Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance

Julia Bernd
International Computer Science Institute
University of California, Berkeley

Ruba Abu-Salma
Centre INRIA Sophia Antipolis-Méditerranée

Alisa Frik
International Computer Science Institute
University of California, Berkeley

Abstract

The increasing use of smart home devices affects the privacy not only of device owners, but also of individuals who did not choose to deploy them, and may not even be aware of them. Some smart home devices and systems, especially those with cameras, can be used for remote surveillance of, for example, domestic employees. Domestic workers represent a special case of bystanders' privacy, due to the blending of home, work, and care contexts, and employer–employee power differentials. To examine the experiences, perspectives, and privacy concerns of domestic workers, we begin with a case study of nannies and of parents who employ nannies. We conducted 26 interviews with nannies and 16 with parents. This paper describes the research agenda, motivation, and methodology for our study, along with preliminary findings.

1 Introduction

IoT devices are designed to collect data from their whole environment. That environment may include the individuals who chose to deploy the devices, but may also include bystanders—or surveillance targets—who did not have a choice about them being deployed, do not have any control over what they collect and share, and may not even be aware of them. Further, such devices are embedded in a social and economic context that may constrain who is more or less likely to be able to make choices about whether data is being collected about them.

To develop a more comprehensive understanding of IoT privacy, we are conducting case studies with groups who are especially likely to interact with IoT devices—particularly smart home devices—that they do not control. In some cases, such groups might really be unintended bystanders to data collection, and, in some cases, they might be explicit targets.

As smart-home technologies become more ubiquitous [52, 54], using cameras or other devices to keep tabs on domestic workers has moved from being a niche practice to being quite common, and even to some degree—or in some places—expected [16, 19, 28]. This integration of surveillance practices carries a complex set of privacy ramifications for domestic employees or service workers. Furthermore, it may affect the nature of the individual relationships between those employees/service workers and their employers/clients, as well as reflecting or amplifying general socio-economic dynamics.

Our first case study focuses on nannies, au pairs, and full-time babysitters. Our decision to begin with this group has several motivations. First, by analysing employer–employee relationships, we hope to shed light on the interplay between socio-economic power differentials and privacy outcomes—and how we can reduce the effects of those differentials. Second, most research on privacy concerns, attitudes, and expectations focuses either on primary end users of a specific technology, or else on general public surveillance or tracking, where data subjects have no connection to the privacy decision-makers. Domestic workers present an in-between case, in that there is direct interaction and some degree of personal accountability between the primary users who deployed the device and the bystanders.

Finally, surveillance of nannies takes place within a blended multi-dimensional context. The devices are installed in a home, but, for a nanny, that home is also a workplace. In addition, it is a childcare situation, which may seem to require a different balance between safety and worker privacy than in other workplaces.

We explored nannies' experiences with and perspectives on smart home devices by conducting qualitative interviews with 26 nannies, au pairs, and professional babysitters in the U.S., as well as conducting 16 interviews with parents who employ nannies or au pairs. Parallel studies are also taking place in the UK and Germany; these will be discussed in later work.

2 Related Work

IoT technologies can have differential impacts on privacy across populations, due to differences in knowledge [e.g., 4, 23, 47] or because social and political power imbalances mean data collection reinforces existing discrimination [e.g.,

14, 25, 38, 47]. In particular, such imbalances can play out in workplace data collection [e.g., 3, 35, 37, 46]—including in care situations such as nursing homes [e.g., 6, 34].

Specific to smart homes, control of devices may reflect socio-cultural dynamics in family/household life [18, 29, 30] or, in the worst case, may be an element in domestic abuse [e.g., 7, 33].

Preferences and concerns about smart home data collection vary according to contextual factors [e.g., 1, 17, 20, 31, 32, 39, 40, 42]. Most studies that compared locales found more sensitivity about data collected in homes than workplaces or business establishments [e.g., 12, 31, 42] [*contra* 21]. This observation raises interesting questions about what happens when one person's workplace is another person's home.

The Theory of Contextual Integrity (CI) [43, 44, 45] argues that norms about privacy and appropriate information sharing heavily depend on the *context*, or social domains, in which the information is shared, and that privacy violations may occur when information is reshared in a context different from the original sharing. Existing work on smart homes within the CI framework investigates how people's reasoning about privacy draws on norms for the home vs. the Internet, finding that the blending of contexts can give rise to new considerations with regard to transparency and control [e.g., 1, 8, 36, 58]. CI also provides a lens for examining how competing norms are resolved in situations involving power imbalances [e.g., 5, 26, 27, 29, 30].

