or more concerning than cameras usually either were sure their employers did not use cameras to monitor them, or were comfortable with (light) monitoring in the context of a generally positive relationship with their employers:

> We have other kinds of devices [like Alexas] that are in the house that maybe I feel less comfortable with, but [...] the cameras I feel are perfectly comfortable, within the context of how they're being utilized and the specific family that I work with. (N4)

The few nanny participants who expressed strong privacy concerns about smart speakers and smart TVs were mostly concerned about uses by manufacturers and developers (e.g., selling data to third parties):

> The camera [even if it was] collecting audio, [...] it stays within the, like, [...] the family, the individual. Whereas the smart devices [...] seems more like it's going to another source. Like, there are more sources that are able to access this information. (N37)

(However, concerns about smart TVs were generally less than those about smart speakers, largely because it was clearer whether or when they were collecting sensor data.)

For most nanny participants, use by manufacturers and developers—or even hackers—did not loom as large in discussions of cameras. This is perhaps in part because the smart home camera market is more diverse, whereas the smart speaker market is dominated by Amazon's Echo/Alexa, which had recently received bad press about privacy. However, it is also worth noting that most nannies' ideas about privacy threats posed by camera manufacturers were relatively vague, whereas many had very specific notions about how camera use by employers could directly impinge on their job security and relationships with employers. In other words, privacy threats from employers may have been so much more immediate with (indoor) cameras that they overshadowed and left little room to worry about privacy threats from other quarters. As one participant put it:

> Most of [the families] are either working with a security system in which they have no control over the footage, how it's stored, how it's destroyed—which I'm perfectly fine with. Parents can't micromanage if they're not in control. (N3)

*Device Disclosure and Discussions.* Nanny participants had significantly different attitudes toward discussing with employers the different types of devices. Though opinions were mixed, nannies were less likely to say that it was necessary for parents to disclose or provide details about smart speakers or smart TVs than about cameras, due to the visibility and clear purpose of use of non-camera devices. Even more than with cameras, undisclosed monitoring was of especial concern for location tracking—and lack of disclosure was similarly viewed as a signal of bad intentions.

Nanny participants generally would be more comfortable discussing their privacy concerns about non-camera devices with employers, or asking for changes to settings, whereas with cameras they worried that expressing concern might be taken as suspicious. But on the other hand, they were less likely to care enough about non-cameras to bother bringing it up.

*Protections and Controls.* Many nanny participants thought it was necessary, or at least desirable, for employment contracts to mention the presence and purpose of use of cameras, and suggested agencies should encourage disclosure. Yet, very few thought it was necessary to do those things for other devices. Additionally, a few nanny participants thought that it was important to negotiate with employers about data collection, processing, storage, and retention by cameras (even if they were hesitant to do so in practice), but none thought it important to negotiate about or have control of other devices.

*5.5.2 Comparing Employers' Perspectives by Device.* For the most part, parent participants' privacy threat models for cameras were more similar to their threat models for smart speakers and smart TVs than was the case with nannies.

*Differences in Views on Their Own/Their Children's Privacy.* Most parent participants had fairly similar privacy attitudes, concerns, and threat models for all types of smart home devices discussed. However, some viewed cameras as more invasive, or had more concerns about the consequences of hacking, than with non-camera devices. Meanwhile, some others expressed more comfort with cameras and smart TVs than smart speakers, as a result of being more certain about when they were collecting data, where it went, and how it was stored.

If a camera did not send data over the Internet, or if they were certain it only livestreamed (no recording), participants felt in better control of their privacy, whereas smart speakers engendered a fair amount of uncertainty. Parent participants were much more likely to have investigated or changed the privacy settings on their cameras than their smart speakers or smart TVs, reflecting either more privacy resignation about non-camera devices or more urgency about controlling camera data.

*Device Disclosure.* While most parent participants at least theoretically believed they should disclose indoor cameras, they did not think they needed to disclose other devices:

> I feel like a Nest Cam [...] is more something where I feel like it's necessary to inform someone. But with all these other smart devices [...] it's not as top of mind that it's a privacy concern. (P4)

Those who hadn't bothered to disclose cameras presented similar reasoning to the reasoning they and other parent participants had for not disclosing non-cameras: visibility, commonness, and/or the assumption that the nanny would ask if she wanted to know.

*Differences in Views on Nannies' Privacy.* Some recognized the unique threats to nannies' privacy and autonomy posed even by disclosed cameras, but most did not differentiate between cameras and non-camera devices in terms of nannies' privacy—and since almost none were concerned about non-cameras, this set a low baseline. The assumption that nannies did not have concerns if they hadn't expressed any tended to apply equally to all devices.

Parent participants were more likely to be worried or suspicious if a nanny did not want to work with cameras, or if they wanted to cover or unplug them, thinking they might be hiding something. They had no such worries about non-camera devices. Similarly, they were more likely to be open to nannies requesting access to or changes in privacy settings for non-camera devices.

## 6 Discussion

In Section 6.1, we highlight our main findings, and in Section 6.2, we compare them with related work. Section 6.3 suggests design priorities, and Section 6.4 suggests future research.

### 6.1 Summary of Findings

*RQ1: Nannies' Experiences and Views; Factors Affecting Views; Differences between Devices.* Nanny participants were most concerned about whether and how indoor cameras might be used by employers to supervise their work, and they drew fine distinctions between acceptable and unacceptable modes of supervision (e.g., frequency of checking, interference with childcare). Disclosure of cameras was also important to acceptability, and nannies wanted to know their purpose.

Views on cameras that nannies were certain were *not* being used for monitoring were more similar to views on smart speakers and smart TVs, whose purposes were unrelated to them. In comparison with access by employers, few nanny participants were concerned about how device data would be used by manufacturers and developers. Yet in all cases, nanny participants believed they had limited ability to control devices' collection of data about them, as well as privacy setting configuration, given power imbalances in employer–employee relationships.

*RQ2: Parents' Views and Purposes; Views regarding Self/Kids vs. Nanny.* Most parent participants were comfortable with their devices. Some parent participants were concerned about the privacy downsides of cameras, but they believed these downsides were justified for the purposes of ensuring the safety of their children and homes. Several parent participants used cameras in part to manage their nannies, and they expected that nannies would not object to cameras—nor even have privacy concerns about them.

