Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships

Julia Bernd, *International Computer Science Institute;*
Ruba Abu-Salma, *King's College London;* Junghyun Choy
and Alisa Frik, *International Computer Science Institute*

https://www.usenix.org/conference/soups2022/presentation/bernd

This paper is included in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).

August 8–9, 2022 • Boston, MA, USA

978-1-939133-30-4

Open access to the Proceedings of the Eighteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships

Julia Bernd
International Computer Science Institute

Ruba Abu-Salma
King's College London

Junghyun Choy
International Computer Science Institute

Alisa Frik
International Computer Science Institute

Abstract

Smart home cameras raise privacy concerns in part because they frequently collect data not only about the primary users who deployed them but also other parties—who may be targets of intentional surveillance or incidental bystanders. Domestic employees working in smart homes must navigate a complex situation that blends privacy and social norms for homes, workplaces, and caregiving. This paper presents findings from 25 semi-structured interviews with domestic childcare workers in the U.S. about smart home cameras, focusing on how privacy considerations interact with the dynamics of their employer–employee relationships. We show how participants' views on camera data collection, and their desire and ability to set conditions on data use and sharing, were affected by power differentials and norms about who should control information flows in a given context. Participants' attitudes about employers' cameras often hinged on how employers used the data; whether participants viewed camera use as likely to reinforce negative tendencies in the employer–employee relationship; and how camera use and disclosure might reflect existing relationship tendencies. We also suggest technical and social interventions to mitigate the adverse effects of power imbalances on domestic employees' privacy and individual agency.

1 Introduction

Privacy choices that individuals make regarding their own connected devices often affect the privacy of those around them. These knock-on privacy effects are becoming rapidly more urgent with the expanding use of connected smart devices—many of which are designed to collect data in what was formerly a prototypical private place, the home. In addition to collecting data about the primary user who installed it, a smart home device may also collect data about other members of the household, incidental visitors or bystanders, and potentially targets of deliberate surveillance within the home. These secondary "users" may have more or less power to control what data the devices collect about them, depending on their social and economic position relative to the primary user(s).

In this paper, we examine how social and economic power dynamics affect the privacy consequences of smart home cameras for domestic childcare workers. Childcare workers such as nannies, au pairs, and professional babysitters may sometimes be incidental bystanders to data collection, as a result of increasing use of smart home technology in general [118, 125]. And they may sometimes be deliberate targets of monitoring by their employers—a practice that is becoming more expected, at least in some places [35, 43, 57, 127].[1] This case study of nannies contributes to a growing body of work on how socio-economic power differentials may result in differential privacy outcomes for different types of people.

In this research—the first on smart home privacy for domestic workers in the U.S.—we focus on nannies because they operate in a complex, multi-layered context that blends disparate sets of potentially conflicting norms and priorities about data collection and sharing [cf. 4, 17].[2] In addition to being a home, where the residents tend to have more control over decisions about technology (or whatever else) than they do elsewhere, the smart home is also the nanny's workplace. This may imply a different set of data norms, and control over any aspect of the environment is also mediated by the employer–employee relationship and its power dynamics. Finally, it is

[1] In this paper, we refer to domestic childcare workers as "nannies", and the job as "nannying", for the sake of brevity. But our study included au pairs and professional babysitters as well, and findings are based on all participants.

[2] Brief preliminary findings based on interviewers' impressions were previously published as a work-in-progress workshop paper [17]. This paper is the first full publication based on systematic analysis of the transcripts.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

a care situation, which complicates the usual professional divides—and at the same time may imply a different balance between the employer's safety concerns and the employee's privacy, compared to other workplaces.

Within this blended context, this paper focuses on the effects of cameras (as opposed to other devices), because they have unique implications in terms of power dynamics and employer–employee relationships. Employers may use camera data in a way that affects nannies' day-to-day experiences of their job, as well as their job security [cf. 35, 53, 122], while devices such as smart speakers or smart thermostats rarely have such uses.[3]

This paper addresses the following research questions:

1. How are domestic childcare workers' privacy attitudes, experiences, expectations, concerns, and choices with regard to working with smart home cameras shaped by their relationships with their employers?
2. How do employers' use of and interactions with employees about cameras reflect, reinforce, or change existing power dynamics in those relationships?
3. What are potential points of intervention (social and technical) for mitigating the effects of power imbalances on how domestic childcare workers' privacy preferences are enacted with regard to smart home cameras?

Based on a qualitative analysis of 25 interviews with nannies, au pairs, and professional babysitters in the U.S., we show how privacy attitudes and expectations in a domestic childcare context may be affected by power differentials and norms about who makes decisions about data flows in a given context, as well as childcare workers' specific concerns about how their employers may use the data. We also show how nannies' ability to exert control over their data is limited by both social norms and practical economic considerations. In the process, we identify potential points of intervention to mitigate the privacy effects of power differentials. We suggest corresponding solutions that focus on promoting and improving communication between employers and employees about camera use, supporting technical and social designs that are not only privacy-enhancing but also agency-enhancing.

2 Related Work

User and Bystander Privacy in Smart Homes Researchers have explored primary users' experiences, perspectives, expectations, and privacy concerns with regard to smart home devices' data practices [e.g. 1, 14, 23, 51, 93, 128, 138, 139, 140, 147] [overview in 72]. Many studies focus on how particular situational factors shape people's attitudes and concerns with regard to data collection, use, and sharing [e.g. 7, 38, 44, 67, 68, 81, 82, 94]. Most studies that compared locales have found that people are more sensitive about devices gathering data in their homes than, for example, in their workplaces or in business establishments [e.g. 4, 27, 67, 94, 112] [*contra* 45]. Consequently, several questions about privacy preferences and concerns arise when one person's workplace is also another person's home.

Researchers have used the Theory of Privacy as Contextual Integrity (CI) [15, 96, 97, 98] to examine how people reason about data collection that blurs or crosses the boundary between private and public contexts (e.g. home vs. Internet, [e.g. 7, 77, 141]). From the intersection of these contexts, new ideas about privacy and power can emerge [20]. CI asserts that it is the *context*, or particular social situation, that dictates norms about digital privacy and acceptable data sharing. Information redistribution that is considered appropriate in one situation may be too sensitive or a violation of privacy in another. If there are power imbalances, CI analysis can also uncover how the parties in a given context negotiate conflicting norms [e.g. 16, 55, 56, 63, 64].

Most research on smart home privacy preferences and expectations has focused on people's views as primary users—including their concerns about bystanders [e.g. 52, 145, 146, 147]. However, secondary users of various kinds have recently received more research attention. Research on multi-user smart homes shows the complexity of balancing differing privacy preferences of household members [e.g. 6, 40, 42, 51, 60, 62, 144, 148]. In some cases, research on residents of smart homes has also noted potential issues for non-residents [e.g. 23, 26, 65, 81, 82, 106, 117, 128].

Other work has focused more closely on visitors and guests as bystanders, including Airbnb guests [29, 84, 123]. Situations in which people become smart home bystanders are very common, and span a variety of social and employment contexts [25, 85, 91]. Even if bystanders know devices are present, they often have incomplete or incorrect ideas about the extent of data collection and use [3, 4, 85, 86], and they may not have socially appropriate ways to express their privacy preferences even when they understand the implications [3, 4, 53, 86, 144]. Some of these studies suggest technical and/or social solutions to these issues, some of which will be described later in this section.

Privacy and Social and Economic Power Discussions about technology and social and economic power rest on a substantial body of work on the digital divide. Research on digital inequalities [e.g. 22, 39, 109, 114, 136, 150] [for IoT: 73], and on demographic differences in online privacy knowledge, behaviors, and attitudes [e.g. 30, 49, 80, 100, 132, 133, 134], has shown how vulnerabilities arise from such differences [e.g.

[3] We compare nannies' experiences, views, and adversarial models with regard to cameras vs. other smart home devices in a forthcoming paper.

24, 46, 49, 100] [for IoT: 10, 47, 103]. Existing power imbalances between those who collect data and those data is collected from mean the disadvantaged tend to have less control over their privacy [e.g. 5, 19, 24, 33, 78, 83, 111, 115, 134]. Collected data can then lead to further discrimination [e.g. 79] [for IoT: 31, 103].

Power imbalances and accompanying privacy vulnerabilities can play out in employer-employee relationships within surveiled workplaces, creating complex trade-offs [11, 69, 137] [for IoT: 9, 75, 78, 99] [for care contexts: 18, 71, 124]. These trade-offs are especially prominent with in-home work [4, 53]. For example, where parents use nanny cams as a means of control [35], it can result in evasion [4, 53], and may also reduce nannies' capacity to deliver the best care [53]. We compare findings from our study with other research on domestic workers in smart homes in §6.2; however, there are no published studies from the U.S. Additionally, our study adds depth in aiming to understand the relationship between smart home privacy and employer–employee power dynamics.