Bystanders in smart homes, such as visitors or even co-habitants who did not make the choice to install the devices, are beginning to receive more research attention [e.g., 60]; [also mentioned in, e.g., 11, 40, 48, 51, 61]. Bystander issues may interact with family/household dynamics in smart homes, as mentioned above. In particular, children may be bystanders to or targets of smart-home devices installed by their parents [e.g., 50, 55], or of smart toys [2]. Studies have also explored the reactions of visitors to shared housing, such as AirBnB rentals [e.g., 41, 53].

A recent survey by the Matahari Center explored Boston nannies' experiences with and knowledge about nanny cams [16]. In contrast, our study focuses on collecting rich qualitative data, revealing the nuances of expectations and preferences about a variety of smart devices, including smart speakers, smart TVs, and domestic security systems as well as cameras. In addition, we are exploring the opinions of both nannies and parents, to obtain a holistic view based on the perspectives of the two main stakeholders.

To our knowledge, ours is the first in-depth study exploring how smart home surveillance of in-home care workers is contextualized and negotiated within the employer-employee relationship.

3 Research Questions

Our overarching research goal is to explore and contextualize privacy norms, expectations, and preferences of smart-home bystanders, with reference to the CI framework [43, 44, 45], and to understand how those norms relate to the power imbalances between the primary users and bystanders.

Our first case study of smart-home bystanders is a two-side study, of nannies, professional babysitters, and au pairs, and of parents who employ nannies or au pairs. Our research questions include:

1. What are nannies' experiences with—and their privacy attitudes, expectations, and concerns about—being observed and recorded by smart home devices that they did not choose to deploy?
2. What are the employers' (parents') attitudes about nannies' privacy with respect to smart home devices?
3. How do employers' and nannies' attitudes toward, and choices about, smart home data collection reflect, reinforce, or change existing power dynamics in their relationships?
4. If there are privacy-related conflicts between nannies and parents, how are those conflicts negotiated?
5. What are the potential points of intervention for representing nannies' preferences with respect to data being collected and shared about them by their employers' devices?

To examine whether our findings are particular to the U.S. or are more generalizable, we are also conducting studies in two European countries, the UK and Germany (the latter in collaboration with colleagues at Leibniz University Hannover). In a later stage of this work, we will compare the three samples to analyze whether, e.g., differences in sociocultural norms or legal climate affect the participants' perspectives.

4 Methodology

For the U.S. portion of the study, with approval from the UC Berkeley Institutional Review Board (IRB), we designed and conducted semi-structured interviews with 26 nannies, professional babysitters, and au pairs, along with 16 parents who employ nannies or au pairs, between October and December 2019.

Recruitment. We recruited participants by posting or distributing flyers locally (e.g., in cafes, colleges, preschools, schools, playgrounds), posting online (e.g., Reddit, Facebook groups, email lists), advertising on Prolific,[1] and snowballing/referrals (see Table 1).

[1] We used Prolific for the parents' side only, as we had not gotten enough potential participants using other methods.

	Nannies		Parents	
Venue	N	%	N	%
Social media	18	69%	2	13%
Flyering	6	23%	0	0%
Word of mouth/referral	2	8%	0	0%
Prolific	–	–	13	81%
Email lists	0	0%	1	6%

Table 1: Participants recruited using each method. All methods were tried with both target groups, except Prolific.

We included both nannies/au pairs who had experience working with cameras and/or smart home devices and those who did not. The parents' study was smaller, serving as a cross-check for findings from the nannies' side. We therefore only included parents who had cameras they could check remotely (though not all parent participants used them that way). When screening potential participants to make sure they met the criteria for the study, we made sure we did not include anyone whose employer or nanny also expressed interest (to ensure participants did not feel constrained in their interview answers due to confidentiality concerns)—though we did not, in the end, receive inquiries from any such pairs.[2]

All nannies who contacted us and met the criteria were invited to participate. As we received inquiries from more parents than our target number, we selected participants from the parent pool by random drawing.

Interviews. We designed the interview guides based on a review of academic literature on smart home user perspectives (see §2), as well as by reading content for and from nannies and other domestic workers, especially online forums (such as Reddit's Nanny forum), and content for and from parents who employ nannies. The UK and Germany portions of the study used the same interview instruments (modulo translation into German) and similar procedures. The UK interviews began first and included a pilot of the instruments; we therefore did not run a separate pilot for the U.S. study.

The U.S. interviews with nannies generally took one to one and half hours (though ranging from three quarters of an hour to two hours and a quarter); most were conducted by phone or video chat, except two in person. Nanny participants were compensated $50. After briefly explaining the study and obtaining informed consent, we began with warm-up questions to get some context about how participants view nannying as a career and their relationships with their employers.