Although many parent participants believed that cameras should be disclosed to nannies, most did not disclose them in practice. In contrast, parent participants felt there was no need to disclose non-camera devices like smart speakers and smart TVs, as they are common fixtures, used for non-nanny-related purposes, and generally in obvious locations.

*RQ3: Alignments and Disconnects between Nannies and Parents' Views.* Parent participants' reasons for having cameras generally aligned with the assumptions that nanny participants had about why their employers used cameras. However, parent participants made a stronger differentiation between using indoor cameras to *check in on kids* vs. to *monitor nannies*, while nannies tended to view these as similarly consequential in terms of the effect on their privacy at work. Meanwhile, parent participants did not think of their own access to camera data as a privacy threat to nannies, whatever the purpose.

Although both nanny and parent participants believed that cameras were a normal work condition, nanny participants emphasized the importance of disclosure, as enabling consent and allowing them to discuss camera use with their employers without seeming suspicious. Fewer parents viewed disclosure as highly important, especially if cameras were obviously visible.

Nanny and parent participants' views, particularly concerns and threat models, were more similar to each other when it came to non-camera smart home devices than to smart home cameras. Both groups believed that smart speakers, smart TVs, and the like were common, and they were used by all parties for entertainment and information. Both nanny and parent participants were mainly concerned about external threats such as hackers or data repurposing by manufacturers, but most said it was not a substantial worry. Consequently, most participants in both groups did not think that nannies needed special protections (including disclosure) against non-camera devices.

However, when it came to indoor smart cameras, most nannies were much less concerned about external actors than they were about their employers, whose use of data about them had much clearer and more direct potential for causing harm.

*RQ4: Interventions to Balance Privacy Needs.* Most participants in both groups thought disclosure of cameras (though not other smart home devices) was a feasible and important protection, along with including it in employment contracts. Although both participant groups believed it would not be reasonable to stop using cameras in homes where nannies worked, nanny participants suggested that laws should mandate both *disclosure* of and *consent* to the use of indoor cameras. Some mentioned it would be helpful for an outside entity to facilitate discussions about cameras, such as agencies—but few actually worked with agencies. In Section 6.3, we discuss and prioritize interventions to address this communication gap, encourage disclosure, and provide alternate ways for nannies to be aware of and have some (appropriately limited) control over data collection for multiple device types.

## 6.2 Comparison with Similar Studies

Our study builds on prior research about domestic workers in smart homes, but specifically focuses on childcare, which introduces an expectation that parents may be due some leeway in wanting to assure their child's safety—but also an increased need for interpersonal trust. Our study also differed from others in being conducted in the U.S. and in involving mostly nannies or employers of nannies who did not depend on employers for housing or immigration status; also, only one previous study had also involved employers. Here we describe how these differences resulted in contrasts between our study and others', and also where similar themes arose.

Like the interviews by Johnson et al. [37] with Filipina migrant domestic workers in Hong Kong, our study found that using cameras for surveillance purposes could undermine nannies' trust in their employers, especially if undisclosed, and that many nanny participants viewed employers accessing their camera data as the most significant privacy threat. As we also interviewed parents, we can add that parent participants often did not share this perspective. Because we covered a broader range of circumstances and purposes of use for cameras, our participants had a wider range of attitudes and experiences. But participants in both studies cited some of the same dependency factors, like devices' potential to affect their working conditions (especially micromanaging), relationships with their employers, and job prospects.

Johnson et al. [37], Ju et al. [38], and Słupska et al. [67] all focused on *migrant* domestic workers, and all noted that the imperative of keeping a job could lead to a diminished subjectivity, especially for live-in workers. Only two of our participants (au pairs) mentioned depending on employers for immigration status and housing; most nannies in our sample had more freedom to decline or leave a job, and so felt they had more agency over their working conditions, including surveillance. The findings of Ju et al. [38] did parallel ours in that attitudes toward surveillance were modulated by generally good relationships with employers, and their findings about increased empowerment among live-out workers are echoed at a smaller scale in our nanny participants' comments on needing a non-monitored space for breaks.

Albayaydh and Flechais's [3, 4, 6] interview studies with domestic workers, employers, and regulators in Jordan found that, despite some regulators' assertions that workers' privacy would be protected by socio-cultural norms, few employers disclosed devices. It is not clear whether employers subscribed to those norms, but it is worth noting that we found a similar disconnect, where more parent participants thought they *should* disclose devices than actually *had* disclosed. In addition, employers in both their studies and ours opined that, if domestic workers cared about whether there were devices, it was up to them to ask.

Unlike our participants, Albayaydh and Flechais found that few employers and employees had the technical skills to configure the privacy settings of devices. Most of their recommended interventions (including most functions of a prototype app they developed [5]) were therefore either based on automated detection or were more social and educational, such as public awareness campaigns about device privacy that leverage culturally specific social and religious norms.

Finally, Tan et al. [74] discussed the value to camera owners (including some employers of nannies) of what they term *mere-potential* monitoring, defined as the *capability* to monitor events, even when the owner has not yet done so. We find this is indeed an active value for parent participants, but perhaps even more important to nannies. Some may value it as potentially protective against accusations—but at the same time, many nanny participants weighed mere-potential monitoring as part of the *risk* of a camera.

### 6.3 Priorities for Design Interventions

To ameliorate privacy impacts of smart home devices on secondary users, bystanders, and surveillance targets, researchers have proposed, prototyped, and/or evaluated a variety of solutions, including technical, social, and educational interventions. Here we discuss four types of design interventions we think should be prioritized as potentially most helpful in improving privacy and agency for the use case of domestic employees, given the complex social dimensions of domestic work, with notes on how they could be adapted to this use case. Our prioritization is based both on participants' explicit comments on privacy protections (see Sections 5.2.8 and 5.4.4) and on other relevant comments about their main privacy concerns around smart devices.

*Discussion Guides to Build Communication.* Technical interventions (such as those mentioned below) are necessary but insufficient; we view social and sociotechnical interventions as the highest priority to specifically address domestic worker privacy. Several prior studies have suggested that incidental users' or bystanders' concerns about smart devices could be mitigated by better communication with device owners, possibly supporting collective privacy management [e.g., 10, 20, 53, 74, 86, 89]. However, as some prior work pointed out, it can be difficult for non-owners to *initiate* conversations, because they may violate social norms—especially when there is a power imbalance involved, like with domestic work [3, 5, 16, 43].