Smart devices can also affect family or household dynamics in multi-user smart homes. For example, Apthorpe et al. [6] found that IoT devices benefit interpersonal relationships (e.g. easing household management) but also cause interpersonal conflicts (e.g. facilitating surveillance, causing distrust, causing disagreements over device use). On the other hand, the question of exactly who has control over devices in the home may be an indicator of existing interpersonal and/or sociocultural dynamics [42, 53, 61, 63, 64]. In extreme scenarios, imbalances in device control can enable domestic abuse [36, 53, 70, 76, 101, 116]. If there are children involved, smart home devices [13, 66, 113, 126] and smart toys [8, 90] can turn children into targets of or bystanders to data collection.

Protections for Bystander Privacy Proposals for or attempts to implement stronger bystander protections have focused on detecting hidden cameras [e.g. 21, 74, 102, 123, 131] or clearly signaling that a device is recording or transmitting data [e.g. 3, 4, 23, 25, 32, 54, 59, 85, 86, 105, 108, 128, 129, 143, 147]. Others have proposed using objects [e.g. 2, 119] or contextual cues (such as people's locations, presence of multiple people in a room) [e.g. 12, 51, 65, 92, 95, 104] to signal preference to obfuscate or not record data about bystanders at all. However, there are limitations to such technical approaches, and not all users trust manufacturers or service providers to implement them [58, 65, 149].

There have been calls for more granular smart device settings to accommodate the privacy interests of different parties in the same household [6, 40, 42, 48, 50, 50, 51, 63, 65, 91, 105, 130, 135, 143, 144, 148]. For instance, parents have expressed interest in nuanced parental controls that would allow children to use devices without compromising safety [6, 126]. Other potential design practices for increased bystander protections—which could especially benefit domestic employees, if extended—include simplifying the privacy control process [148] and expanding the platforms through which smart controls can be adjusted [3, 42, 60, 86, 143, 148]. Besides technical implementations, other suggestions include raising awareness of smart device function [4] and facilitating more open and transparent conversations about device usage between primary users and bystanders [25, 128, 144, 148].

Such recommendations, however, were not made with specifically domestic workers in mind. We expand upon these recommendations, and suggest our own interventions to address the privacy concerns of domestic workers and power imbalances with their employers, in §6.3.

3 Methodology

We designed and conducted semi-structured interviews with 25 domestic childcare workers (including nannies, babysitters, and au pairs) in the U.S. in late 2019.[4] The Institutional Review Board (IRB) at University of California, Berkeley, reviewed and approved our study, and we obtained written consent from participants.

Data Collection We used a mix of offline and online recruitment. We distributed flyers in cafes, daycares, schools, colleges, and playgrounds. We also advertised in nanny-specific Facebook groups, Reddit communities, and other online venues, and used snowball sampling. We recruited both individuals who had worked with cameras and those who had not.

Our interviews included warm-up questions about participants' nannying experiences and relationships with their current and past employers. We next asked about participants' personal experiences working in houses that had cameras, and discussions with their employers about the cameras. Other questions included participants' expectations, attitudes, privacy concerns, and choices they had (or would have) made related to camera use and disclosure, as well as their knowledge of legal and technical protections. When participants had not had specific experiences, such as working with cameras or finding hidden cameras, we probed hypotheticals to explore their views. We also administered an exit questionnaire covering demographics, experiences with technology, current employment situation, and what smart devices they and their employers owned.[5]

[4] In parallel, we also conducted 15 interviews with parents who employ nannies. Information on those interviews may be found in Bernd et al. [17], and results will be published in a future paper.

[5] Our recruitment materials, screening scripts, interview scripts, and exit questionnaires can be found at https://bit.ly/3zIEpov, so that other researchers can use them in related work (as some already have).

We conducted one pilot to finalize and prioritize questions. Interviews took 1 to 1 1/2 hours. Two were in person and the rest were by phone or video chat. We compensated participants $50. Interviews were professionally transcribed.

Data Analysis We used inductive coding to identify common topics and themes in our qualitative data. To develop an initial coding frame, three researchers each independently coded a separate test transcript using MAXQDA. The three researchers then discussed their coding frames and merged them after resolving disagreements. These researchers and an additional researcher then independently coded two more transcripts (the same ones) to test the merged frame. After making further changes to the coding frame, we divided up all the interviews (including the test transcripts) so that each transcript was coded by two researchers, continuing to check agreement and discuss questions about code application throughout.[6] No further codes were identified, indicating saturation.[7] All four researchers participated in organizing codes into themes specific to addressing our research questions. We all reviewed the excerpts on each topic to further refine the themes.

Limitations Study materials and interviews were in English. All participants were comfortable conversing in English, but some did not speak it as their first language; 20% spoke another language primarily or equally. This may have increased the possibility of misunderstanding. We may also have missed insights about the effects of limited English fluency on communication and power imbalances for U.S. nannies that we could have captured by offering interviews in other languages.

Around 28% of domestic childcare workers in the U.S. are immigrants [142], and we believe that understanding the experiences of immigrant workers is key to understanding power imbalances and privacy in the workplace [cf. 46]. We do not know whether our sample was representative in this regard, as we did not ask about immigration status. (We did not believe the limited scientific benefit would outweigh distress undocumented participants could have experienced at the question.) Immigrant workers may be less likely to take part in studies, due to language barriers or—especially for those with precarious immigration status—enhanced privacy concerns [e.g. 28, 107]. As we describe in §6.4, this qualitative work should be expanded and quantified, increasing generalizability with multiple languages and focused recruitment of immigrants.

[6] We checked agreement rates to ensure coders were using codes similarly. We do not report formal agreement measures as we do not make quantitative claims [cf. 89]. Rather, we aim for transparency and thick description [41].

[7] A text copy of the codebook can be found at https://bit.ly/3aEDRoU, or as a MAXQDA file upon request, again so it can be used in future comparative research.

4 Participants

Demographics and Job Experience With the potential exception of immigration status, our sample is representative of the demographics of nannies and childcare workers in the U.S. Participants' ages ranged from 19 to 55, with a median of 30. All participants self-identified as female/women. Asked to self-describe ethnicity, 72% said white or Caucasian, 16% Hispanic, Latina/x, or Mexican, and 8% Asian or Indian-from-India. Most participants were either nannies (60%) or nannies/household managers (16%), while 12% were professional babysitters and 8% were au pairs. 4% had other similar nannying jobs. Additional details about participant demographics (and comparisons with the target population) may be found in Bernd et al. [17], Appendix A.

Experience With Cameras 22 out of 25 participants had worked with indoor cameras on while they were present. All who had worked with cameras had encountered livestreaming ones, usually Internet-enabled. Most had worked with cameras that recorded (often simultaneously streaming), though some recorded only when triggered. (The other participants were not sure about recording.) Cameras were most commonly located in children's bedrooms/playrooms and entryways, and some in common areas.

5 Findings

In this section, we describe how smart home cameras intersect with the employer–employee relationship and its power dynamics in an in-home childcare context. In §5.1, we discuss participants' privacy attitudes and concerns about how cameras *reflect* the employer–employee relationship—i.e. what camera use or disclosure may indicate about employers' attitudes toward the nannies or the operation of power dynamics in the relationship (RQ1). At the same time, many participants were concerned about how cameras could *affect* the employer–employee relationship, e.g. by reinforcing power dynamics or encouraging parents to be critical of nannies (RQ2); we discuss these perceptions in §5.2. However, as we discuss in §5.3, potentially-conflicting contextual norms about control of information flows constrained participants' ability and desire to make choices about their collected camera data (RQ1, RQ2). In §5.4, we show how participants' choices with regard to accepting or restricting data collection (including whether to accept a job at all) could be either motivated or constrained by the power differentials in those relationships (RQ1, RQ2). Throughout our analysis, we saw that purposes of data collection and how data was used were central themes—in particular, whether the purpose of the camera was related to the nanny's employment and job prospects. Some of the views discussed in this section implicate potential *points of intervention*, where intervening could have substantive effects on nannies' experiences with cameras (RQ3).

5.1 Cameras Reflecting Employer–Employee Relationships

With a well-matched family, participants said they could build a good working relationship with the parents, and strongly bond with children: "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) Participants considered mutual trust, respect, and open and honest communication as essential components in building a common ground and effectively resolving disagreements. Our participants often expressed opinions about how cameras, or interactions around cameras, might illuminate or *reflect* those important relationship values.

5.1.1 Cameras and Trust

What cameras signaled about trust was a frequent theme. Many participants viewed cameras as at least a *potential* sign that parents might not trust them:[8] "I think [the cameras] made me a little bit more cautious about if they trust me or not." (N36)[9] (Participants occasionally mentioned specific ways parents might not trust them, such as not trusting them to be attentive, but usually phrased it more generally.) However, participants had more nuanced perspectives on the likelihood that a camera signaled distrust and how uncomfortable they were with it, depending on the specific context.

