Smart Home Bystanders: Further Complexifying a Complex Context

Julia Bernd[1,2], Alisa Frik[1,2], Maritza Johnson[2], and Nathan Malkin[2]
[1]International Computer Science Institute; [2]University of California, Berkeley
{jbernd,afrik}@icsi.berkeley.edu,maritzaj@ischool.berkeley.edu,nmalkin@cs.berkeley.edu

ABSTRACT

This paper outlines a research agenda to understand how the expanding use of smart home devices affects the privacy of individuals who did not choose to deploy them, and may not even be aware of them. We describe current and planned studies with domestic workers and people who employ domestic workers, other populations likely to be affected by the increasing use of smart home devices, and product teams who design such devices. Findings will support guidelines, and recommendations for developers of smart-home devices and for policymakers, as well as public-education materials.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing** → *Ubiquitous computing*; • **Social and professional topics** → *Surveillance.*

KEYWORDS

privacy, smart homes, surveillance, bystanders, digital inequality

1 INTRODUCTION

As technology development becomes more focused on devices that are designed to be part of an environment—i.e., the Internet of Things—those devices are increasingly collecting data about that whole environment, not just specific users. These IoT devices therefore impact the privacy not only of the individuals who choose to deploy them, but of the people around them (i.e., bystanders).

This paper lays out a research agenda to examine how the growth of the IoT, especially smart homes, is affecting the privacy of people who are *not* the primary end users of the devices—and how those effects can be mitigated in product development.

Problems with typical proposed privacy solutions such as better disclosure, improved controls, and conservative defaults have been raised even with regard to primary users [e.g., 22, 24, 33, 35, 46], but the issues are even more complicated when we consider how people interact with devices they do not control, or may even be unaware of. In addition, some basics of privacy protection can be implemented without needing to know much about the specific context of use, but designing meaningful and useful controls and choosing defaults that represent people's expectations and interests requires an understanding of specific contexts.

Context is likely to play an even greater role in future smart-home devices, which will collect more data more of the time. One likely source of contextual challenges will be devices designed for one context that may inadvertently collect data about another, such as a voice-controlled microwave that overhears a non–cooking related conversation that takes place in the kitchen. Presenting an extra challenge will be devices explicitly designed to operate in multiple contexts; for example, smart speakers today are used primarily for entertainment but also have current and future uses that involve health and work. To adequately navigate these settings, devices will need to develop a much greater level of situational awareness, differentiating between currently active contexts as well as resolving potential differences between the preferences of the people present. Yet, since many people present will be bystanders, their preferences might not be known ahead of time.

We plan to approach these issues from two angles. First, we will study groups of people for whom bystander concerns are likely to be amplified, such as domestic employees (e.g. nannies, caregivers for the elderly and disabled, housecleaners, gardeners) and those who employ them, older adults who have safety monitors in their homes, and residents of pre-equipped "smart" housing. At the same time, we will study smart home product teams, to understand how they currently make decisions about data use, both for the direct customer and for people who *aren't* the direct customer (if they consider the latter at all). Based on our findings, we will develop and test an experimental training for product teams to increase the visibility of bystanders in product design.

Our decision to begin with case studies of household employees has three main reasons. First, we 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 on more general public surveillance or tracking, where decisions about privacy are completely removed from the subjects of the data collection. Domestic workers present an interesting in-between case, in that there is direct interaction and some kind of personal accountability between the primary users choosing to deploy the device and others whose privacy may be affected by it.

Finally, the study of in-home employees presents an interesting case for the theory of Privacy as Contextual Integrity (CI), due to the multi-dimensional nature of the context. Firstly, it is a home—a private space, and one where the householders traditionally have more control of what goes on than they do elsewhere—but it is also a workplace. Secondly, there is an employer–employee relationship (with attendant financial dependence). But for caregiving employees, there is also a care relationship involved, so the usual professional divides cannot be applied simply. So, for example, perspectives on the balance between safety concerns and privacy rights are likely to be different than in other workplaces.