Many nanny participants had questions about details of data collection, or (in the case of cameras) how their employers used that data and why, which they had been uncomfortable bringing up. Discussion about data use would be most pertinent for indoor cameras, where the question of purpose is both especially difficult to guess and especially difficult to ask about. At the same time, attitudes and concerns depended heavily on such details, and cameras were the subject of the most striking disconnects we noticed between nanny and parent participants (see Section 5.2.9).

In Bernd et al. [16], we present a detailed proposal for camera discussion guides we are developing for domestic employees and their employers, to reduce discomfort (by providing an external reference point) and help shape the *content* of such conversations (see similar suggestion in Mare et al. [51] for Airbnb). We plan to integrate such a guide with interface nudges (see Nudges below); they could also be included in educational materials such as those previously suggested for device owners and/or workers [3–5, 53, 67, 72] (see Słupska et al. [66] for an implementation of educational materials about privacy for domestic workers).

This intervention would not likely be very effective given an adversarial, untrusting relationship (e.g., where employers are generally not willing to discuss working conditions), but could improve communication about cameras within a generally cooperative relationship. Guides could be structured around successful examples of conflict mediation (see suggestion in Apthorpe et al. [10] for interface nudges), emphasize how communication helps both parties resolve uncertainties and build trust—an important value in domestic childcare work (see Section 5.2.2)—and materials for domestic workers might also include advice on how to bring up the topic without sounding defensive, if employers do not initiate discussions.

*Clear, Flexible Indicators.* Frequently mentioned in previous literature on both multi-user smart homes and smart home visitors [e.g., 2, 4, 22, 46, 52–54, 64, 67, 75, 90] (as well as on primary users [e.g., 21, 26, 39, 40, 58, 65, 74, 88]) are clear, intuitive indicators that show when a device is on and when it is collecting data. Domestic employees are frequently exposed to devices where they do not have other ways to access information about data collection. In fact, many of our nanny participants mentioned explicitly that they would like such features on any smart devices they encounter in their employers' homes.

For example, some nanny participants were uncertain about whether cameras collected audio, and whether they recorded as well as live-streaming. Some said they would like indicators showing when their employers were specifically watching a camera feed—and yet, some pointed out that they preferred *not* to know when they were being watched, to avoid feeling self-conscious, so such mechanisms may need to be flexible. Clearer indicators for active data collection could provide reassurance for nannies who are uncomfortable with smart speakers, so they would not be faced with the potential awkwardness of unplugging a device. Unlike our other prioritized suggestions, indicators could help in either cooperative or adversarial situations, especially if designed to prevent tampering.

*Expanded Account Types.* Most nanny participants did not have access to device privacy settings and controls, nor the ability to view data. For indoor cameras, those who had access to data felt more comfortable and confident, especially when it helped in childcare. Hence, there is a need for power sharing mechanisms. Researchers have suggested, designed, and/or evaluated mechanisms to better accommodate different types of multi-user households and/or accounts for non–household members encountering the device.

Of particular interest are proposals to include limited control or access for children, short-term rental guests, or other types of secondary users [e.g., 7, 10, 31, 33–35, 43, 44, 46, 51, 59, 64, 70, 77, 83, 88, 90, 91]. As one option, highly granular controls could allow calibrating levels of control to specific household norms [30, 34, 35, 64, 70, 76]. However, researchers have found that smart home residents do not necessarily use such fine-grained controls in practice, so have suggested more easily usable options such as reviewable bids for more control (in high-trust environments) [50], or preset account types [43, 91]. Specifically, researchers have proposed preset account types with defaults that represent common household configurations [10, 31, 43], such as child accounts [10, 44, 70] or short-term rental guest accounts [51]; we suggest also including an "in-home worker" preset.

For cameras, having accounts would allow nannies to use cameras as baby monitors. Meanwhile, expanded account types could improve domestic workers' privacy and agency over data collection, thus providing an avenue for direct control (even in situations where they are monitored by parents), while mitigating concerns that trying to control someone else's device flouts social norms (see Sections 5.2.8 and 5.4.4; see also, e.g., [2, 16, 50, 75]).

This could address domestic workers' desires to know what data is collected about them (including scope of view for cameras, usage records for smart speakers), and confirm or even choose retention limits. As we noted in Section 5.2.9, negotiating automatic deletion after a reasonable window for review could allow nannies some control without triggering concerns they might tamper with footage to hide bad behavior. (Negotiating retention limits could be suggested in a Discussion Guide.) Account types where capabilities are limited, especially as regards data deletion and access to others' data, could help mitigate such concerns, as could allowing device owners to review any data-related actions in such accounts. At the same time, special accounts could address employers' needs to limit employees' access to data collected when they are not in the home.

*Nudges during Device Setup.* Authors have suggested that device setup dialogues and/or configuration interfaces should explicitly nudge primary users—and make it easy—to add separate accounts or use settings that allow non-primary users some control over the device [10, 16, 31, 41]; use settings that limit data collection to protect bystanders [22, 64, 72, 74]; and/or discuss devices with cohabitants or frequent bystanders and consult them about their preferences [16, 31, 59, 67].

Although most parent participants believed that indoor cameras should be disclosed, many did not disclose, nor discuss any further details. At the same time, many nanny participants would have liked to know more about smart devices but feared initiating an inquiry about them might seem suspicious. Adding nudges to disclose the device and discuss settings with any domestic workers—and potentially even seek their input on those settings, when appropriate—could lessen the burden on employees to initiate a potentially uncomfortable discussion. In a prototype intervention we are developing, nudges in a device interface also incorporate specific points to discuss. As with Discussion Guides, nudges would be most effective given reasonably cooperative relationships.

## 6.4 Future Work

*Study Other Types of Domestic Workers.* Future work should explore the views, privacy concerns, and threat models of other groups of domestic workers, as different job types may lead to differences in experiences and views. For example, elder-care is less well-paid and less prestigious than childcare, and has a different set of considerations regarding the vulnerability and privacy of those being cared for. Gardeners and maintenance people may not need to establish trust with their short-term employers in the way that care workers do, resulting in different expectations about safeguards.

*Quantify and Generalize Findings.* We recommend that future work design and conduct large-scale, cross-cultural surveys with domestic workers and other types of bystanders. In Despres et al. [23], our research group compared bystanders' views in Germany, Mexico, the UK, and the U.S.; we suggest expanding this type of study to a broader set of WEIRD and non-WEIRD countries. Such surveys could quantify insights from our study and others, and compare across countries, for example, how differing social norms and (for workers) immigration rules influence people's views on smart homes.