Some participants viewed cameras fairly broadly as a sign of outright mistrust, to a degree that always made them uncomfortable: "It's just a feeling, like, that you're not trusted and you're being watched." (N33) Some were concerned about lack of trust when the camera's purpose was specifically to monitor or even micromanage the participant: "*[Interviewer: If the main reason was actually to check in on you, how would you feel about that?]* [...] I would be uncomfortable. Cause again, I think the whole circumstances of the nanny and the family is the trust and the communication." (N37)

Different participants also noted that their judgment about whether cameras indicated a lack of trust might depend on how often employers checked the cameras or how many cameras were in the house: "I wouldn't be comfortable working in a home where there are cameras in all of [...] the communal spaces, like the living room and the kitchen [...]. And if those cameras are being monitored constantly. I just wouldn't be able to relax ever and I wouldn't feel trusted at all." (N6) In particular, some participants did not view it as a serious trust problem even if the employers said the cameras were there to monitor the nanny, as long as it really seemed to be a just-in-case protection rather than constant monitoring: "I don't have a problem with there being observational devices. [...] But if they felt the need to monitor me 24/7, [...] I would be uncomfortable with that, because that shows us a level of distrust that would make me probably leave and go find another position." (N14)

A few opined that a trust gap at the beginning was not unexpected, but that trust should build over time and be reflected in decreasing camera use: "[An employer should] maybe consider using it only as the trust is being built. And then, once [...] she realize[s] that she can trust this person, then to stop using the cameras." (N19) However, some worried that employers who frequently used cameras might end up relying too much on them: "I would see something parents need to avoid would be to use [cameras] to build trust as opposed to actually building trust with the person." (N14)

5.1.2 Disclosure and Respect

Mentions of trust *per se* did not necessarily explicitly relate to power dynamics (though such dynamics might be implicit, in who had power to entrust whom with what). However, trust was often discussed together with other relationship aspects with more clear power implications, such as respect: "[If] a camera just shows up all of a sudden one day without any discussion, that's not gonna make me feel very trusted and like they respect my profession." (N27)

With both trust and respect, participants had a range of views on whether having cameras in itself was a bad sign—and some noted the meaning was changing as smart homes became more popular: "Earlier in my career, it was very odd to see a camera in a house, and it meant that a family didn't trust you. But now it's become so much more commonplace." (N27) However, opinions of *undisclosed* cameras tended to be more negative—and in particular, not disclosing cameras to a nanny was seen by many participants as a bad sign in terms of relationship values like trust, respect, and good communication: "That would feel better [if employers had disclosed their cameras] because [...] you can see a good communication between you and them." (N15) An undisclosed camera could make someone feel untrusted even when they believed the camera was not there to watch them: "They never told me that they have [cameras]. [...] I understand that they don't have them for me, they have them for the children, they're like, you know, cameras to watch the kids, so... But I had that feeling of feeling, like, not trusted." (N36)

In particular, several participants drew a strong connection between disclosure and respecting or valuing the nanny: "I have no problem being recorded as long as you're telling me you're doing it. You know, as long as there's some respect for privacy. [...] Respecting you enough to let you know." (N10)

A few participants also viewed parents' sharing of data with others through the lens of respect: "*[I: Do you know if either of*

[8] As this research is qualitative, we did not try to count and verify the number of participants who expressed a given view. We use words like *most*, *many*, *some*, or *a few* only to give a rough insight into prevalence.

[9] Numbers run higher than 25 because we assigned them when contacting potential participants to set up interviews; some did not follow through, or canceled.

[your employers] have ever shared any recordings or showed anybody what was happening?] I don't know but I would be shocked if they had. *[I: Why would you be shocked?]* Because they respect me." (N20) Others were less concerned about sharing generally, though they might draw inferences about employers' attitudes if it was done without consent: "If they've already shared [camera footage] without my consent, I would kind of assume that they are finding an issue with my work in some way." (N7)

5.2 Cameras Affecting Employer–Employee Relationships

In addition to being an indicator of relationship tendencies, cameras can also actively *affect* relationships. Nannies' expectations or concerns about how cameras might change their relationships with their employers—positively, negatively, or not at all—could, in turn, affect participants' privacy attitudes about cameras: whether they were comfortable, uncomfortable, or simply resigned.

5.2.1 Uses, Power Implications, and Discomfort With Cameras

Participants' attitudes about cameras (including attitudes about audio vs. video) often depended on the employer's camera usage. Such attitudes were often entangled with how camera usage and purpose impacted power dynamics and relationship quality. Even nannies who might generally be comfortable with cameras in an employer's home might be less comfortable if they thought the devices could facilitate or exacerbate poor treatment or intrusive supervision: "If the purpose is to babysit me while I'm nannying the children, then I really feel uncomfortable with that." (N37) However, there was notable variation amongst participants in what they considered intrusive supervision.

Catching the Nanny Out Cameras could reinforce existing power imbalances by giving employers new evidence to excuse firing a nanny over small infractions: "I [got] fired over the cameras last summer, or that was their official excuse. Because they denied unemployment cause they said I got fired 'for cause' instead of, 'she's not Christian' or whatever. [...] Other ladies have also had [...] personality conflicts [...], and then all of a sudden there's something on the camera that they do, because the parents are watching [...] for the first wrong thing that's a little bit out of line." (N27) Even participants who had not been fired could be concerned they might be: "If I curse in front of an audio system, even if I'm not with their child, I could get fired." (N3) Concerns about employers trying to catch nannies out were amplified when cameras were not disclosed: "'We have hidden this camera because we believe that you will be lying to us,' is the message that I get when I see or suspect a hidden camera." (N29)

Cameras could also make nannies nervous about their perceived job performance, or make them feel as if they had to perform for an audience [cf. 128]: "I could see [the camera] turn, it would make me feel extremely uncomfortable. [...] It would almost feel like I'm putting on a show." (N16)

Micromanaging Many participants mentioned that nannying provided them with more autonomy and flexibility than other jobs; however, this benefit could be undermined by excessive supervision. How cameras enabled or even encouraged micromanaging was a major concern for many participants. Some participants explicitly discussed the power implications of micromanaging: "I'm a grown adult. They don't have their boss sitting at their desk watching them do the minutia of their day. I deserve to be treated with the same amount of respect." (N3)

Even when power was not mentioned, the term *micromanaging* evoked the employer's ability to exert additional and unwelcome control over the employee: "So long as they're not using the cameras to micromanage. I've had friends who get [...] little messages throughout the day to show that the parents are watching and criticizing their work." (N29)

Participants were especially uncomfortable with micromanaging via camera when it was used to enforce completion of tasks unrelated to childcare: "If I had just done anything [with their child] that they didn't like, that would be okay [for employers to talk about something they saw on-camera]. But if it was something really nitpicky or if it was something like, 'Oh, I saw that when our daughter was napping, you were on your phone. Can you clean the kitchen next time?' that would be something [...] I would take more offense to." (N26)

"Spying" or Illegitimate Use The connection between camera purposes and power also played out in discussions about employers using cameras for "spying", a term that had different meanings for different participants. In addition to using that term to refer to undisclosed cameras generally, a few referred to it as "spying" when employers observed them when they were not directly with the kids. Such nannies were comfortable with being monitored only while they were with the kids (because then they did not view it as spying on them): "When they're doing it to spy, then I'm less comfortable about it. [But], if it's centered around the kids, I'll accept most explanations." (N7)

Some participants even viewed it as "spying" if they were monitored via camera while they were with the kids: "When you feel like you're being observed by camera, that's different. That's an invasion. [...] If you're watching your nanny do something and then you text her [...] [about something you saw], that's different than if you notice something in the house. That feels like you're being spied on." (N12)

Abuse In addition to concerns about how cameras could negatively impact supervision practices, some nannies were concerned that cameras provided the means for intimidating or creepy behavior: "If they were watching me [when] I wasn't even with the child, I probably would leave the job. [...] When you're in someone's house, it's their territory. And when they make that unsafe [...] I just wouldn't feel comfortable in their house again." (N26)

Risks could be higher for employees who belonged to more vulnerable populations or who knew less about the technology (discussed further in §6.2): "A lot of nannies are older and they might not even understand what some of this technology is, and how it's used. [...] A lot of domestic workers don't speak English very well. A lot of domestic workers are from different countries. So, there's a lot of potential for vulnerable populations to be taken advantage of using this technology." (N27)

5.2.2 Disclosure, (Dis)Trust, and Mitigating Discomfort

One participant pointed out that hidden cameras in particular aroused suspicions of harassment, whatever the actual reason for nondisclosure might be, and connected it to the equation of disclosure with respect: "I don't want to be giving anybody a private show by accident and not know. [...] I don't think it's respectful to have a camera and hide it. [...] Like it just feels creepy." (N16)

Several participants highlighted how undisclosed cameras—or undisclosed uses of disclosed cameras—could erode the participant's trust in parents: "I would feel like [a camera is] a violation of my trust and my privacy if I don't know about it." (N20) On the flip side, some participants noted that disclosing cameras and their purposes could facilitate nannies' trust in their employers' intentions and attitudes, and thus reduce their discomfort with cameras: "If they give me a good explanation [...] I am generally okay with that. It's the hiding of it, and then the spying, and the saying that it's all just so they can look at the kids, when [...] they would not have those cameras if there was not a nanny present. [...] There needs to be two-way communication, so that I feel trust, so that I can provide good care while still feeling watched." (N7)

However, a few participants preferred their employer *not* disclose, to avoid the discomfort of feeling watched: "I don't want to know [whether it captures audio], because I don't want to be self-conscious. I want to do my job without thought of the camera." (N12)