We then asked participants about their experiences with smart home devices in their employers' homes, and interactions they had had about those devices. If nannies had not worked with such devices, or had not experienced a particular situation, we asked what they would do in hypothetical scenarios. We also asked about their general expectations, preferences, and concerns with regard to smart home device use and disclosure—including under what conditions nannies who had never worked with such devices would agree to do so—and what they knew about current legal and technical protections. The bulk of most interviews was devoted to cameras or similar devices marketed as explicitly for surveillance, though we also asked a similar series of questions about other smart home devices, such as smart speakers and smart TVs.

We asked a more condensed set of questions in the interviews with parents who employ nannies, focusing on interactions with nannies about devices and their reasoning about device use and disclosure. Phone or video-call interviews lasted half to three quarters of an hour; parent participants were compensated $25.

After the interviews, both nannies and parents completed exit questionnaires covering demographic information, experience with technology, details of their job situation (nannies) or childcare situation (parents), what smart devices they own, and (for nannies) what smart devices their employers own (see §5 and Appendix A).

Analysis. As of the time of writing, we are conducting inductive thematic analysis of 25 of the nanny interview transcripts (one was dropped due to language difficulties). Three coders (the authors) independently coded the same three test interviews to develop codebooks of common topics and initial themes. We discussed our codebooks and merged them by consensus. We then piloted the agreed coding frame on additional test interviews to make final adjustments. Using the finalized coding frame, we are splitting the remaining interviews, with each interview being coded by two coders (in addition to recoding the test interviews).

Once all interviews are coded, we will review the excerpts on each topic to refine our analysis of the themes and the relationships between them. We will then conduct a similar process with the transcripts of the 16 parent interviews, so we can compare the analyses and identify any important connections—or disconnects. In a later stage of the research, we will compare the findings from the U.S., UK, and Germany studies, as well as conduct surveys (see §7).

Limitations. The interviews were conducted in English (and our recruiting materials were all in English). While our sample included non-native English speakers (see Appendix A), all participants were at least reasonably comfortable speaking English (other than the excluded nanny interview mentioned above). Therefore, our analysis may be unable to capture issues that are unique to—or at least more severe for—nannies with limited fluency in English; such issues might potentially include misunderstandings and effects on power dynamics.

[2] Screening scripts, interview protocols, and exit questionnaires can be found at https://www1.icsi.berkeley.edu/~jbernd/Nannies_Study_Instruments.pdf.

In particular, interviewing in English may mean that our sample is not representative of the proportion of immigrants in the nanny workforce; around 28% of nannies in the U.S. are immigrants [59].[3] In addition to the desirability of a representative sample, the experiences of immigrants may be of particular interest due both to the exacerbation of employer-employee power imbalances and to higher risks arising from any form of surveillance, especially for undocumented immigrants [cf. 22]. In addition to language barriers, undocumented immigrants specifically may be less likely to participate in research studies due to enhanced privacy concerns [e.g., 13, 49].

For the surveys we plan to conduct in the future (see §7), we will use several languages, and adopt focused strategies to recruit immigrant participants.

In addition, it is possible that some of our recruitment strategies favored more tech-savvy participants, or (for nannies) participants whose employers were more likely to have smart home devices. While some of our online strategies drew from all over the U.S. (Reddit, Prolific), the city-specific email and Facebook groups we were approved to post in happened to be for major tech industry centers—and in-person flyering was conducted only in the high-tech Bay Area.

Finally, we chose to include only parents who have in-home surveillance devices in our limited sample, as the parents study is intended mainly as a cross-check to findings from the nanny study. However, it is possible there are insights we might miss from excluding parents who do not have such devices.

5 Participants

Table 2 describes the job situations and some demographic characteristics of the 25 nannies whose interviews are included in the analysis. Most nannies did not live in their employers' houses, except for the au pairs. Full details about demographics, job situations, technology background, and experience with smart home devices can be found in Appendix A, along with comparisons to demographic statistics and job situations for nannies from government and industry data. As indicated in Appendix A, our sample is representative of the demographics of nannies and childcare workers in the U.S.

6 Preliminary Findings

In this section, we provide an overview of our high-level findings. Note that these findings are preliminary and are not meant to indicate the prevalence, consistency, or reliability of the observed themes.

[3] We say 'may mean' because we did not ask about immigration status on the exit questionnaires. For our sample size, the likely scientific benefit—especially dubious given that undocumented immigrants in particular might be more likely to skip such a question or answer untruthfully—did not outweigh the potential distress to any undocumented participants in deciding how or whether to answer the question.