*Develop Trust-Building Interventions.* Our nanny participants considered mutual trust key to develop a good working relationship with their employers. Besides technical interventions (see Section 6.3), the computer security and privacy community should focus on exploring and developing social interventions that help build rapport and honest communication between employers and employees. Technical interventions (see Section 6.3) that enable employers to share power with their employees, for example, via separate accounts, are necessary, but insufficient if employers do not trust their employees enough to use them. At best, technical and social interventions can work together, as in suggestions for interface nudges or norm-sensitive access control mentioned in Section 6.3.

## 7 Conclusion

Our two-side study revealed disconnects in views and threat models of smart home devices between domestic childcare workers and parents who employ such workers.

Unlike smart speakers and smart TVs, indoor smart home cameras—especially if used for targeted surveillance or not disclosed by employers—had the power to change nanny participants' perceptions of a nannying job and cause problems in employer–employee relationships. Therefore, while almost all nanny participants were comfortable working in homes with other types of devices, they had a much wider variety of attitudes toward cameras. Where nanny participants believed that employers' purposes in having cameras were not targeted toward the nanny, their views on cameras were similar to their views on other smart home devices—though they had stronger opinions about disclosure. Views on cameras used with purposes that targeted the nanny, such as monitoring her work, were more nuanced, and depended on specific details of use (such as frequency of checking or whether their employers tended to micromanage). Nanny participants were also more likely to believe that their employment contracts should mention cameras than other smart home devices.

In contrast, most parent participants tended to have similar views on and threat models of cameras and non-camera smart home devices, when considering their own and their children's privacy, though a few parent participants found cameras more privacy-invasive. Although some parent participants recognized the unique threats of indoor cameras to nannies' privacy, most parent participants would worry if a nanny did not want to work with cameras. Nanny participants were sensitive to such concerns, and were sometimes reluctant even to ask about cameras—while most parents would not mind discussing them, but assumed nannies would bring it up if they cared. In contrast with cameras, on the whole, parent and nanny participants had similar views and expectations about non-camera smart home devices, with fewer disconnects.

Drawing on these findings, we recommend prioritizing a set of social and technical interventions that respect parents' prerogative to use devices while mitigating potential negative effects on the privacy and individual agency of domestic childcare workers.

## Acknowledgments

We are grateful to Maritza Johnson for proposing this project, and to others who have helped with suggestions and resources along the way, including Franziska Roesner, Serge Egelman, Yasemin Acar, Sascha Fahl, Julia Słupska, Nathan Malkin, Wael Albayaydh, James Pierce, and Chris Geeng. Special thanks are due to George Chalhoub for help preparing to analyze the parent interviews. We also thank participants at the 2019 Symposium on the Applications of Contextual Integrity, the 2020 Workshop on Free and Open Communications on the Internet (FOCI), and the 2022 Symposium on Usable Privacy and Security (SOUPS), as well as anonymous reviewers for FOCI, SOUPS, PoPETS, and TOCHI, for their helpful comments. Finally, this work would not have been possible without the study participants' generosity in sharing their time, and their wide-ranging, thoughtful insights.

## References

[1] 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 '21)*, 1–14. DOI: https://doi.org/10.1145/3411764.3445122

[2] 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.

[3] 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)*, 1–24. DOI: https://doi.org/10.1145/3491102.3502097

[4] Wael Albayaydh and Ivan Flechais. 2023. Examining Power Dynamics and User Privacy in Smart Technology Use among Jordanian Households. In the 32nd USENIX Security Symposium (USENIX Security '23), 4643–4659.

[5] Wael 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 *the 33nd USENIX Security Symposium (USENIX Security '24)*, 4963–4980.

[6] Wael Albayaydh and Ivan Flechais. 2024. "Innovative Technologies or Invasive Technologies?" Exploring Design Challenges of Privacy Protection with Smart Home in Jordan. In *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW1 (2024), 1–54.

[7] Ahmed Alshehri, Malek Ben Salem, and Lei Ding. 2020. Are Smart Home Devices Abandoning IPV Victims? In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, Los Alamitos, CA, 1368–1375. DOI: https://doi.org/10.1109/trustcom50675.2020.00184

[8] 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.

[9] Denise Anthony, Carl A. Gunter, Weijia He, Mounib Khanafer, Susan Landau, Ravindra Mangar, and Nathan Reitinger. 2023. The HandyTech's Coming between 1 and 4: Privacy Opportunities and Challenges for the IoT Handyperson. In *22nd Workshop on Privacy in the Electronic Society*, 129–134.

[10] 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]. Retrieved from http://arxiv.org/abs/2001.10608

[11] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2022. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. *ACM Transactions on Internet of Things* 3, 4, Article 25 (Sep. 2022), 29 pages. DOI: https://doi.org/10.1145/3539737

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

[13] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms versus COPPA. In *USENIX Security Symposium (USENIX Security)*, 123–140. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

[14] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 417–435. Retrieved from https://www.usenix.org/conference/soups2020/presentation/barbosa

[15] Vince Bartle, Janice Lyu, Freesoul El Shabazz-Thompson, Yunmin Oh, Angela Anqi Chen, Yu-Jan Chang, Kenneth Holstein, and Nicola Dell. 2022. "A Second Voice": Investigating Opportunities and Challenges for Interactive Voice Assistants to Support Home Health Aides. In *2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. ACM, New York, NY, 1–17. DOI: https://doi.org/10.1145/3491102.3517683

[16] 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 *18th Symposium on Usable Privacy and Security (SOUPS '22)*. USENIX Association, Boston, MA. 687–706. Retrieved from https://www.usenix.org/conference/soups2022/presentation/bernd

[17] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*. Retrieved from https://www.usenix.org/conference/foci20/presentation/bernd

[18] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. 2019. Smart Home Bystanders: Further Complexifying a Complex Context. In *Presentation at the 2nd Annual Symposium on Applications of Contextual Integrity*. Retrieved from https://privaci.info/symposium2/papers_and_slides/Sub_Bernd_et_al_Bystanders_CI_2019.pdf

[19] Clara Berridge, Jodi Halpern, and Karen Levy. 2019. Cameras on Beds: The Ethics of Surveillance in Nursing Home Rooms. *AJOB Empirical Bioethics* 10, 1 (2019), 55–62. DOI: https://doi.org/10.1080/23294515.2019.1568320

[20] Yi-Shyuan Chiang, Omar Khan, Adam Bates, and Camille Cobb. 2024. More Than Just Informed: The Importance of Consent Facets in Smart Homes. In *ACM CHI Conference on Human Factors in Computing Systems (CHI '24)*. ACM, New York, NY, Article 849, 21 pages. DOI: https://doi.org/10.1145/3613904.3642288

[21] 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 *ACM Conference on Ubiquitous Computing (UbiComp)*, 61–70. DOI: https://doi.org/10.1145/2370216.2370226

[22] 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* 2021, 4 (2021), 54–75.