A couple of participants also mentioned that discomfort or concerns about potential problematic use of cameras could be averted if data were not retained indefinitely: "It just seems like there's less potential for abuse or misusing a camera if you can't [...] save tons and tons of video." (N18)

5.2.3 Power and Comfort With Cameras

A few participants expressed positive views of cameras based on their benefits to relationships, such as how cameras might support good communication and employers' respect for them as professionals: "What I try to do when there are cameras around is to model for parents how I would handle situations. So, if [the cameras are recording audio] the parents can hear what I'm saying to their child, [...] that's all the better. [...] And it's also a way of making sure that we're on the same page." (N32)

Relationship benefits like increasing trust might be traded off against potential sources of discomfort: "[Having cameras] gives them the sense [...] that I am who I am with their kids, and who I said I was at the interview. And that's why I kind of don't mind the cameras, in a big sense? [...] [Even though] you're conscious of how you look and [...] all these little things, [...] they don't really bother me." (N12)

Another mentioned benefit was that if something went wrong where the nanny was not at fault, cameras could provide exculpatory evidence: "If [the child] runs and falls and smacks her head and gets a bruise, there's now proof on camera that I'm not the one who caused that to happen. [...] So I definitely prefer working with cameras." (N20) Further, cameras could mitigate some of the negative consequences of a difficult dynamic, by providing evidence when the nanny would have no other recourse against an employer looking for an excuse to reprimand or fire them: "That way, they can't say, he said, she said. It's on the footage." (N40)

A few nannies expressed comfort with cameras not because of work relationship benefits, but because they had not experienced negative relationship effects with their current employer: "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)

5.2.4 Social Factors in Privacy Resignation

Often participants were resigned to camera data collection because it accorded with the norms for employee–employer or caregiver–child relationships; we describe these norms in §5.3.

A couple of nannies pointed out that cameras could reinforce a general dynamic they were already resigned to, where being in someone else's home compromised their privacy: "For the most part, there's no breaks. So, there's no privacy. [...] Last month, my aunt passed away [...] and at an office job, I might have taken the day off to maintain some privacy. [...] And I feel like I'm overstimulated by kids clinging onto me, no privacy. And then when you add cameras in the home, there's no privacy." (N7)

5.3 Prerogatives and Privacy Expectations

Our participants often phrased their expectations about cameras in terms of *prerogatives*. In these examples, participants' expectations were based on privacy norms about who had the prerogative to make decisions about data collection and sharing in a given situation—where those privacy norms were part of a broader set of social norms about who made decisions in that situation [cf. 3, 88, 110].[10]

As we noted in §1, domestic childcare work combines three contexts with different norms about information sharing—home, work, and caregiving [cf. 4, 17]). We observed three common ways of framing prerogatives to control data flows, loosely related to those three contexts. First, participants could see it as *the homeowners' prerogative* to install what technology they chose and use it how they liked, and to protect the safety of their homes. Second, it could be *employers' prerogative* to dictate working conditions and rules. Finally, some participants viewed it as *parents' prerogative* to make choices about how to protect their children's safety, or to keep track of what is happening with their children.

The examples below are roughly grouped according to home, work, and caregiving contexts, but many explicitly highlight the tensions that arise from the overlap—and it is worth noting that participants did not always endorse prerogatives, even when they referred to them as norms.

5.3.1 Homeowner Prerogatives and Home as Baseline

Some participants explained their acceptance of cameras by invoking homeowner prerogatives as an *a priori* assertion, without further explanation: "We have to respect too that we are not in our house, you know, so..." (N15) For some participants, homeowner prerogatives (or device-owner prerogatives) also precluded negotiation about specifics (see §5.4.2): "*[I: Do you feel like parents should ask nannies if there's any preferences that they have about the privacy settings? [...]]* No. It's your camera. It's your life." (N16)

A couple of participants invoked the home context in explaining that they understood the use of cameras for monitoring because it could be difficult or strange having someone in your home: "It doesn't get any more personal and private than your home. That's where you go to retreat from the world. If you need a camera there because there's a stranger..." (N16) Other participants were resigned to having less control in someone else's home—especially if it was also a workplace: "I feel that there's a level of relinquishment of my privacy here in the house when I'm working in somebody else's home; I recognize that that is part of the job." (N4)

[10] In general, we assume that someone's *privacy expectations* in a given context are a result of their individual *past experiences* with information flows in that context, their *accumulated knowledge* of how information usually flows in that context, and the *social norms* they are aware of about how information should flow in that context.

As a counterpoint, some viewed cameras as potentially concerning because they felt out of sync with general expectations of privacy when in someone's home: "Like just blowing noses, or just like random stuff like that, that you think, 'Oh, I'm in someone's house. Like, it's private. I'm fine.' But it's not private, you know, cause you're on camera. So it's stuff like that that I've had to just think twice about." (N26)

In particular, the difference between a home and other workplaces made some nannies feel personally targeted: "The daycare center is [...] less sort of, targeted because there's lots of different kids and I assume [...] different employees instead of just sort of the more one-on-one kind of thing." (N19) A few thought that cameras were *less* expected in a home-based care situation because of the close relationship: "I feel like in a daycare, camera, it's more normal cause [...] you don't have a personal relationship. [...] It's just like a standard. Whereas, if people are trusting you to be in their house with their kids, that's different to me." (N18)

Several nannies also pointed out how their presence disrupted the privacy the *parents* might expect in their home [cf. 86, 91, 127]: "You're in somebody's home, it's their privacy. [...] I am learning a lot of very intimate details about their lives that they might not show to the outside world." (N29) A couple of participants viewed cameras as a sort of trade-off for this, even if they would have preferred to work without cameras: "We're kind of like outsiders here, in their private home. So we need to maybe give in a little bit of our privacy." (N10)

5.3.2 Employer Prerogatives and Workplace as Baseline

Some participants mentioned they would expect to be monitored by their employers in any workplace: "It's not isolated to domestic work; I think that it is not terribly uncommon to work with a camera. [...] I don't expect privacy necessarily while I'm working." (N4) However, the same participant referenced workplace-based privacy norms she felt should be respected even in a private home: "Because it also your job, for you as a nanny it feels more like a public area, because [...] you're in somebody else's private space, that for you is a workspace. So, I do think that it's important to know when and where there are cameras, for basic privacy reasons." (N4)

Several nannies pointed out that differences between privacy norms in a home and a workplace caused them to evaluate home cameras differently from other workplace cameras: "*[I: Do you feel like [having cameras] is different in a [preschool] versus if it was in somebody's house?]* Yeah. [Laughs] Yeah, because it's their house. I mean, like I said, it's something more personal. But, the job is your professional job. [...] This is the difference." (N24) For this participant, N24, being a live-in au pair—where her employers' home was also hers—introduced additional needs: "If I don't live there, I don't care [whether the camera collects audio], but, I'm going to live, like an au pair, [...] I prefer just video." (N24)

The tension between expectations based on home norms versus workplace norms manifested in several ways, such as what counted as public versus private space: "I think making sure that the current laws are more clear on what is a private area versus a public area when a home becomes a workplace would be great, [...] especially for live-in nannies, and where they can be recorded and stuff like that." (N3)

5.3.3 Parental Prerogatives and Shared Caregiving as Baseline

Many participants said that they expected and accepted monitoring at least in part because it was a care situation, and parents were expected to prioritize their children's safety: "It's their home and their children, and they have every right to do whatever is in their power to keep their children safe, and if they think that includes video recording, then that is their right." (N29) Some framed it more generally as parents' prerogative to make decisions about their children's care: "That is pretty much my feelings on cameras. It's your house. It's your child. You can raise it and do whatever you choose to. [...] I'm not gonna judge a parent on that." (N16)

In some cases, participants discussed power dynamics and prerogatives negatively, in terms of potential harms or constraints on their choices (see §5.4). However, especially when talking about the care relationship and parental prerogatives, some participants said their understanding of prerogatives made them less uncomfortable with monitoring: "I understand the big brother overtones, but I also understand that parents want to be able to see if their children are doing okay while they're in the care of somebody else. So it doesn't bother me, because I recognize my role in the house." (N4)

While most of the discussion of prerogatives and power dynamics situated the employers as having the most power in the relationship (with nannies having, at most, the power to choose to leave), a few participants highlighted that—whatever the economics of the situation—parents might feel like they were losing power by relinquishing control of their children and their homes: "I understand that in someone's home, I'm by myself. If I choose to [...] abuse a kid, there's no one to stop me. So I understand the need for cameras in that sense, where I have all the power with their child." (N26)

5.4 Power Dynamics Motivating and Constraining Privacy-Related Choices

Participants sometimes made job choices based on how their employers used cameras. But at the same time, their ability to make choices or express preferences about camera data collection was constrained by the power dynamics of employer–employee relationships.