2 RELATED WORK

Privacy researchers have begun developing a body of work on people's understandings of, expectations about, and concerns about how IoT devices—particularly smart home devices—collect, use, and share data [e.g. 8, 15, 36, 47, 49–51, 55]. Privacy impacts of IoT

technologies can have differential impacts across populations, due to differences in knowledge and skills [e.g. 4, 20, 40] or because power imbalances mean collected data end up reinforcing existing discrimination [e.g. 13, 40].

Such imbalances can also play out in workplace data collection, for example wearable health trackers distributed by employers, e.g. to reduce insurance costs [e.g., 30, 32, 39] or to track details of professional athletes' performance [3]. Ongoing work by Kraemer and Flechais [25] relates control over smart-home devices to existing socio-cultural dynamics (the social order within the home). In the worst case, taking advantage of control over smart-home devices may be an element in domestic abuse [6, 29].

Many studies focus on how people's preferences and concerns about smart home data collection and sharing vary according to particular contextual and situational factors [e.g. 2, 16, 18, 27, 28, 34, 37]. Most studies that compared locales for data collection found that people are more sensitive about data collected in their homes than, for example, in their workplaces or in business establishments [e.g. 9, 27, 37] [*contra* 19]. This raises interesting questions about what happens when one person's workplace is another person's home, as in some of our planned case studies.

Work within the framework of Contextual Integrity [5, 38] investigates how people reason about privacy when the context for data collection blends features and norms from multiple contexts. CI researchers have examined how people think about smart-home devices based on (or not based on) norms about privacy in the home vs., for example, the Internet [e.g. 2, 31, 52], finding that the crossing of contexts these devices represent can give rise to new considerations [7]. We anticipate that CI will be important in helping us reveal the additional complexities when this already intricate situation is blended with norms about information collection and sharing in the workplace.

While most work on IoT privacy expectations and preferences has focused on primary users—including their concerns about bystanders [21, 23, 53, 54]—there is relatively little work on the expectations of bystanders and non-primary users. Some studies have investigated bystanders' views of wearable computing devices [e.g. 1, 41]. Studies on wearables, autonomous vehicles, and drones have examined the influence of contextual factors such as purpose and location, as well as signalling mechanisms and bystanders' ability to control data collection [e.g. 11, 14, 17, 26, 42, 44, 45, 48, 54].

Smart-home devices have received less attention, but concerns of bystanders such as visitors to smart homes—or even co-habitants who did not make the choice to install the device—are discussed briefly in some of the literature [e.g., 8, 43, 55]. However, to our knowledge, there have not been any studies on the expectations and concerns of in-home care workers in smart homes.

3 PLANNED RESEARCH STUDIES

3.1 Studies With Likely Bystanders

To develop a more comprehensive understanding of how the expanding use of smart home devices affects the privacy of everyone who interacts with them, we are conducting focused case studies with groups of people who are especially likely to interact with smart home devices they do not control. In some cases, such groups might really be unintended bystanders to the data collection, and in some cases, they might be explicit targets. At a high level, our research question for these studies is:

- What are the smart home experiences, privacy expectations, and privacy concerns of people who aren't (usually) the primary users of the devices?

Nannies and Parents. We are beginning with a two-side case study of nannies and parents who employ nannies. We will investigate parents' deliberate use of smart home devices (such as home security systems or baby-cams/remote monitors, as well as nanny cams *per se*) to keep tabs on nannies, babysitters, and au pairs. We will also investigate the dynamics around smart home devices that parents are most likely deploying for other reasons, such as smart speakers, smart toys, or smart TVs that use sensors for, e.g., voice commands or presence detection. In the first case (surveillance devices), nannies may be the targets of the data collection; in the second case (other smart home devices), they are likely to be bystanders.