Characteristics	N	%
Age (Range 19–55; Median 30)		
≤ 22	3	12%
23–39	17	68%
40–59	5	20%
Gender (participants' self-descriptors)		
Female, Cis-female, F	25	100%
Ethnicity (participants' self-descriptors)		
White, Caucasian	18	72%
Hispanic, Latina, Latinx, Mexican	5	20%
Asian, Indian-from-India	2	8%
No answer	*1*	*4%*
Current Position		
Nanny	15	60%
Nanny/Household manager	4	16%
Professional babysitter	3	12%
Au pair	2	8%
Other	1	4%

Table 2: Individual characteristics of nanny participants.

The interviews focused mainly on smart home devices that are designed primarily for surveillance (e.g., home security systems, security cameras, Internet-enabled baby monitors, "nanny cams"). Among nanny participants who had experience with such devices, some believed themselves to have been the primary targets of data collection, while others described being bystanders to cameras deployed for other reasons. Similarly, some of the parent participants we interviewed had gotten cameras specifically to observe their nannies, while others had them for other reasons. We also investigated the dynamics around other smart home devices that use sensors (e.g., for voice commands or presence detection), such as smart speakers, smart toys, or smart TVs. With respect to those devices, nannies were generally bystanders to, rather than targets of, data collection by their employers.

The remainder of this section pertains specifically to findings from our interviews with nannies, au pairs, and professional babysitters, not the interviews with parents who employ nannies (which we have not yet begun to analyze).

Expectations and Attitudes About Cameras. Our analysis so far has shown that most of our nanny participants view the use of cameras in homes where nannies work to be relatively common and—to a certain degree—expected (at least in the U.S.); most have worked with them. Participants generally view it as desirable (or even ethically imperative) for employers to inform nannies about cameras; lack of disclosure may be viewed as a breach of trust, and potentially as signalling a lack of respect. However, there is more variation with regard to whether they view it as likely that employers

will actually do so. In addition, participants have a diversity of expectations about how data might be used, either by their employers or by device service providers—though many noted they had not thought much about the latter.

The nannies we interviewed have a broad range of positive and negative attitudes toward the use of cameras, in general and within the workplace. However, few expressed views that were entirely positive or entirely negative. Participants' attitudes toward and acceptance of cameras are based on many factors and conditions, which might play off against each other in a given situation; our interview script was designed in part to draw out the specifics of such conditions and trade-offs.

For instance, some participants are more concerned about devices capturing information pertinent to their private lives or behaviors (e.g., changing clothes, having a private phone conversation, or activities during leisure time even if those activities were not privacy-sensitive) than to their professional childcare activities. Some mentioned that their attitudes have changed, and over time they have gotten used to smart home devices and the idea of potential surveillance by their employers (or by device service providers). However, a few participants mentioned that awareness of domestic surveillance devices also changes the way they do their job (e.g., making them more self-conscious about and less likely to engage in singing, joking, or making funny faces to entertain kids).

Some participants also acknowledged the benefits of cameras in providing protection against wrongful accusations or protecting physical safety (including nannies' own safety), and other advantages associated with the primary purpose of smart home devices (e.g., convenience, entertainment, facilitating communication or childcare duties).

The Importance of Purposes and Intentions. A central consideration is often the purpose(s) of camera deployment and data collection, and how employers use the device and data. At a high level, participants' views may depend on whether they believe the primary purpose is to monitor the nanny or whether the camera is primarily for other purposes, such as home security or feeling connected with the children.

However, there are many nuances. A nanny who is generally okay with cameras that are there to check on her might have a different opinion depending on how exactly that information is used (e.g., spot-checks against neglect vs. frequent critiquing and micromanaging care). Some participants also expressed concern about whether cameras that were ostensibly installed for home security might actually also be used to monitor or spy on them; many emphasized the importance of being transparent about the purpose of a camera.

Participants' views on cameras also interact with the dynamics of their relationships with their employers. In particular, nannies often framed their concerns about the purposes and uses of cameras in terms of what those purposes/uses mean about the relationship. For example, constant checking of cameras and "micromanagement" based on what employers observe may be seen as a sign of mistrust or disrespect, and may therefore engender more resentment.

However, the interaction of attitudes toward cameras with relationship dynamics can also go the other way, with nannies making assumptions about camera use based on their overall impression of their relationship with their employers: being more willing to assume good intentions behind monitoring in a relationship that is otherwise good, and vice versa.