[23] Tess Despres, Marcelino Ayala Constantino, Naomi Zacarias Lizola, Gerardo Sánchez Romero, Shijing He, Xiao Zhan, Noura Abdi, Ruba Abu-Salma, Jose Such, and Julia Bernd. 2024. "My Best Friend's Husband Sees and Knows

Everything": A Cross-Contextual and Cross-Country Approach to Understanding Smart Home Privacy. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024), 413–449. Retrieved from https://petsymposium.org/popets/2024/popets-2024-0124.php

[24] David Eckhoff and Isabel Wagner. 2018. Privacy in the Smart City: Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials* 20, 1 (Firstquarter 2018), 489–516. DOI: https://doi.org/10.1109/COMST.2017.2748998

[25] Economic Policy Institute. 2020. Current Population Survey Extracts, Version 1.0.7. Retrieved July 21, 2020 from https://microdata.epi.org

[26] Serge Egelman, Raghudeep Kannavara, and Richard Chow. 2015. Is This Thing On? Crowdsourcing Privacy Indicators for Ubiquitous Sensing Platforms. In *ACM Conference on Human Factors in Computing Systems (CHI)*, 1669–1678.

[27] Nils Ehrenberg and Turkka Keinonen. 2021. The Technology Is Enemy for Me at the Moment: How Smart Home Technologies Assert Control Beyond Intent. In *ACM Conference on Human Factors in Computing Systems (CHI '21)*. ACM, New York, NY, Article 407. DOI: https://doi.org/10.1145/3411764.3445058

[28] Angella Foster. 2019. When Parents Eavesdrop on Nannies. *New York Times* (August 2019). Retrieved June 8, 2020 from https://www.nytimes.com/2019/08/19/opinion/nanny-cams-privacy.html

[29] Alisa Frik, Julia Bernd, and Serge Egelman. 2023. A Model of Contextual Factors Affecting Older Adults' Information-Sharing Decisions in the US. *ACM Transactions on Computer-Human Interaction* 30, 1 (Apr. 2023), 1073–0516. DOI: https://doi.org/10.1145/3557888

[30] Radhika Garg and Hua Cui. 2022. Social Contexts, Agency, and Conflicts: Exploring Critical Aspects of Design for Future Smart Home Technologies. *ACM Transactions on Computer-Human Interaction* 29, 2 (Jan. 2022), 11:1–11:30. DOI: https://doi.org/10.1145/3485058

[31] Christine Geeng and Franziska Roesner. 2019. Who's in Control? Interactions in Multi-User Smart Homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, 1–13. DOI: https://doi.org/10.1145/3290605.3300498

[32] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 2017. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In *International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*. Lecture Notes in Computer Science, Springer, Cham, 656–674.

[33] 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. DOI: https://doi.org/10.1007/978-3-030-50309-3_26

[34] 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)*, 255–272. Retrieved from https://www.usenix.org/conference/usenixsecurity18/presentation/he

[35] 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 *ACM Conference on Human Factors in Computing Systems (CHI)*, 1–13. DOI: https://doi.org/10.1145/3313831.3376529

[36] International Nanny Association. 2017. 2017 INA Salary and Benefits Survey. Retrieved July 8, 2020 from https://nanny.org/wp-content/uploads/2021/11/2017-INA-Nanny-Salary-Benefits-Survey-FINAL.pdf

[37] 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. DOI: https://doi.org/10.1080/00141844.2018.1545794

[38] Bei Ju, Xiao Yang, Xiao Hong Pu, and T. L. Sandel. 2023. (Re) Making Live-in or Live-out Choice: The Lived Experience of Filipina Migrant Domestic Workers in Macao. *Gender, Place & Culture* 31, 12 (2023), 1–22.

[39] Omead Kohanteb, Owen Tong, Heidi Yang, T. Saensuksopa, and Saba Kazi. 2015. Decoding Sensors: Creating Guidelines for Designing Connected Devices. Retrieved March 7, 2018 from http://www.signifiers.io/summer.pdf

[40] Omead Kohanteb, Owen Tong, Heidi Yang, Thidanun Saensuksopa, and Saba Kazi. 2015. Signifiers.io – Guidelines for Designing Connected Devices. Retrieved February 26, 2018 from http://signifiers.io/signifiers/guidelines.html

[41] 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)*, Article 41, 14 pages. DOI: https://doi.org/10.1145/3411764.3445598

[42] Martin J. Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *ACM Halfway to the Future Symposium (HTTF)*, Article 5, 8 pages. DOI: https://doi.org/10.1145/3363384.3363389

[43] 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*, 1–7. DOI: https://doi.org/10.1145/3334480.3382972

[44] 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.

[45] Tama Leaver. 2017. Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online. *Social Media+ Society* 3, 2 (2017), 2056305117707192.

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

[47] 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*. Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.), Springer, 233.

[48] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used for?" Privacy Expectations about Smart TVs in the U.S. In *European Workshop on Usable Security (EuroUSEC)*. Retrieved from https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurousec2018_16_Malkin_paper.pdf

[49] 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), 250–271. DOI: https://doi.org/10.2478/popets-2019-0068

[50] 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)*. IEEE, 3043–3060.

[51] 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. DOI: https://doi.org/10.2478/popets-2020-0035

[52] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. 2022. "You Offer Privacy Like You Offer Tea": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households. (2022).

[53] 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 *International Conference on Mobile and Ubiquitous Multimedia (MUM)*, 83–95.

[54] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *the 20th International Conference on Mobile and Ubiquitous Multimedia*, 108–122.