As of the time of writing, we are currently conducting an analysis of data from an online forum for nannies (preliminary findings in §4), and will soon begin conducting qualitative interviews with both nannies and parents who employ nannies. We are also planning quantitative surveys. Research questions for this case study include:

(1) What are the experiences and the privacy attitudes, expectations, and concerns of domestic workers who may be observed and recorded by smart home devices they did not choose to deploy?
(2) Do potentially different framings of the context by domestic workers and by their employers affect each party's expectations, attitudes, and choices about data collection and sharing?
(3) How do employers' and employees' attitudes and choices about smart home data collection reflect, reinforce, or change existing power dynamics in those 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 caregivers' preferences about data being collected and shared about them by their employers' devices?

Home Care Attendants, Care Clients, and Families. The second planned case study is similar to the nannies and parents study, but will be three-side, including both elderly or disabled care clients, and family members of such care clients who have control of remote monitoring systems in the care client's homes. (In the case of nannies and parents, there is of course a third side, i.e. the children, but they will not be included in the study.) We hope that the three-side dynamic will provide an opportunity to examine how contextual privacy norms and expectations compare between seniors and the family members who want to protect them. We also plan to compare how those family members reason about the privacy of the seniors vs. their care attendants., potentially revealing power dynamics at play.

Housecleaners/In-Home Maintenance Workers. Another potential study could focus on smart-home devices in homes where more intermittent domestic employees or service providers, such as housecleaners, gardeners, and/or repairpeople, are employed.

Again, this would be a two-side study, investigating the experiences and attitudes of both in-home workers and people who employ such workers. It would likely present interesting contrasts with nannies or care attendants, in that these workers work in many different houses for many different clients. We speculate that differences might arise from the fact that clients do not have the impetus of concern for their loved ones to deliberately spy on workers, but on the other hand, would usually have less personal connection and thus perhaps less feeling of accountability to respect the workers' privacy with regard to incidental data capture.

Groups/Organizations That Hold In-Home Meetings. A rather different study might examine how hosts and attendees of regular meetings that may take place in people's homes (e.g. church groups, support groups, HOAs, political/activist groups, volunteer cohorts, or craft clubs) view the use or potential use of smart-home devices that might collect data about visitors. We anticipate that studying different types of groups might yield insights about how the sensitivity of the topic might—or might not—affect people's attitudes in combination with specific expectations about the home context. Studying groups in different places may also be of value, as both attendees and hosts may have different expectations about how likely or taken-for-granted smart home devices would be.

Smart Housing Residents. Another possible case study could reach out to residents of housing that is "smart by default," for example dorm rooms equipped with smart speakers [10] or housing in new developments that comes with a suite of IoT devices built in [12]. This would allow us to explore what considerations come into play when the primary user—the one who controls the device—is not necessarily an IoT enthusiast/early adopter.

3.2 Studies With the General Population

We expect the case studies described above with employees and employers/clients to illuminate how socio-economic power dynamics can impact privacy negotiations with regard to smart home dynamics. To develop a broader picture of the potentially differing effects of indirect interactions with IoT across demographic divides, we also plan to conduct a survey study with the general population (via intercepts in public spaces in different locales). Research questions include:

- How do IoT experiences and privacy concerns vary across different communities/populations, for example, by socio-economic status?
- How do people who aren't (necessarily) primary users/early adopters encounter and interact with IoT/smart home devices?
- How do the contexts in which non–primary users encounter IoT/smart home devices affect their expectations about data collection and sharing?

3.3 Developer Studies and Design Impact

In parallel with the studies of non–primary users of smart home devices, we intend to conduct research with smart home product teams to discover how we may be able to increase developers' attention to bystander privacy. We will then develop and test an experimental training based on the research results. Research questions include:

- How and to what degree do smart home product designers currently account for non–primary users' privacy concerns?
- What approaches could be effective in increasing non–primary users' visibility in product design?

The overall goal of our research program is to have impact through training materials, guidelines, and best practices for different stakeholders: product teams, consumer advocacy groups, policymakers, and users (primary and non-primary) of the devices. In particular, improving the design of IoT products in regard to privacy and data protections requires that more product designers and developers understand the importance of addressing the needs of a broad audience, including secondary users and bystanders. In the best case, even companies who are not invested in the privacy of non–primary users for its own sake will increasingly be concerned about brand reputation and compliance, as these issues gain media traction and continue to be a focus of new laws and regulations.