5.4.1 Power Implications Motivating Job Choices

As we described in §5.1 and §5.2, participants were concerned about both what cameras could indicate about their relationships with their employers, and how they might affect those relationships. Those factors might affect whether a nanny accepted a job, or kept a job they had, in a house with cameras. For example, participants might quit or consider quitting a job when video surveillance exacerbated the problem of micromanaging: "That's actually a reason why I left my previous nanny family. They would constantly check the cameras and text me on certain things that they would do differently or things I was doing wrong in their eyes." (N35) Participants might also quit if cameras were used in ways that indicated disrespect, distrust, or other negative dynamics (as described in §5.1), e.g. watching at inappropriate times or failing to disclose the cameras at all: "I might actually consider leaving [if I found a hidden camera], because [...] if they didn't trust me enough to, one, not have them; two, tell me they were putting them up, then there's the underlying issue there that needs to be addressed. And if they don't feel comfortable talking to me about it, then maybe we're not the right fit." (N33)

5.4.2 Power Constraining Choices About Taking or Keeping Jobs With Cameras

Concerns about the presence and use of cameras might be weighed against other factors—including socioeconomic factors that determined how selective a participant could be. As we noted earlier, participants might not feel they had the power to refuse or leave a job with cameras, given that jobs in camera-free houses were increasingly hard to find: "They're your boss. You can't really say no to them. And it's their house, not only are they your boss, their house, they're allowed to do what they want. So, saying no, whether or not my feelings [about cameras] are valid for whatever reason is... Yeah, there're probably gonna be consequences for that." (N33) On the flip side, a few participants said they might be more willing to put up with cameras—and even micromanaging via cameras—as a trade-off for a higher salary: "I felt like they really expected a lot of me. And that's why they had cameras, which made it okay for me because they were paying for high expectations. [...] If someone wasn't paying me well and they wanted to put me on camera, I think I would not." (N26)

5.4.3 Power Constraining Discussions and Condition-Setting About Data Flows

In discussing the downsides of nannying as a career, many participants noted that having no intermediary (or having only agencies) put them at a disadvantage in negotiating working conditions: "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, and that way it can be

really tricky for a lot of nannies." (N4) Against that background, participants had a range of views on what they could reasonably expect an employer to discuss about a camera.

Some participants did not feel that employers were—or even should be—obligated to disclose the existence of cameras at all. However, most believed they had a right to know. But even participants who thought employers *should* disclose did not necessarily assume they *would* disclose, if not forced to do so: "I would expect [employers to tell me if there were cameras], but I know they don't have to. They're not obligated to. I think they should [be obligated]." (N32)

The right to know might be framed in terms of *consent* (including implicit consent by accepting a job or continuing to work after camera disclosure): "I probably would not return to that family [to babysit]. [Because of] trust and respect. If they don't tell me that there are cameras recording, then I do not consent to being recorded." (N29) However, when we asked whether employers should seek *permission* from their employees, most participants said they did not view that as appropriate. While the words *consent* and *permission* can describe the same interaction, the two words profile a different power balance between the parties involved. While a couple of participants seemed to use the two words interchangably, others drew an explicit distinction:[11] "*[I: Do you think employers should ask nannies for their permission to install cameras inside the house?]* I don't know if I would probably use the word 'permission'. I think it is up to the parent. It's their home, it's their kids. But I do think asking for the nanny's consent is [...] necessary." (N6)

Opinions also differed as to whether it was reasonable to expect employers to discuss details such as purpose and planned use, or specifics about data flows and privacy settings. Some considered it reasonable to ask about these details, especially about the purpose of the camera: "I would still [...] advise [a first-time nanny] to ask about it and ask where they are, and [...] what their plan is with those. How often they're going to be checking those, and things like that." (N34) Some viewed it as inappropriate or risky to ask too many questions, even if there were things they would have liked to discuss: "I don't want to make it seem like I don't want to be videotaped, [...] like, 'Oh gosh, what have you seen?' But then, I would like to ask because I'm curious." (N26) Others viewed feasibility of asking for details as depending on the current relationship and how good communication was with that employer: "I feel, like, with the boy's family, I would be comfortable discussing it. And I'd be kind of afraid to discuss it with the girls' parents because [...] I feel they would get on the defensive." (N19)

Very few participants thought they were in a position to set conditions on camera use, such as requesting changes to privacy settings. Most viewed cameras as take-it-or-leave-it—even in the rare cases where they were offered a say in whether cameras were used: "My current nanny families, they both asked me if I'm okay with [cameras], and if not, they would take them down, but prefer to leave them up to monitor the kids in case anything happens. [...] *[I: If you had access to the privacy settings, would you change anything, or would you ask the parents to change anything in these settings?]* [...] No, I think that that is pretty much up to the parents and [...] I've already known about the cameras, so the privacy settings are really up to them." (N35) However, some believed they would have no problem requesting changes if they had an issue: "*[I: Have you ever asked parents about your preferences about the privacy settings of the cameras? [...]]* No, I have never felt like that boundary was crossed. If I did, I would feel very comfortable saying something." (N4)

[11] We were not deliberately varying the wording of our questions to compare participants' reactions; this was an accidental experiment.

6 Discussion

6.1 Summary of Findings

The major takeaways from our findings above are:

- Participants' views on camera data collection depended in large part on the purpose of data collection, how they thought the data would be used, and how those data uses might affect their relationships with their employers; they were most concerned about whether and how cameras would be used to supervise their work. (RQ1)
- Participants believed that the way employers used cameras reflected relationship qualities, such as trust, respect, and open communication. (RQ2)
- Participants' views on whether and how employers should use cameras—and how that use interacted with nannies' privacy rights—often made reference to prerogatives or social norms about who should control data flows, based on general social norms about who made decisions in a given context. (RQ1, RQ2)
- Even where participants believed they had a *right* to control data collection about them, most saw themselves as having a limited *ability* to make choices or express preferences about it, due to power dynamics in employer–employee relationships. (RQ1, RQ2)

In §6.3, we recap specific problems where interventions could have the most potential to mitigate the effects of power dynamics and promote clear, open communication about cameras (RQ3), and suggest corresponding interventions.

6.2 Comparison With Similar Studies

Johnson et al. [53] collected ethnographic data about Filipino migrant domestic workers in Hong Kong, including nannies, and their perceptions of home cameras used for surveillance.

The research showed that pervasive digital surveillance resulted in workers finding ways to evade control, not delivering the best care, and showing signs of negligence. These practices undermined trust between domestic workers and employers. In addition, the study found that control aligned with social hierarchies of gender, race, and class.

The participants in Johnson et al.'s study were in a more precarious position than most of ours reported being, in part because they were subject to rigid immigration rules that required them to live in their employers' house. (Only the two au pairs in our study lived with their employers; no other participants mentioned being dependent on employers for visas.) Also, our study was not limited to cameras used for surveillance. We therefore found a greater range of perspectives on cameras and how they helped or hindered employer–employee relationships, job performance, and job satisfaction. But at the same time, some of the same patterns were reflected in our participants' concerns about excessive surveillance, loss of trust, and control or micromanaging of work.

Albayaydh and Flechais [4] conducted qualitative interviews with domestic workers and employers of domestic workers, exploring privacy attitudes about smart home devices in the home workplace (not specific to cameras). The study was conducted in Jordan and focused on how religion and customs influenced perceptions of smart home devices. The study did not explore device purposes and uses in depth, but noted that some employees expected employers not to hide or use monitoring devices maliciously, due to norms based on Islamic religious beliefs that forbid breaching the privacy rights of others. However, in the end, many employers did not disclose smart devices, either purposely or because they assumed employees already knew—and similarly to our study, employees viewed nondisclosure as an indicator of distrust.

6.3 Points of Intervention and Recommended Mitigation Strategies

We found that power imbalances had adverse effects on nannies' privacy and individual agency with regard to camera data collection—mainly due to the fact that employers own the cameras, and, hence, employers have the power to choose who can access cameras and their settings. Efforts to create advanced controls (see §2) and education about device functions and configuration are insufficient. Social interventions such as those we suggest here are needed to guide parents and nannies in negotiating privacy matters and increase nannies' agency in the smart home context.

Privacy and Security Discussion Guides for Parents and Nannies Participants valued transparency about the existence and uses of cameras, to the point where they might quit if they found a hidden camera, or even hidden uses of a disclosed camera. They identified *communication at time of hire* as an especially effective point of intervention at which to mitigate concerns. Even with very obviously visible cameras, they said they would like an opportunity to ask questions. To help both parents and nannies navigate such conversations and make it easier to introduce potentially sensitive questions, we propose designing digital privacy and security discussion guides. Such guides might include advice about the mutual benefits of transparency around cameras; a list of possible discussion points to structure the conversation; and guidelines on how different smart home stakeholders can be involved in deciding on the configuration of a camera.

Further research is needed to expand on, verify, and quantify the considerations to prioritize for such a guide. However, our findings so far suggest these frequently-mentioned questions:

- Whether there are cameras present, how many there are, and where they are located.
- What type of data cameras collect (audio/video), whether it is recorded (as opposed to livestreamed), and, if so, how long recordings will be kept.
- How often cameras will be checked and how camera data will be used, especially whether they will be used to supervise nannies' work.
- Whether the nanny will be able to use the camera as a baby monitor, or otherwise have access to the data.
- Under what conditions the nanny is comfortable with the employer sharing video of her with third parties or on social media—*and* when nannies may share pictures or videos of children.

Encouraging such open conversations about cameras may function as a trust-building intervention to help address power imbalances.