Not Being in a Position to Express Preferences. While nannies often expressed privacy concerns and feelings of discomfort about surveillance, due to power dynamics, many said they defer to parents' decisions about installing smart home devices, choices about placement, and configuration of settings. We observed three major ways nannies framed how power dynamics manifest in their relationships with their employers. First, working in their employers' houses, nannies view parents—as *home owners*—as having a right (or feeling they have a right) to protect the safety of their houses, and to choose what devices to install, where to locate them, and how to use them in their own houses. (In fact, though location-tracking devices and phone apps can be used to monitor a nanny who is out and about with her charges, few of our participants have had employers who have done so.)

Second, nannies recognize *parental prerogatives* to install technologies that can protect their children's safety, help to keep tabs on them, and facilitate communication between parents and children while the parents were not at home. Third, nannies believe that as their *bosses*, employers exercise freedom to set the rules, which nannies, as employees, might not always feel empowered to oppose or negotiate, due to job security concerns (e.g., fear of losing a job or receiving negative references).

In fact, few of the nannies we interviewed who have worked with cameras have ever discussed any details with their employers, beyond (usually) being informed of the cameras' existence. Discussions about data handling or privacy settings are rare, and few have stipulations about cameras in their contracts. However, while some nannies said they would like to have such discussions, or have access to privacy settings, others are not interested, especially if they have good relationships with their employers and trust that the employers will act in good faith. Examining the circumstances under which those conversations do occur—who initiates them, what triggers them, what each party's goals are, and what compromises are made—is a major focus of our analysis.

Cameras vs. Other Devices. With regard to other smart-home devices, such as smart speakers or smart TVs, few of our participants expressed strong privacy concerns. Many mentioned that they view cameras as enabling targeted surveillance, because cameras give their employers the power to collect and use data about them in ways that impact their day-to-day job performance, and might even result in job loss.

Employers' limited access to, say, smart speaker query history, has little potential to harm the nanny's job. Meanwhile, device service providers' collection and use of the data (from any device) does not target nannies specifically, and is, for most of our participants, a secondary concern at best.

7 Future Work

Once we have completed our analysis of the qualitative interviews with nannies and employers of nannies, we plan to quantify via surveys the prevalence of the themes emerging from our qualitative work, and to test statistically any observed relationships between those themes, or between themes and independent variables. For instance, we are interested in testing whether such factors as demographics, nannies' career history, attitudes toward technology and technological self-efficacy, whether the nanny/au pair lives in the employer's house, whether there is a contract, and/or whether nannies and/or parents have access to an agency's resources affect privacy norms, preferences, expectations, or power dynamics.

As part of the broader research program, we plan to investigate additional case studies focused on other groups of smart home bystanders, including caregivers for older adults, housecleaners or in-home maintenance workers, groups or organizations that hold in-home meetings, and residents of pre-equipped smart housing.

Finally, we plan to conduct research with designers, developers, and manufacturers of smart home devices, to understand the potential differences in mental models, opinions, norms, and expectations of those who create the devices, those who own them, and those who play the bystander role [cf. 9, 10, on how designers factor in the experiences of smart home primary users].

Based on our findings, we plan to develop conversation guides to facilitate discussion of privacy matters between smart home device owners and bystanders, and information materials and recommendations for domestic work force agencies, professional associations, and other relevant entities or platforms. We will also develop recommendations for policymakers for including considerations about bystanders' privacy concerns in consumer protection regulations.

Some participants mentioned the role of professional associations, such as the National Domestic Workers' Alliance (NDWA), in alerting domestic employees to laws about surveillance. We believe that, through industry standards, professional associations (e.g., International Nanny Association, American Caregiver Association, and the National Alliance for Caregiving, as well as the NDWA) and nanny agencies can take concrete steps to protect the privacy rights of smart home bystanders in specific groups of care and domestic workers. They can also—through the results of their experiments and experiences—set the example for other sectors, domains, and contexts, for industry self-regulation, as well as for general regulatory policy.

8 Conclusion

The research described here seeks to examine how the growing use of smart home and other IoT devices affects the privacy of bystanders and other non–primary users, to discover potential points of intervention for improving non–primary user privacy. Investigating the needs and practices of different user groups with regard to smart home devices helps us to untangle the specific ways in which both primary users and bystanders to (or targets of) smart home data collection reason about the privacy implications of their own and each other's choices, given the asymmetries of knowledge and control involved. Results from this research can feed into interventions in product design, policy, and employer-employee interactions, in order to achieve more privacy-respecting outcomes.

To explore the experiences, perspectives, and privacy concerns of domestic workers with regard to smart home devices, we conducted 26 interviews with nannies and 16 with parents who employ nannies. We focused mainly on devices designed primarily for home surveillance (e.g., security cameras). We found that some nannies perceived themselves as the primary targets of data collection by their employers who deployed cameras, while others described themselves as being bystanders to cameras.