[55] 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)*, Article 4, 11 pages. DOI: https://doi.org/10.1145/3419249.3420164

[56] Joseph A. Maxwell. 2010. Using Numbers in Qualitative Research. *Qualitative Inquiry* 16, 6 (2010), 475–482.

[57] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[58] 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)*, 5197–5207.

[59] Nicole Meng, Dilara Keküllüoğlu, 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 (Apr. 2021), 29 pages. DOI: https://doi.org/10.1145/3449119

[60] Nicole Meng-Schneider, Rabia Yasa Kostas, Kami Vaniea, and Maria K. Wolters. 2023. Multi-User Smart Speakers—A Narrative Review of Concerns and Problematic Interactions. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*. ACM, New York, NY, Article 213, 7 pages. DOI: https://doi.org/10.1145/3544549.3585689

[61] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L. Mazurek. 2023. Characterizing Everyday Misuse of Smart Home Devices. In *2023 IEEE Symposium on Security and Privacy*, 2835–2849.

[62] 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! (HCI)*. BCS Learning & Development Ltd., Swindon, UK, Article 18, 18:1–18:13 pages. DOI: https://doi.org/10.14236/ewic/HCI2016.18

[63] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. 2023. A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *Computing Surveys* 55, 9 (2023), 1–38.

[64] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurle, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, et al. 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)*, 26–40. Retrieved from https://dl.acm.org/doi/abs/10.1145/3532106.3535195

[65] 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 *ACM Conference on Human Factors in Computing Systems (CHI)*, 1649–1658. DOI: http://doi.acm.org/10.1145/2702123.2702164

[66] Julia Słupska, Marissa Begonia, Nayana Prakash, Selina Cho, Ruba Abu-Salma, Mallika Balakrishnan, and Natalie Sedacca. 2021. *Digital Privacy & Security Guide for Migrant Domestic Workers*. Technical Report. University of Oxford, King's College London, Voice of Domestic Workers, and Migrants Organise. Retrieved February 14, 2022 from https://domesticworkerprivacy.github.io/

[67] 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)*, 323–340.

[68] Luke Stark and Karen Levy. 2018. The Surveillant Consumer. *Media, Culture, and Society* 40, 8 (Nov. 2018), 1202–1220. DOI: https://doi.org/10.1177/0163443718781985

[69] Taro Sugihara, Kenichi Nakagawa, Tsutomu Fujinami, and Ryozo Takatsuka. 2008. Evaluation of a Prototype of the Mimamori-Care System for Persons with Dementia. In *Knowledge-Based Intelligent Information and Engineering Systems*. Ignac Lovrek, Robert J. Howlett, and Lakhmi C. Jain (Eds.), Springer, Berlin, 839–846.

[70] Kaiwen Sun, Yixin Zhou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2021. Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–41. DOI: https://dl.acm.org/doi/10.1145/3479858

[71] Janos Mark Szakolczai. 2021. "What Have You Caught?": Nannycams and Hidden Cameras as Normalised Surveillance of the Intimate. In *The Technologisation of the Social*. Paul O'Connor and Marius Ion Bența (Eds.), Routledge.

[72] Madiha Tabassum and Heather Lipford. 2023. Exploring Privacy Implications of Awareness and Control Mechanisms in Smart Home Devices. *Proceedings on Privacy Enhancing Technologies* 2023 (Jan. 2023), 571–588. DOI: https://doi.org/10.56553/popets-2023-0033

[73] 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)*, 3787–3798.

[74] 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 Conference on Human Factors in Computing Systems (CHI)*, 1–25.

[75] 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 *ACM Conference on Human Factors in Computing Systems (CHI)*, 1–13. DOI: https://doi.org/10.1145/3491102.3502137

[76] Peter Tolmie, Andy Crabtree, Tom Rodden, James Colley, and Ewa Luger. 2016. "This Has to Be the Cats": Personal Data Legibility in Networked Sensing Systems. *Proceedings of the ACM on Human-Computer Interaction* CSCW (2016), 491–502. DOI: https://doi.org/10.1145/2818048.2819992

[77] 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)*, 129–139. DOI: https://doi.org/10.1145/2632048.2632107

[78] U.S. Census Bureau and U.S. Bureau of Labor Statistics. [n. d.]. Current Populations Survey (CPS). Retrieved July 21, 2020 from https://www.census.gov/programs-surveys/cps.html

[79] Sandra Wachter. 2018. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security Review* 34, 3 (2018), 436–449. DOI: https://doi.org/10.1016/j.clsr.2018.02.002

[80] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring Tenants' Preferences of Privacy Negotiation in Airbnb. In *32nd USENIX Security Symposium (USENIX Security '23)*, 535–551.

[81] Sarah Widmer and Anders Albrechtslund. 2021. The Ambiguities of Surveillance as Care and Control: Struggles in the Domestication of Location-Tracking Applications by Danish Parents. *Nordicom Review* 42, s4 (Aug. 2021), 79–93. DOI: https://doi.org/10.2478/nor-2021-0042

[82] 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.

[83] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, New York, NY, Article 70, 16 pages. DOI: https://doi.org/10.1145/3544548.3581167

[84] Julia Wolfe, Jori Kandra, Lora Engdahl, and Heidi Shierholz. 2020. *Domestic Workers Chartbook: A Comprehensive Look at the Demographics, Wages, Benefits, and Poverty Rates of the Professionals Who Care for Our Family Members and Clean Our Homes*. Technical Report. Economic Policy Institute. Retrieved July 21, 2020 from https://files.epi.org/pdf/194214.pdf

[85] 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 *2023 ACM Designing Interactive Systems Conference (DIS '23)*. ACM, New York, NY, 1093–1113. DOI: https://doi.org/10.1145/3563657.3596012

[86] 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, CSCW1 (2023), 1–29.

[87] Anuo Yang, Shuangle Fu, Linping Liu, Changyu Fan, and Maitixirepu Jilili. 2022. Act Tough and Soft: Video Monitoring, Hongbao Gifts, and the Job Satisfaction of Domestic Workers. *Frontiers in Public Health* 10 (2022). Retrieved from https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.862162/full

[88] 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)*, 1–12. DOI: https://doi.org/10.1145/3290605.3300428

[89] 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. DOI: https://doi.org/10.1145/3359161

[90] 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)*, 65–80. Retrieved from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[91] 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 *USENIX Security Symposium (USENIX Security)*, 159–176. Retrieved from https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[92] 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.