Discussion guides should be co-designed with participation from domestic childcare workers and employers thereof [cf. 121, 122], and iteratively tested, refined, and validated. Guides should be jargon-free and accessible and translated into non-English languages commonly spoken in the U.S.

These discussion guides can supplement existing materials for nannies and other domestic workers about privacy issues and rights with respect to cameras and other smart home devices, provided by organizations like the National Domestic Workers Alliance in the U.S. or Voice of Domestic Workers in the UK [121]. Agencies are also well-positioned to mitigate power imbalances by encouraging discussions, and when asked, some participants thought *agencies could facilitate conversations about cameras*—or at least inform parents that the conversation should be had [cf. 4].

Promoting Domestic Worker Agency at Point of Configuration Few of our participants had discussed camera con-

figuration and privacy settings with employers, and none had been actively involved in choosing settings. When asked, many did not have strong opinions about what the settings should be, or thought it was not their place—but more did at least want to know what the current configurations were. Some participants opined that employers did not think to bring it up because it was not a normal *expectation to discuss device settings with non–household members*. Meanwhile, some employers could configure or use cameras in problematic ways unintentionally; in such cases, an alert might be effective in averting privacy infringement.

Prior work on bystander and secondary-user privacy has suggested nudging a device owner about a visitor's known preferences [144], or incorporating social interventions such as alerts and nudges into the interfaces of smart home devices [42, 91, 148] that would encourage the owner of the device to involve other occupants of the home in setup processes and alert them to potential violations of information-sharing norms. This idea could be expanded to encourage owners to consider the needs of non-occupants as well [25, 105, 128], including domestic workers, and could incorporate a discussion guide such as that suggested above.

Relatedly, some participants noted that nannies' *control over or access to camera data* was a point of intervention where employers could feasibly share power, reducing uncertainty about data handling and allowing nannies to use the same device to monitor children. Nudges could encourage configuring options to allow this.

Design Guidelines for Smart Home Camera Product Teams To bridge the gap between academic research findings and industry practice, we suggest creating design guidelines that explicitly foreground the needs of domestic workers, and provide practical recommendations for balancing conflicting needs and privacy concerns of employers and employees. Different stakeholders should take part in developing and refining the design guidelines [cf. 34]: primary users/device owners, domestic childcare workers, and camera product teams, e.g. in participatory design workshops [87, 120]. Guidelines could also incorporate findings from other user studies with diverse types of bystanders (see §2). In addition, guidelines could promote value-sensitive tech product design (VSD) [survey in 37] [for privacy: 10] (e.g. accounting for potential use of cameras in covert surveillance) and educate developers about relevant privacy regulations.

In many cases, there are existing solutions that could be adapted to the use case; however, guidelines should emphasize that enhanced features may need to accommodate nuance. For example, as we noted in §5.4.3, some participants found it overly distracting to know when a camera was being watched live. It should therefore be possible for the nanny to choose to turn this feature off—and yet the design ought not to make it easy for employers to hide that they are watching.

6.4 Future Research

Different smart home devices have different purposes of use and data practices (collection, use, storage, and sharing), leading nannies to think differently about them. Besides cameras, our interview script included questions asking participants about their views on smart speakers, smart TVs, and location trackers. In a forthcoming paper, we compare nannies' perspectives on these different devices.

In this paper, we focused on the employees' (nannies') perspectives. In future work, we will explore the other side of the equation: employers (parents), based on the interviews we conducted (see §3). In that work, we will compare the privacy threats perceived by nannies with those perceived by parents in smart homes, and examine how those threat models may influence the choices of each.

This paper explored the perspectives of nannies; future work should explore and compare the needs and concerns of other groups of bystanders with regard to cameras as well as other smart home devices, as specific needs and threats may differ, and different vulnerabilities may need to be addressed. Even amongst domestic workers, different job types may lead to differences in experiences and views, due to differences in social prestige, central management, and opportunities for building relationships and trust with employers. We are currently designing large-scale surveys to quantify our findings with domestic childcare workers and compare that situation with other bystander contexts in smart homes.

7 Conclusion

We conducted 25 semi-structured interviews with domestic childcare workers in the U.S. about smart home cameras, investigating how domestic employees navigate a multi-layered context that blends privacy and social norms for homes, workplaces, and caregiving. We examined how privacy considerations interact with the dynamics of employer–employee relationships in an in-home childcare context. Power differentials and norms about who should decide how information flows in a given situation affected participants' perspectives on camera data practices, as well as their ability to make choices and requests about camera data collection. Purposes and manner of use especially influenced participants' attitudes about cameras, because those factors both reflected and affected their relationships with their employers. (E.G., employers using cameras to micromanage and excessively monitor participants signaled disrespect and a lack of trust on the employers' part.) Drawing on the findings of this study, we suggest a set of technical and social interventions that balance power dynamics in smart homes with a focus on cameras, to improve domestic employees' privacy and support their individual agency.

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, and Wael Albayaydh. We also thank participants at the 2019 Symposium on the Applications of Contextual Integrity and the 2020 Workshop on Free and Open Communications on the Internet (FOCI), as well as anonymous reviewers for FOCI and SOUPS, for their helpful comments.

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 Security Agency (contract H98230-18-D-0006), and the U.S. National Science Foundation (award CNS-2114229).

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 451–466, Santa Clara, CA, USA, 2019.

[2] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. I-pic: A platform for privacy-compliant image capture. In *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 235–248, New York, NY, USA, 2016.

[3] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW):1–28, 2020.

[4] Wael Albayaydh and Ivan Flechais. Exploring bystanders' privacy concerns with smart homes in Jordan. In *ACM Conference on Human Factors in Computing Systems (CHI)*, New York, NY, USA, 2022.

[5] Mark Andrejevic. Big data, big questions: The big data divide. *International Journal of Communication*, 8(0), 2014.

[6] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. You, me, and IoT: How Internet-connected consumer devices affect interpersonal relationships. *arXiv:2001.10608 [cs]*, July 2020.

[7] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home Internet of Things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies (IMWUT)*, 2(2), June 2018.

[8] Noah Apthorpe, Sarah Varghese, and Nick Feamster. Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA. In *USENIX Security Symposium (USENIX Security)*, pages 123–140, Santa Clara, CA, USA, August 2019.

[9] Andrew Baerg. Big data, sport, and the digital divide: Theorizing how athletes might respond to big data monitoring. *Journal of Sport and Social Issues*, 41(1):3–20, 2017.

[10] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. Ethical design in the Internet of Things. *Science and Engineering Ethics*, 24(3):905–925, June 2018.

[11] Kirstie Ball. Workplace surveillance: An overview. *Labor History*, 51(1):87–106, 2010.

[12] Till Ballendat, Nicolai Marquardt, and Saul Greenberg. Proxemic interaction: Designing for a proximity and orientation-aware environment. In *ACM International Conference on Interactive Tabletops and Surfaces (ITS)*, pages 121–130, 2010.

[13] William Balmford, Larissa Hjorth, and Ingrid Richardson. Supervised play: Intimate surveillance and children's mobile media usage. *The Routledge Companion to Digital Media and Children*, page 185, 2020.

[14] Natã M. Barbosa, Zhuohao Zhang, and Yang Wang. 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)*, pages 417–435, August 2020.

[15] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. Privacy and contextual integrity: Framework and applications. In *IEEE Symposium on Security and Privacy (SP)*, pages 184–198, Washington, DC, USA, 2006.

[16] Sebastian Benthall and Bruce D. Haynes. Contexts are political: Field theory and privacy. Presentation at the Symposium on Applications of Contextual Integrity, Berkeley, CA, USA, August 19–20, 2019.

[17] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, August 2020.

[18] Clara Berridge, Jodi Halpern, and Karen Levy. Cameras on beds: The ethics of surveillance in nursing home rooms. *AJOB Empirical Bioethics*, 10(1):55–62, 2019.

[19] danah boyd and Kate Crawford. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication, & Society*, 15(5):662–679, 2012.

[20] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place*, 50:112–118, 2018.

[21] Anadi Chaman, Jiaming Wang, Jiachen Sun, Haitham Hassanieh, and Romit Roy Choudhury. Ghostbuster: Detecting the presence of hidden eavesdroppers. In *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 337–351, New Delhi, India, 2018.

[22] Menzie D. Chinn and Robert W. Fairlie. The determinants of the global digital divide: A cross-country analysis of computer and Internet penetration. *Oxford Economic Papers*, 59(1):16–44, 2007.

[23] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *ACM Conference on Ubiquitous Computing (UbiComp)*, pages 61–70, 2012.

[24] Ian Clark. The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2, March 2016.

[25] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2021(4):54–75, 2021.

[26] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. How risky are real users' IFTTT applets? In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 505–529, August 2020.

[27] Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, and Mahadev Satyanarayanan. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pages 1387–1396, July 2017.

[28] Mario De La Rosa, Rosa Babino, Adelaida Rosario, Natalia Valiente Martinez, and Lubna Aijaz. Challenges and strategies in recruiting, interviewing, and retaining recent Latino immigrants in substance abuse and HIV epidemiologic studies. *The American Journal on Addictions*, 21(1):11–22, 2012.