Our preliminary findings, based on initial analysis, show that most nanny participants expect that houses they work in may have cameras, and some acknowledged the benefits of cameras. However, most participants want their employers to inform them about the existence, location, and purpose(s) of cameras; nannies view lack of disclosure as a sign of disrespect. Further, we noticed that nannies' perceptions of parents' intentions in deploying a smart home device strongly influence how the nannies feel about the device. Some nannies expressed more concern about devices collecting data about private rather than professional activities.

Although nanny participants often expressed privacy concerns and feelings of discomfort about surveillance, many mentioned that, due to power dynamics, they accept their employers' decisions to install cameras and how employers configure privacy settings. This power dynamic may explain—in part—why many of the nannies we interviewed have never discussed with their employers any details of how cameras or other devices collect, handle, and process data.

Acknowledgments

The authors thank for valuable comments Maritza Johnson, Franziska Roesner, Christine Geeng, Serge Egelman, Nathan Malkin, Yasemin Acar, Sascha Fahl, participants at the 2019 Symposium on the Applications of Contextual Integrity, and anonymous FOCI reviewers. This work was supported by grants from the Center for Long-Term Cybersecurity at the University of California, Berkeley, and from the U.S. National Security Agency.

References

[1] 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*, 2(2), June 2018. URL https://dl.acm.org/doi/abs/10.1145/3214262.

[2] Noah Apthorpe, Sarah Varghese, and Nick Feamster. Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 123–140, Santa Clara, CA, August 2019. USENIX Association. ISBN 978-1-939133-06-9. URL https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe.

[3] 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. doi: 10.1177/0193723516673409. URL https://doi.org/10.1177/0193723516673409.

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

[5] Sebastian Benthall and Bruce D. Haynes. Contexts are political: Field Theory and privacy. Presentation at the 2nd Symposium on Applications of Contextual Integrity, August 19–20, 2019, Berkeley, CA, USA.

[6] 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. URL https://doi.org/10.1080/23294515.2019.1568320.

[7] Nellie Bowls. Thermostats, locks and lights: Digital tools of domestic abuse. *New York Times*, June 2018. URL https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. Accessed: 23 July 2018.

[8] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place*, 50:112–118, 2018. ISSN 1353-8292. doi: https://doi.org/10.1016/j.healthplace.2018.01.006. URL http://www.sciencedirect.com/science/article/pii/S135382921730477X.

[9] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. Innovation inaction or in action? the role of user experience in the security and privacy design of smart home cameras. In *Proceedings of the Symposium on Usable Privacy and Security*. ACM Digital Library, 2020.

[10] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. Factoring user experience into the security and privacy design of smart home devices: A case study. In *Proceedings of the 2020 ACM Conference on Human Factors in Computing Systems (CHI '20)*, pages 1–9, 2020.

[11] 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 *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*, pages 61–70, New York, 2012. ACM. doi: 10.1145/2370216.2370226. URL http://doi.acm.org/10.1145/2370216.2370226.

[12] 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 *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pages 1387–1396. IEEE, July 2017. doi: 10.1109/CVPRW.2017.181. URL http://openaccess.thecvf.com/content_cvpr_2017_workshops/w16/papers/Satyanarayanan_Assisting_Users_in_CVPR_2017_paper.pdf.

[13] 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.

[14] 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. ISSN 1553-877X. doi: 10.1109/COMST.2017.2748998.

[15] Economic Policy Institute. Current Population Survey extracts, version 1.0.7, 2020. URL https://microdata.epi.org. Web page; accessed: 21 July 2020.

[16] Angella Foster. When parents eavesdrop on nannies. *New York Times*, August 2019. URL https://www.nytimes.com/2019/08/19/opinion/nanny-cams-privacy.html. Accessed: 8 June 2020.

[17] Vaibhav Garg, L. Jean Camp, Lesa Lorenzen-Huber, Kalpana Shankar, and Kay Connelly. Privacy concerns in assisted living technologies. *annals of telecommunications - annales des télécommunications*, 69(1):75–88, Feb 2014. ISSN 1958-9395. doi: 10.1007/s12243-013-0397-0. URL https://doi.org/10.1007/s12243-013-0397-0.

[18] Christine Geeng and Franziska Roesner. Who's in control?: Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 268:1–268:13, New York, NY, USA, 2019. ACM. doi: 10.1145/3290605.3300498. URL http://doi.acm.org/10.1145/3290605.3300498.

[19] Emily Starbuck Gerson. Nanny cams: What parents need to know before installing a home security camera, January 2019. URL https://www.care.com/c/stories/4337/nanny-cam-yes-or-no-plus-nanny-cam-reviews/. Blog post; accessed: 8 June 2020.