# Appendix

## A Detailed Participant Characteristics

### A.1 Participant Characteristics: Nannies

The data in Tables A1–A4, covering demographics, job position and experience as a nanny, experience with technology, and exposure to devices, were collected via exit questionnaires after the interviews with our nanny participants.[15]

While our sample is not demographically representative of the U.S. population as a whole (especially with respect to gender), we include in Table A1 data for nannies specifically, to show that our sample is closer to representing the target group.

*Sources for Comparison Data.* Tables A1 and A2 include statistics from the following sources, for comparison:

***Economic Policy Institute (EPI)** Report*: A report by the EPI on the demographics and economic status of domestic workers in the U.S. [84], based on analysis of projection data from the **Current Population Survey (CPS)** conducted by the U.S. Census Bureau and U.S. Bureau of Labor Statistics (2017–2019 combined estimates) [25, 78]. Note that the CPS counts Hispanic/Non-Hispanic ethnicity separately from race, so EPI derives the ethnicity groupings we refer to in Table A1 (which parallel our participants' self-descriptors) by regrouping everyone of Hispanic ethnicity together, rather than using their race identifications.

***International Nanny Association (INA)** Survey*: The INA's 2017 survey of members [36] (N = 1,927). This survey was conducted internationally; however, 95% of the respondents were from the U.S., so we view it as providing a fair comparison.

[15] These four tables appeared in almost identical form in Bernd et al. [17].

Table A1. Demographic Characteristics of Nanny Participants, with Comparisons to Statistics from an EPI Report Based on Projection Data from the U.S. CPS [84], and to INA Statistics from an International Survey [36]

| | Participants | | *EPI Data* | *INA Data* |
|---|---|---|---|---|
| Demographics—Nanny Participants | N | % | % | % |
| *Age* (Range 19–55) | | | | |
| ≤ 22 | 3 | 12% | *36%* | |
| 23–39 | 17 | 68% | *37%* | |
| 40–59 | 5 | 20% | *20%* | |
| Median | | 30 | *26* | |
| *Gender* (participants' self-descriptors) | | | | |
| Female, Cis-female, F | 25 | 100% | *97%* | *97%* |
| *Ethnicity* (participants' self-descriptors) | | | | |
| White, Caucasian | 18 | 72% | *65%* | |
| Hispanic, Latina, Latinx, Mexican | 4 | 16% | *24%* | |
| Asian, Indian-from-India | 2 | 8% | *3%* | |
| No answer | 1 | 4% | – | |
| *Educational Attainment* | | | | |
| High school | 1 | 4% | *31%* | *11%* |
| Associate's/Some college | 9 | 36% | *33%* | *54%* |
| Bachelor's | 14 | 56% | *18%* | *28%* |
| Graduate degree | 1 | 4% | *4%* | *5%* |
| *Language Used with Friends and Family* | | | | |
| Mainly English | 20 | 80% | | |
| English and Spanish (about equally) | 3 | 12% | | |
| English and Gujarati (about equally) | 1 | 4% | | |
| Mainly Spanish | 1 | 4% | | |
| *Region of City of Employment* | | | | |
| West | 16 | 64% | *26%* | |
| Northeast | 4 | 16% | *20%* | |
| South | 3 | 12% | *32%* | |
| Midwest | 2 | 8% | *22%* | |

INA percentages are out of participants who answered a given question. EPI percentages and INA percentages may not add up to 100% due to rounding *or* due to additional categories/ranges beyond what we found.

Table A2. Job Situations and Career Trajectories of Nanny Participants, with Comparisons to INA Survey Statistics [36]

| | Participants | | *INA Data* |
|---|---|---|---|
| Job/Career Characteristics—Nanny Participants | N | % | % |
| *Current (Main) Position* | | | |
| Nanny | 15 | 60% | *57%* |
| Nanny/Household manager | 4 | 16% | *42%* |
| Professional babysitter | 3 | 12% | *N/A* |
| Au pair[a] | 2 | 8% | *< 1%* |
| Other | 1 | 4% | *1%* |
| *Current Employment as Nanny/Au Pair/Babysitter*[b] | | | |
| Full-time | 16 | 64% | *77%* |
| Part-time (with another job) | 5 | 20% | – |
| Part-time (also a student) | 2 | 8% | – |
| Part-time (no other job/not a student) | 1 | 4% | – |
| No answer | 1 | 4% | – |
| *All part-time* | – | – | *23%* |
| *Time Working for Current Employer(s)* | | | |
| < 1 year | 11 | 44% | *39%* |
| 1–2 years | 7 | 28% | *40%* |
| 3–4 years | 1 | 4% | *12%* |
| 5–6 years | 1 | 4% | *12%* |
| No answer | 5 | 20% | – |
| *Time in Nanny Career* | | | |
| < 2 years | 3 | 12% | *7%* |
| 2–4 years | 4 | 16% | *22%* |
| 5–9 years | 6 | 24% | *32%* |
| ≥ 10 years | 12 | 48% | *40%* |
| *# of Families Prtpt. Has Worked for* (Past and present) | | | |
| 1 family | 2 | 8% | |
| 2–3 families | 6 | 24% | |
| 4–7 families | 7 | 28% | |
| 8+ families | 10 | 40% | |
| *Plans to Continue Nannying* | | | |
| As a career | 13 | 52% | |
| As a short-term thing | 6 | 24% | |
| Not sure | 5 | 20% | |
| No answer | 1 | 4% | |

INA percentages are out of participants who answered a given question. INA percentages may not add up to 100% due to rounding *or* due to additional categories/ranges beyond what we found.

[a] The INA mainly serves nannies *per se*, not au pairs.

[b] The EPI report projects 52% of U.S. nannies are full-time and 48% are part-time [84].

Table A3. Technology Experience and Knowledge of Nanny Participants

| Technology Experience—Nanny Participants | N | % |
|---|---|---|
| *Technology Background* (Positive Answers, per Question) | | |
| Worked in a computer engineering or IT job position | 2 | 8% |
| Majored/minored in computer science or computer engineering | 0 | 0% |
| Has written a computer program | 0 | 0% |
| *How Often Participant Is Asked for Advice about Computers/Technology* | | |
| Rarely | 8 | 32% |
| Sometimes | 14 | 56% |
| Frequently | 3 | 12% |

Questions borrowed with modifications from Tan et al. [73].