4 (VERY) PRELIMINARY FINDINGS

As a first pass at sketching out some factors that might come into play for nannies working in smart homes, we looked at around eight months' worth of posts in the Nanny forum on Reddit.[1] This is a public forum, mostly frequented by nannies, au pairs, and professional babysitters, but open to parents as well. The preliminary impressions below are based on 75 threads where nanny cams, security cameras, or audio monitors[2] were mentioned and 16 posts mentioning other types of IoT devices.

4.1 Cameras and Deliberate Surveillance

Expectations, Opinions, Preferences, and Choices. Even nannies who have not worked with cameras anticipate having to make choices about it in the future. However, nannies who don't work in the U.S. believe such monitoring is less common in other countries. They do not expect it *a priori*, would expect to be informed it it took place, and would be more likely to view it as indicating a potentially problematic employer (because it is not the norm). Nannies in the U.S. are more likely to say they expect monitoring or at least view it as normal, and some say they always assume they are being monitored whether they are informed or not.

However, such discussions still make reference to privacy norms, even if the posters/commenters do not count on them being followed. Some comments refer explicitly to the clash between workplace and home contexts that can give rise to nannies' and parents' differing reasoning about privacy and data collection (among other things). Nannies (especially experienced/career nannies) view themselves as professionals and try to promote professional employer–employee relationships, workplace-based norms for communication, and respect for boundaries. But they are aware that the blurring of boundaries—due to the personal nature of the relationship and the fact that the work takes place in their employer's home—means that parents may not be applying those norms (or if they are not experienced supervisors, may not know what the norms are).

Some Reddit nannies are so uncomfortable with being on camera that they simply will not accept (or keep) jobs where they know

[1] https://www.reddit.com/r/Nanny/

[2] We did not include references to standard audio or A/V baby monitors that do not record and are not accessible to the parents when the nanny is at work.

CI Parameter	Expected/Acceptable Collection	(Potential) Privacy Violation
Recipients	Only Mom Boss views video	Dad Boss views video
	Only parents view data	Parents show data to friends
	Data stays on-device	Data is sent/stored off-device
Subjects	Monitors nanny with children	Monitors nanny by themself (at naptime, etc.)
Attributes	Monitors common areas, children's bedrooms, outside	Monitors bathrooms**
	Video collected	Audio collected*
Transmission Principles	Nanny knows there are cameras/monitors	Nanny doesn't know about cameras/monitoring**
	Nanny knows where all cameras/monitors are	Nanny doesn't know where cameras/monitors are**
	Parents only use to check for abuse/neglect	Parents micromanage based on observations*
	Parents spot-check occasionally	Parents continually watch/listen to live feed*
	Nanny can use, or has separate baby monitor	Nanny is monitored but can't monitor*
	Passive observation	Parents give orders to nanny through monitor
	Data is erased regularly	Data is stored indefinitely
	Data is kept secure/transmitted securely	Poor data security

Table 1: Conditions of acceptance for cameras (for at least some nannies). * indicates more commonly mentioned.

there are cameras. Others say they are totally used to cameras and barely think about them. This basic comfort or discomfort—in combination with job possibilities—may drive choices about working with monitoring more than more abstract attitudes or opinions about whether cameras are appropriate.

Discussions that mention cameras also often mention potential benefits to nannies. The most commonly mentioned benefit is that cameras can protect a nanny from spurious or incorrect accusations. Other benefits include parents seeing the nanny being good at their job; providing evidence for conversations about children's problematic behavior; and even helping nannies keep their cool because they know they're being observed.

Parameters of Acceptable Collection. Even nannies who agree with cameras and are comfortable working with them are likely to mention factors that make the camera use/monitoring acceptable to them (at least in theory, even if they don't enforce those conditions). Some of the conditions mentioned by Reddit nannies are listed in Table 1, grouped according to the parameters of information transmission outlined in the Contextual Integrity framework [5].