[20] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. Exploring consumers' attitudes of smart TV related privacy risks. In Theo Tryfonas, editor, *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*, Lecture Notes in Computer Science, pages 656–674, Cham, 2017. Springer.

[21] 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. URL http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf. Accessed: 17 February 2018.

[22] 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 *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2018.

[23] Loni Hagen. Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, dg.o '17, pages 598–599, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-5317-5. doi: 10.1145/3085228.3085254. URL http://doi.acm.org/10.1145/3085228.3085254.

[24] International Nanny Association. 2017 INA salary and benefits survey, December 2017. URL https://nanny.org/production/wp-content/uploads/2018/01/2017-INA-Nanny-Salary-Benefits-Survey-FINAL.pdf. Accessed: 8 July 2020.

[25] George Joseph. Racial disparities in police 'Stingray' surveillance, mapped. *CityLab*, October 2016. URL https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-surveillance-mapped/502715/. Accessed: 7 June 2020.

[26] Jennifer King. *Privacy, Disclosure, and Social Exchange Theory*. PhD thesis, University of California, Berkeley, CA, 2018. URL https://escholarship.org/content/qt5hw5w5c1/qt5hw5w5c1.pdf.

[27] 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, August 19–20, 2019, Berkeley, CA, USA.

[28] Thorin Klosowski. Your visitors deserve to know they're on camera. *New York Times*, October 2019. URL https://www.nytimes.com/2019/10/07/opinion/security-camera-privacy.html. Accessed: 8 June 2020.

[29] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. Further exploring communal technology use in smart homes: Social expectations. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems (CHI '20)*, pages 1–7, 2020. URL https://doi.org/10.1145/3334480.3382972.

[30] Martin J. Kraemer, William Seymour, and Ivan Flechais. Responsibility and privacy: Caring for a dependent in a digital age. In *Proceedings of the Workshop on Privacy and Power (Networked Privacy 2020), at the ACM Conference on Human Factors in Computing Systems (CHI '20)*, 2020.

[31] Hosub Lee and Alfred Kobsa. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, Dec 2016. doi: 10.1109/WF-IoT.2016.7845392.

[32] Linda Lee, Joong Hwa Lee, Serge Egelman, and David Wagner. Information disclosure concerns in the age of wearable computing. In *Proceedings of the NDSS Workshop on Usable Security (USEC '16)*. Internet Society, 2016. URL http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/information-disclosure-concerns-in-the-age-of-wearable-computing.pdf.

[33] Roxanne Leitão. Digital technologies and their role in intimate partner violence. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2018. ACM. doi: 10.1145/3170427.3180305. URL http://doi.acm.org/10.1145/3170427.3180305.

[34] 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. URL https://theelderlawjournal.com/2019/02/18/levy-kilgour-and-berridge/.

[35] Steve Lohr. Unblinking eyes track employees. *New York Times*, June 2014. URL https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html. Accessed: 23 July 2018.

[36] 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, Jun 2011. ISSN 1936-606X. doi: 10.1007/s12126-010-9083-y. URL https://doi.org/10.1007/s12126-010-9083-y.

[37] Deborah Lupton. Self-tracking cultures: Towards a sociology of personal informatics. In *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design*, OzCHI '14, pages 77–86, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-0653-9. doi: 10.1145/2686612.2686623. URL http://doi.acm.org/10.1145/2686612.2686623.

[38] Mary Madden. The devastating consequences of being poor in the digital age. *New York Times*, April 2019. URL https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html. Accessed: 7 June 2020.

[39] 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 *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK, April 23, 2018*, 2018. URL https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurousec2018_16_Malkin_paper.pdf.

[40] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4):250–271, 2019. doi: https://doi.org/10.2478/popets-2019-0068. URL https://content.sciendo.com/view/journals/popets/2019/4/article-p250.xml.

[41] 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), 2020.

[42] 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 *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA, 2017. USENIX Association. URL https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

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

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

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

[46] Parmy Olson. Wearable tech is plugging into health insurance. *Forbes*, June 2014. URL https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#360eb27018bd. Accessed: 23 July 2018.

[47] Scott R. Peppet. Regulating the Internet of Things: First steps toward managing discrimination, privacy, security & consent. *Texas Law Review*, 93:85–178, 2014. URL https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr93&div=5&id=&page=.

[48] James Pierce, Richmond Y. Wong, and Nick Merrill. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *Proceedings of the 2020 ACM Conference on Human Factors in Computing Systems (CHI '20)*, pages 1–19, 2020. URL https://doi.org/10.1145/3313831.3376347.

[49] 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. URL http://www.jstor.org/stable/26332001.

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

at the ACM Conference on Human Factors in Computing Systems (CHI '20), 2020.