Table A4. Number and Percentage of Nanny Participants Whose Employer(s) Has/Have Certain Smart Devices in Their Home(s) (N = 24) and Who Have Smart Devices in Their Own Home (N = 25)

| | Employers' Home(s) | | Own Home | |
|---|---|---|---|---|
| Current Device Exposure—Nanny Participants | N | % | N | % |
| *Device Types in Employers' and Own Homes* | | | | |
| Security camera(s) | 16 | 67% | 5 | 20% |
| Full security/alarm system | 12 | 50% | 3 | 12% |
| Individual spy cameras/nanny cams | 12 | 50% | 0 | 0% |
| Audio security monitoring system | 3 | 13% | 0 | 0% |
| Video or A/V baby monitor(s) (any type) | 18 | 75% | 1 | 4% |
| Audio-only baby monitor(s) (any type) | 6 | 25% | 0 | 0% |
| Smart TV(s)/streaming box(es)/home entertainment system(s) | 13 | 54% | 9 | 36% |
| Smart speaker/home assistant (with or without screen) | 16 | 67% | 6 | 24% |
| Smart speaker/home assistant with camera | 1 | 4% | 1 | 4% |
| Smart lock(s)/door(s) | 7 | 29% | 3 | 12% |
| Smart lights | 8 | 33% | 3 | 12% |
| Smart thermostat | 8 | 33% | 1 | 4% |
| Smart toy(s) | 8 | 33% | 1 | 4% |

One participant did not provide answers about their own home. If a device fell into more than one category, participants checked both. Answers for "Other smart devices" were re-categorized by the authors as all belonging to existing categories.

## A.2 Participant Characteristics: Parents

The data in Tables A5–A8, covering demographics, care situation, experience with technology, and exposure to devices, were collected via exit questionnaires after the interviews with our parent participants.

The parent sample is not representative of the general population in the U.S. People able to hire a nanny necessarily have higher incomes, which tends to correlate with a number of other demographic characteristics. People with young children are also likely to fall into a certain age range.

Table A5. Demographic Characteristics of Parent Participants

| Demographics—Parent Participants | N | % | |
|---|---|---|---|
| *Age* (Range 25–40) | | | |
| 23–39 | 15 | 94% | |
| 40–59 | 1 | 6% | |
| Median | | | 33 |
| *Gender* (Participants' Self-Descriptors) | | | |
| Female, F | 7 | 44% | |
| Male | 9 | 56% | |
| *Ethnicity* (Participants' Self-Descriptors) | | | |
| White, Caucasian, White American | 9 | 56% | |
| Asian, Asian American Pacific Islander | 5 | 31% | |
| Hispanic, Latino | 2 | 13% | |
| *Educational Attainment* | | | |
| Associate's/Some college | 3 | 19% | |
| Bachelor's | 7 | 44% | |
| Graduate degree | 6 | 38% | |
| *Language Used with Friends and Family* | | | |
| Mainly English | 15 | 94% | |
| English and Chinese (about equally) | 1 | 6% | |
| *Region* | | | |
| South | 7 | 44% | |
| West | 4 | 25% | |
| Midwest | 3 | 19% | |
| Northeast | 2 | 13% | |

Table A6. Care Situations of Parent Participants, and Past Experience Employing Domestic Childcare Workers

| Care Situation—Parent Participants | N | % |
|---|---|---|
| *Position of Caregiver* | | |
| Nanny | 14 | 88% |
| Au pair | 1 | 6% |
| Other | 1 | 6% |
| *Length of Current Caregiver's Employment* | | |
| <1 year | 6 | 38% |
| 1–2 years | 7 | 44% |
| 3–4 years | 1 | 6% |
| 5–6 years | 1 | 6% |
| 7–9 years | 1 | 6% |
| *Total Time Employing a Caregiver* | | |
| <1 year | 4 | 25% |
| 1–2 years | 7 | 44% |
| 3–4 years | 2 | 13% |
| 5–6 years | 1 | 6% |
| 7–9 years | 1 | 6% |
| 10–14 years | 1 | 6% |
| *Youngest Child Currently Being Cared for by Caregiver* | | |
| 6–12 months old | 2 | 13% |
| 1–2 years old | 4 | 25% |
| 2–3 years old | 2 | 13% |
| 3–5 years old | 4 | 25% |
| 5–9 years old | 4 | 25% |

Table A7. Technology Experience and Knowledge of Parent Participants

| Technology Experience—Parent Participants | N | % |
|---|---|---|
| *Technology Background* (Positive Answers, per Question) | | |
| Worked in a computer engineering or IT job position | 5 | 31% |
| Majored/minored in computer science or computer engineering | 4 | 25% |
| Has written a computer program | 4 | 25% |
| *How Often Participant Is Asked for Advice about Computers/Technology* | | |
| Rarely | 3 | 19% |
| Sometimes | 8 | 50% |
| Frequently | 5 | 31% |

Questions borrowed with modifications from Tan et al. [73].

Table A8. Number and Percentage of Parent Participants Who Have Certain Smart Devices in Their Home

| Device Exposure—Parent Participants | N | % |
|---|---|---|
| *Device Types Currently in Homes* | | |
| Security camera(s) | 11 | 69% |
| Full security/alarm system | 4 | 25% |
| Individual spy cameras/nanny cams | 5 | 31% |
| Audio security monitoring system | 2 | 13% |
| Video or A/V baby monitor(s) (any type) | 9 | 56% |
| Audio-only baby monitor(s) (any type) | 0 | 0% |
| Smart TV(s)/streaming box(es)/smart home entertainment system(s) | 12 | 75% |
| Smart speaker/home assistant (with or without screen) | 14 | 88% |
| Smart speaker/home assistant with camera | 1 | 6% |
| Smart lock(s)/door(s) | 5 | 31% |
| Smart lights | 4 | 25% |
| Smart thermostat | 6 | 38% |
| Smart toy(s) | 3 | 19% |
| Other smart devices | 2 | 13% |
| *Length of Time Owning a Camera/Security System* | | |
| <1 year | 2 | 13% |
| 1–2 years | 8 | 50% |
| 3–4 years | 5 | 31% |
| 5–6 years | 1 | 6% |

If a device fell into more than one category, participants checked both. Some answers for "Other smart devices" were re-categorized by the authors as belonging to existing categories.

Received 1 April 2024; revised 30 August 2024; accepted 3 September 2024