Employer–Employee Power Dynamics. Discussions of cameras and monitoring on the Nanny subReddit often lead to—or are part of—discussions about employer–employee relationships and nannies' rights to stipulate conditions of their work situations. A common theme in the forum is the importance of having a contract. When newer nannies ask for advice on what should be included, specifications about camera use are mentioned frequently—either complete prohibition or disclosure of cameras and (less commonly) limitations on data use/retention, depending on the nanny's preferences.

In general, older or more experienced nannies will often advise less experienced nannies on how to deal with issues with their employers. Such situations may be discussed in terms of individual personalities and/or contextualized within general social dynamics (undervaluing of care work, overvaluing of rich people). Much of the advice amounts to "Know your worth and demand respect".

Within this framing, an employer who respects their nanny will disclose the existence of cameras and abide by the nanny's stipulations about the data. Failing to disclose cameras is seen as not respecting a nanny's rights. Again, nannies do not necessarily *expect* their employers to treat them with respect, but they view it as a prescriptive norm. Depending on their level of experience, the state of the nanny job market, and their own financial situation—they may view it as grounds for quitting if their rights are not respected (including if they discover hidden cameras). If job prospects are narrower, they may be less in a position to push professional norms.

4.2 Other IoT Devices

Other IoT devices do not come up as often in the Nanny subReddit; online forums may not be a very fruitful source for data about devices whose primary purpose (for the user) is not surveillance. None of the 7 threads mentioning smart speakers touched data collection. In a few cases, nannies inquired about whether particular devices could be used for surveillance (an Amazon Echo Show, a bluetooth TV speaker), demonstrating that IoT data flows may still be a black box for many. Unlike with in-home monitors, location tracking (via phone apps, key fobs, etc.) is not viewed as expectable in any situation, making disclosure even more imperative.

5 CONCLUDING REMARKS

We anticipate that applying the analytical framework of Contextual Integrity will help us to untangle the specific ways in which both primary users and bystanders to (or targets of) smart home data collection—as well as the product teams that design smart home devices—reason about the privacy implications of their own and each other's choices, given the asymmetries of knowledge and control involved. We hope to present the research agenda and some preliminary results from our first case study (textual data and, by then, interviews) at the CI symposium in order to seek feedback on how CI can help to address these complexities.

REFERENCES

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

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies* 2, 2 (June 2018). Preprint: https://arxiv.org/abs/1805.06031.

[3] Andrew Baerg. 2017. Big Data, Sport, and the Digital Divide: Theorizing How Athletes Might Respond to Big Data Monitoring. *Journal of Sport and Social Issues* 41, 1 (2017), 3–20. https://doi.org/10.1177/0193723516673409

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

[5] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. 2006. Privacy and Contextual Integrity: Framework and Applications. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP '06)*. IEEE Computer Society, Washington, DC, 184–198. https://doi.org/10.1109/SP.2006.32

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

[7] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place* 50 (2018), 112–118. https://doi.org/10.1016/j.healthplace.2018.01.006

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

[9] Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, and Mahadev Satyanarayanan. 2017. 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*. IEEE, 1387–1396. https://doi.org/10.1109/CVPRW.2017.181

[10] Dani Deahl. 2018. Saint Louis University is placing 2,300 Echo Dots in student living spaces. *The Verge* (15 August 2018). https://www.theverge.com/2018/8/15/17693174/saint-louis-university-echo-dots-amazon-student-living-spaces Accessed: 7 December 2018.

[11] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-Mediating Technologies. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352

[12] Daniel Eran Dilger. 2018. Lennar now integrating Amazon Alexa surveillance into new home construction. *AppleInsider* (April 2018). https://appleinsider.com/articles/18/04/17/lennar-now-integrating-amazon-alexa-surveillance-into-new-home-construction Accessed: 18 May 2018.