[51] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. Augmented reality: Hard problems of law and policy. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14): Adjunct Publication*, pages 1283–1288, New York, NY, USA, 2014. ACM. doi: 10.1145/2638728.2641709. URL https://ssrn.com/abstract=2482198.

[52] Safe Smart Living. 16 smart home statistics and predictions, October 2019. URL https://www.safesmartliving.com/smart-home/statistics-and-predictions/. Web page; accessed: 16 July 2020.

[53] 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 *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '20)*, pages 1–13, 2020. URL https://doi.org/10.1145/3313831.3376585.

[54] Statista. Smart home penetration rate forecast worldwide from 2017 to 2024, June 2020. URL https://www.statista.com/forecasts/887636/penetration-rate-of-smart-homes-worldwide. Web page; accessed: 16 July 2020.

[55] Kaiwen Sun, Florian Schaub, and Christopher Brooks. It's everyone's home: Designing smart home technologies with children in mind. In *Proceedings of the Workshop on Privacy and Power (Networked Privacy 2020), at the ACM Conference on Human Factors in Computing Systems (CHI '20)*, 2020.

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

[57] U.S. Census Bureau and U.S. Bureau of Labor Statistics. Current populations survey (CPS). URL https://www.census.gov/programs-surveys/cps.html. Web page; accessed: 21 July 2020.

[58] Jenifer Sunrise Winter. Citizen perspectives on the customization/privacy paradox related to smart meter implementation. *International Journal of Technoethics*, 6 (1), 2015. doi: 10.4018/ijt.2015010104.

[59] 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. URL https://files.epi.org/pdf/194214.pdf. Accessed: 21 July 2020.

[60] 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), November 2019. doi: 10.1145/3359161. URL https://doi.org/10.1145/3359161.

[61] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, 2017. USENIX Association. ISBN 978-1-931971-39-3. URL https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

A Detailed Participant Characteristics

The data in Tables 3–6, covering demographics, job position and experience as a nanny, experience with technology, and exposure to devices, was collected via exit questionnaires after the interviews with our nanny participants. (Not including the participant dropped from analysis due to language difficulties.) While our sample is not demographically representative of the U.S. population as a whole (especially with respect to gender), we include in Table 3 data for nannies specifically, to show that our sample is closer to representing the target group.

Sources for Comparison Data. Tables 3 and 4 include statistics from the following sources, for comparison:

EPI Report: A report by the Economic Policy Institute (EPI) on the demographics and economic status of domestic workers in the U.S. [59], based on analysis of projection data from the Current Population Survey (CPS) conducted by the U.S. Census Bureau and U.S. Bureau of Labor Statistics (2017–2019 combined estimates) [15, 57]. Note that the CPS counts Hispanic/Non-Hispanic ethnicity separately from race, so EPI derives the ethnicity groupings we refer to in Table 3 (which parallel our participants' self-descriptors) by regrouping everyone of Hispanic ethnicity together, rather than using their race identifications.

INA Survey: The International Nanny Association's (INA's) 2017 survey of members [24] (N=1927). This survey was conducted internationally; however, 95% of the respondents were from the U.S., so we view it as providing a fair comparison.

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

Table 3: Demographics of nanny participants, with comparisons to statistics from an Economic Policy Institute report based on projection data from the the U.S. Current Population Survey [59], and to International Nanny Association statistics from an international survey [24]. (INA percentages are out of participants who answered a given question. EPI percentages and INA percentages may not add up to 100% due to rounding *or* due to additional categories/ranges beyond what we found.)

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

Table 4: Job situations and career trajectories of nanny participants, with comparisons to International Nanny Association survey statistics [24]. (INA percentages are out of participants who answered a given question. INA percentages may not add up to 100% due to rounding *or* due to additional categories/ranges beyond what we found.)
* The EPI report projects 52% of U.S. nannies are full-time and 48% are part-time [59].

Technology Experience	N	%
Technology Background (Positive answers, per question)		
Worked in a computer engineering or IT job position	2	8%
Majored/minored in computer science or computer engineering	0	0%
Has written a computer program	0	0%
How Often Participant Is Asked for Advice About Computers or Technology		
Rarely	8	32%
Sometimes	14	56%
Frequently	3	12%

Table 5: Technology experience and knowledge of nanny participants. Questions borrowed with modifications from Tan et al. 2017 [56].

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

Table 6: Number and percentage of nanny participants whose employer(s) has/have certain smart devices in their home(s) (N=24) and who have smart devices in their own home (N=25). (One participant answered only about the latter.) Answers for "Other smart devices" were recategorized by the authors as all belonging to existing categories.