[29] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J Wisniewski. Exploring smart home device use by Airbnb hosts. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 1–8, New York, New York, United States, 2020.

[30] Leen d'Haenens and Christine Ogan. Internet-using children and digital inequality: A comparison between majority and minority Europeans. *Communications: The European Journal of Communication Research*, 38(1):41–60, 2013.

[31] David Eckhoff and Isabel Wagner. Privacy in the smart city: Applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, 20(1):489–516, Firstquarter 2018.

[32] Serge Egelman, Raghudeep Kannavara, and Richard Chow. Is this thing on? Crowdsourcing privacy indicators for ubiquitous sensing platforms. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1669–1678, New York, NY, USA, 2015.

[33] Ame Elliott and Sara Brody. Straight talk: New yorkers on mobile messaging and implications for privacy. Technical report, 2015. Accessed: 10 December, 2018.

[34] P. Emami-Naeini, Y. Agarwal, L. Cranor, and H. Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *IEEE Symposium on Security and Privacy (SP)*, pages 771–788, Los Alamitos, CA, USA, may 2020.

[35] Angella Foster. When parents eavesdrop on nannies. *New York Times*, August 2019. Accessed: 8 June, 2020.

[36] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A stalker's paradise": How intimate partner abusers exploit technology. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–13, New York, NY, USA, 2018.

[37] Batya Friedman, David G Hendry, and Alan Borning. A survey of value sensitive design methods. *Foundations and Trends in Human–Computer Interaction*, 11(2):63–125, 2017.

[38] Alisa Frik, Julia Bernd, and Serge Egelman. A model of contextual factors affecting older adults' information-sharing decisions in the US. *ACM Trans-*

actions on Computer-Human Interaction, 2022. To appear.

[39] Jon P. Gant, Nicole E. Turner-Lee, Ying Li, and Joseph S. Miller. Minority broadband adoption: Comparative trends in adoption, acceptance and use. Technical report, Joint Center for Political and Economic Studies, Washington, DC, USA, February 2010.

[40] Radhika Garg and Hua Cui. Social contexts, agency, and conflicts: Exploring critical aspects of design for future smart home technologies. *ACM Transactions on Computer-Human Interaction*, 29(2):11:1–11:30, January 2022.

[41] George Gaskell and Martin W. Bauer. Towards public accountability: Beyond sampling, reliability and validity. In *Qualitative Researching with Text, Image and Sound*, pages 337–350. SAGE Publications Ltd., London, UK, 2000.

[42] Christine Geeng and Franziska Roesner. Who's in control? Interactions in multi-user smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–13, New York, NY, USA, 2019.

[43] Emily Starbuck Gerson. Nanny cams: What parents need to know before installing a home security camera, January 2019. Blog post; accessed: 8 June, 2020.

[44] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 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, pages 656–674, Cham, 2017. Springer.

[45] Jessica Groopman and Susan Etlinger. Consumer perceptions of privacy in the Internet of Things: What brands can learn from a concerned citizenry. Technical report, June 2015. Accessed: 17 February, 2018.

[46] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile?: Technology, risk and privacy among undocumented immigrants. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–15, New York, NY, USA, 2018.

[47] Loni Hagen. Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy. In *ACM International Conference on Digital Government Research*, dg.o '17, pages 598–599, New York, NY, USA, 2017.

[48] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *International Conference on Human-Computer Interaction*, pages 393–411. Springer International Publishing, 2020.

[49] Eszter Hargittai and Eden Litt. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy*, 11(3):38–45, May 2013.

[50] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home Internet of Things (IoT). In *USENIX Security Symposium (USENIX Security)*, pages 255–272, Baltimore, MD, USA, August 2018.

[51] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 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)*, page 1–13, New York, NY, USA, 2020.

[52] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. Exploring the needs of users for supporting privacy-protective behaviors in smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–19, New York, NY, USA, April 2022.

[53] Mark Johnson, Maggy Lee, Michael McCahill, and Ma Rosalyn Mesina. Beyond the 'all seeing eye': Filipino migrant domestic workers' contestation of care and control in Hong Kong. *Ethnos*, 85(2):276–292, 2020.

[54] Saba Kazi, Omead Kohanteb, Thidanun Saensuksopa, Owen Tong, and Heidi Yang. Decoding sensors: Creating guidelines for designing connected devices. Technical report, Carnegie Mellon University, Summer 2015. Accessed: 7 March, 2018.

[55] Jennifer King. *Privacy, Disclosure, and Social Exchange Theory*. PhD thesis, University of California, Berkeley, CA, 2018.

[56] Jennifer King and Andreas Katsanevas. Blending contextual integrity and social exchange theory: Assessing norm building under conditions of "informational inequality". Presentation at the 2nd Symposium on Applications of Contextual Integrity, Berkeley, CA, USA, August 19–20, 2019.

[57] Thorin Klosowski. Your visitors deserve to know they're on camera. *New York Times*, October 2019. Accessed: 8 June, 2020.

[58] Marion Koelle, Katrin Wolf, and Susanne Boll. Beyond LED status lights: Design requirements of privacy no-

tices for body-worn cameras. In *ACM International Conference on Tangible, Embedded, and Embodied Interaction (TEI)*, pages 177–187, New York, NY, USA, 2018.

[59] Omead Kohanteb, Owen Tong, Heidi Yang, Thidanun Saensuksopa, and Saba Kazi. signifiers.io guidelines for designing connected devices, 2015. Accessed: 26 February, 2018.

[60] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. "We just use what they give us": Understanding passenger user perspectives in smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, New York, NY, USA, 2021.

[61] Martin Kraemer and Ivan Flechais. Disentangling privacy in smart homes, 2018. Presentation at the 1st Symposium on Applications of Contextual Integrity, Princeton, NJ, USA, September 13–14, 2018. Accessed: 20 November, 2018.

[62] Martin J. Kraemer, Ivan Flechais, and Helena Webb. Exploring communal technology use in the home. In *ACM Halfway to the Future Symposium (HTTF)*, New York, NY, USA, 2019.

[63] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. Further exploring communal technology use in smart homes: Social expectations. In *ACM Conference on Human Factors in Computing Systems (CHI): Extended Abstracts*, pages 1–7, New York, New York, United States, 2020.

[64] Martin J. Kraemer, William Seymour, and Ivan Flechais. Responsibility and privacy: Caring for a dependent in a digital age. In *CHI Workshop on Privacy and Power (Networked Privacy)*, 2020.

[65] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–31, 2018.

[66] Tama Leaver. Intimate surveillance: Normalizing parental monitoring and mediation of infants online. *Social Media+ Society*, 3(2):2056305117707192, 2017.

[67] Hosub Lee and Alfred Kobsa. Understanding user privacy in Internet of Things environments. In *IEEE World Forum on Internet of Things (WF-IoT)*, pages 407–412, December 2016.

[68] Linda Lee, Joong Hwa Lee, Serge Egelman, and David Wagner. Information disclosure concerns in the age of wearable computing. In *NDSS Workshop on Usable Security (USEC)*. Internet Society, 2016.

[69] Samantha Lee and Brian H Kleiner. Electronic surveillance in the workplace. *Management Research News*, 26:72–81, 2003.

[70] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *ACM Conference on Designing Interactive Systems (DIS)*, page 527–539, New York, NY, USA, 2019.

[71] Karen Levy, Lauren Kilgour, and Clara Berridge. Regulating privacy in public/private space: The case of nursing home monitoring laws. *The Elder Law Journal*, February 2019.

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

[73] Eden Litt and Eszter Hargittai. Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. *Poetics*, 42:1–21, 2014.

[74] Tian Liu, Ziyu Liu, Jun Huang, Rui Tan, and Zhen Tan. Detecting wireless spy cameras via stimulating and probing. In *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 243–255, 2018.

[75] Steve Lohr. Unblinking eyes track employees. *New York Times*, June 2014. Accessed: 23 July, 2018.

[76] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 'Internet of Things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, 63:22–26, 2019. Available at SSRN: https://ssrn.com/abstract=3350615.

[77] Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. Privacy, technology, and aging: A proposed framework. *Ageing International*, 36(2):232–252, June 2011.

[78] Deborah Lupton. Self-tracking cultures: Towards a sociology of personal informatics. In *ACM Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design (OzCHI)*, pages 77–86, New York, NY, USA, 2014.

[79] Mary Madden, Michele E. Gilman, Karen Levy, and Alice E. Marwick. Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review*, 95(1):53–125, 2017.

[80] Mary Madden and Lee Rainie. Americans' attitudes about privacy, security, and surveillance. Technical report, Pew Research Center, May 2015. Accessed: 9 February, 2018.

[81] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What *can't* data be used for?" Privacy expectations about smart TVs in the U.S. In *European Workshop on Usable Security (EuroUSEC), London, UK*, 2018.

[82] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2019(4):250–271, 2019.

[83] Lev Manovich. Trending: The promises and the challenges of big social data. In *Debates in the Digital Humanities*, pages 460–475. The University of Minnesota Press, Minneapolis, MN, 2011.

[84] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020(2):436 – 458, 2020.

[85] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "You just can't know about everything": Privacy perceptions of smart home visitors. In *International Conference on Mobile and Ubiquitous Multimedia (MUM)*, pages 83–95, 2020.

[86] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. "I don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *ACM Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI)*, New York, NY, USA, 2020.

[87] Michael Massimi and Ronald Baecker. Participatory design process with older users. In *UbiComp Workshop on Future Media*, 2006.

[88] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. Access control for home data sharing: Attitudes, needs, and practices. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 645–654, New York, NY, USA, 2010.

[89] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 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):1–23, 2019.

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

[91] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW), April 2021.

[92] Simon Moncrieff, Svetha Venkatesh, and Geoff West. Dynamic privacy in a smart house environment. In *IEEE International Conference on Multimedia and Expo*, pages 2034–2037, 2007.

[93] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. Understanding the privacy design space for personal connected objects. In *International BCS Human Computer Interaction Conference: Fusion! (HCI)*, pages 18:1–18:13, Swindon, UK, 2016. BCS Learning & Development Ltd.

[94] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an IoT world. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 399–412, Santa Clara, CA, 2017.

[95] Carman Neustaedter and Saul Greenberg. The design of a context-aware home media space for balancing privacy and awareness. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 297–314. Springer, 2003.

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

[97] Helen Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

[98] Helen Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, Fall 2011.

[99] Parmy Olson. Wearable tech is plugging into health insurance. *Forbes*, June 2014. Accessed: 23 July, 2018.

[100] Yong Jin Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, 2013.

[101] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In *New Security Paradigms Workshop (NSPW)*, pages 1–15, 2019.

[102] Shwetak N Patel, Jay W Summet, and Khai N Truong. Blindspot: Creating capture-resistant spaces. In *Protecting Privacy in Video Surveillance*, pages 185–201. Springer, 2009.

[103] Scott R. Peppet. Regulating the Internet of Things: First steps toward managing discrimination, privacy, security & consent. *Texas Law Review*, 93:85–178, 2014.

[104] Alfredo J Perez, Sherali Zeadally, and Scott Griffith. Bystanders' privacy. *IT Professional*, 19(3):61–65, 2017.

[105] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurle, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. Addressing adjacent actor privacy: Designing for bystanders, co-users, and surveilled subjects of smart home cameras. In *ACM Conference on Designing Interactive Systems (DIS)*, 2022. To appear.

[106] James Pierce, Richmond Y. Wong, and Nick Merrill. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–19, New York, NY, USA, 2020.

[107] Lucinda Platt, Renee Luthra, and Tom Frere-Smith. Adapting chain referral methods to sample new migrants: Possibilities and limitations. *Demographic Research*, 33:665–700, 2015.

[108] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. Somebody's watching me?: Assessing the effectiveness of webcam indicator lights. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1649–1658, New York, NY, USA, 2015.

[109] Alison Powell, Amelia Bryne, and Dharma Dailey. The essential Internet: Digital exclusion in low-income American communities. *Policy & Internet*, 2(2):161–192, 2010.

[110] Nicholas Proferes. The development of privacy norms. In *Modern Socio-Technical Perspectives on Privacy*, pages 79–90. Springer, Cham, 2022.

[111] Lee Rainie and Janna Anderson. The future of privacy. Technical report, Pew Research Center, December 2014. Accessed: 17 July, 2018.

[112] Lee Rainie and Maeve Duggan. Privacy and information sharing. Technical report, Pew Research Center, January 2016. Accessed: 16 February, 2022.

[113] Olivia Richards and Gabriela Marcu. Children's agency in the age of smart things. In *CHI Workshop on Privacy and Power (Networked Privacy)*, 2020.

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

[115] Laura Robinson and Brian K. Gran. No kid is an island: Privacy scarcities and digital inequalities. *American Behavioral Scientist*, 2018.

[116] Ignacio Rodríguez-Rodríguez, José-Víctor Rodríguez, Aránzazu Elizondo-Moreno, Purificación Heras-González, and Michele Gentili. Towards a holistic ICT platform for protecting intimate partner violence survivors based on the IoT paradigm. *Symmetry*, 12(1):37, 2020.

[117] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. Augmented reality: Hard problems of law and policy. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp): Adjunct Publication*, pages 1283–1288, New York, NY, USA, 2014.

[118] Safe Smart Living. 16 smart home statistics and predictions, October 2019. Web page; accessed: 16 July, 2020.

[119] Jeremy Schiff, Marci Meingast, Deirdre K Mulligan, Shankar Sastry, and Ken Goldberg. Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In *Protecting Privacy in Video Surveillance*, pages 65–89. Springer, 2009.

[120] Douglas Schuler and Aki Namioka. *Participatory design: Principles and practices*. CRC Press, 1993.

[121] Julia Słupska, Marissa Begonia, Nayana Prakash, Selina Cho, Ruba Abu-Salma, Mallika Balakrishnan, and Natalie Sedacca. Digital privacy & security guide for migrant domestic workers. Technical report, University of Oxford, King's College London, Voice of Domestic Workers, and Migrants Organise, September 2021. Web page; accessed: 14 February, 2022.

[122] Julia Słupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *USENIX Security Symposium (USENIX Security)*, Boston, MA, USA, August 2022. To appear.

[123] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. I'm all eyes and ears: Exploring effective locators for privacy awareness in IoT scenarios. In *ACM*

Conference on Human Factors in Computing Systems (CHI), pages 1–13, New York, NY, USA, 2020.

[124] Luke Stark and Karen Levy. The surveillant consumer. *Media, Culture, and Society*, 40(8):1202–20, November 2018.

[125] Statista. Smart home penetration rate forecast worldwide from 2017 to 2024, June 2020. Web page; accessed: 16 July, 2020.

[126] Kaiwen Sun, Yixin Zhou, Jenny Radesky, Christopher Brooks, and Florian Schaub. Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW), 2021.

[127] Janos Mark Szakolczai. "What have you caught?": Nannycams and hidden cameras as normalised surveillance of the intimate. In *The Technologisation of the Social*. Routledge, 2021.

[128] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 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)*, New York, NY, USA, 2022.

[129] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "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)*, pages 1–13, New York, NY, USA, April 2022.

[130] Peter Tolmie, Andy Crabtree, Tom Rodden, James Colley, and Ewa Luger. "This has to be the cats": Personal data legibility in networked sensing systems. *Proceedings of the ACM on Human-Computer Interaction*, (CSCW):491–502, 2016.

[131] Khai N Truong, Shwetak N Patel, Jay W Summet, and Gregory D Abowd. Preventing camera recording by designing a capture-resistant environment. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 73–86. Springer, 2005.

[132] Joseph Turow, Lauren Feldman, and Kimberly Meltzer. Open to exploitation: America's shoppers online and offline. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2005. Accessed: 3 June, 2015.

[133] Joseph Turow, Michael Hennessy, and Nora Draper. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Technical report, Annenberg Public Policy Center of the University of Pennsylvania, June 2015. Accessed: 24 February, 2018.

[134] Joseph Turow, Michael Hennessy, Nora Draper, Ope Akanbi, and Diami Virgilio. Divided we feel: Partisan politics drive Americans' emotions regarding surveillance of low-income population. Technical report, Annenberg School for Communication at the University of Pennsylvania, 2018. Accessed: 24 December, 2018.

[135] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, page 129–139, New York, NY, USA, 2014.

[136] Alexander J.A.M. van Deursen and Jan A.G.M. van Dijk. Internet skills and the digital divide. *New Media & Society*, 13(6):893–911, 2010.

[137] Myria Watkins Allen, Stephanie J Coopman, Joy L Hart, and Kasey L Walker. Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, 21(2):172–200, 2007.

[138] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. "Privacy is the boring bit": User perceptions and behaviour in the Internet-of-Things. In *IEEE International Conference on Privacy, Security, and Trust (PST)*, August 2017.

[139] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Smart homes and their users: A systematic analysis and key challenges. *Personal and Ubiquitous Computing*, 19(2):463–476, February 2015.

[140] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. Benefits and risks of smart home technologies. *Energy Policy*, 103:72–83, April 2017.

[141] Jenifer Sunrise Winter. Citizen perspectives on the customization/privacy paradox related to smart meter implementation. *International Journal of Technoethics*, 6(1), 2015.

[142] Julia Wolfe, Jori Kandra, Lora Engdahl, and Heidi Shierholz. 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, May 2020. Accessed: 21 July, 2020.

[143] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of

privacy mechanisms for smart homes. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–12, New York, NY, USA, May 2019.

[144] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, November 2019.

[145] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Free to fly in public spaces: Drone controllers' privacy perceptions and practices. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 6789–6793, New York, NY, USA, 2017.

[146] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *ACM Conference on Human Factors in Computing Systems (CHI)*, pages 6777–6788, New York, NY, USA, 2017.

[147] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 65–80, Santa Clara, CA, 2017.

[148] Eric Zeng and Franziska Roesner. 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)*, pages 159–176, Santa Clara, CA, August 2019.

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

[150] Nicole Zillien and Eszter Hargittai. Digital distinction: Status-specific types of Internet usage. *Social Science Quarterly*, 90(2):274–291, 2009.