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

[14] Barrett Ens, Tovi Grossman, Fraser Anderson, Justin Matejka, and George Fitzmaurice. 2015. Candid Interaction: Revealing Hidden Mobile and Wearable Computing Activities. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology (UIST '15)*. ACM, New York, NY, USA, 467–476. https://doi.org/10.1145/2807442.2807449

[15] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce S. Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS), August 11–13, 2019.*

[16] Vaibhav Garg, L. Jean Camp, Lesa Lorenzen-Huber, Kalpana Shankar, and Kay Connelly. 2014. Privacy concerns in assisted living technologies. *annals of telecommunications - annales des télécommunications* 69, 1 (01 Feb 2014), 75–88. https://doi.org/10.1007/s12243-013-0397-0

[17] Jun Ge. 2016. *Observers' Privacy Concerns about Wearable Cameras.* Master's thesis. Pennsylvania State University. https://etda.libraries.psu.edu/catalog/28890 Masters thesis.

[18] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 2017. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS) (Lecture Notes in Computer Science)*, Theo Tryfonas (Ed.). Springer, Cham, 656–674.

[19] Jessica Groopman and Susan Etlinger. 2015. *Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry.* Technical Report. http://www.altimetergroup.com/pdf/reports/Consumer-Perceptions-Privacy-IoT-Altimeter-Group.pdf Accessed: 17 February 2018.

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

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

[22] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and Privacy: It's Complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12) (SOUPS)*. ACM, New York, NY, Article 9, 15 pages. https://doi.org/10.1145/2335356.2335369

[23] Marion Koelle, Wilko Heuten, and Susanne Boll. 2017. Are You Hiding It?: Usage Habits of Lifelogging Camera Wearers. In *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '17)*. ACM, New York, NY, USA, Article 80, 8 pages. https://doi.org/10.1145/3098279.3122123

[24] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122 – 134. https://doi.org/10.1016/j.cose.2015.07.002

[25] Martin Kraemer and Ivan Flechais. 2018. Disentangling Privacy in Smart Homes. http://privaci.info/symposium/Disentangling_in_Smart_Homes.pdf Presentation at the Symposium on Applications of Contextual Integrity, Princeton, NJ, September 13–14, 2018. Unpublished work. Accessed 20 November 2018.

[26] Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl. 2017. Exploring Design Directions for Wearable Privacy. In *Proceedings of the Symposium on Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/usec

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

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

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

[30] Steve Lohr. 2014. Unblinking Eyes Track Employees. *New York Times* (June 2014). https://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html Accessed: 23 July 2018.

[31] Lesa Lorenzen-Huber, Mary Boutain, L. Jean Camp, Kalpana Shankar, and Kay H. Connelly. 2011. Privacy, Technology, and Aging: A Proposed Framework. *Ageing International* 36, 2 (01 Jun 2011), 232–252. https://doi.org/10.1007/s12126-010-9083-y

[32] Deborah Lupton. 2014. 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)*. ACM, New York, NY, USA, 77–86. https://doi.org/10.1145/2686612.2686623

[33] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A Study of Privacy Settings Errors in an Online Social Network. In *Proceedings of the 4th IEEE International Workshop on Security and Social Networking (SESOC '12)*.

[34] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. 'What *can't* data be used for?' Privacy expectations about smart TVs in the U.S.. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK, April 23, 2018.* https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurousec2018_16_Malkin_paper.pdf

[35] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal on Law and Policy for the Information Society* 4, 3 (2008), 540–565. https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf

[36] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. 2016. Understanding the Privacy Design Space for Personal Connected Objects. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion! (HCI '16)*. BCS Learning & Development Ltd., Swindon, UK, Article 18, 18:1–18:13 pages. https://doi.org/10.14236/ewic/HCI2016.18

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

[38] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Fall 2011), 32–48.

[39] Parmy Olson. 2014. Wearable Tech Is Plugging into Health Insurance. *Forbes* (June 2014). https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#360eb27018bd Accessed: 23 July 2018.

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

[41] Halley Profita, Reem Albaghli, Leah Findlater, Paul Jaeger, and Shaun K. Kane. 2016. The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use. In *Proceedings of the 2016 ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 4884–4895. https://doi.org/10.1145/2858036.2858130

[42] Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. "You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 143–157. https://www.usenix.org/conference/soups2018/presentation/rashidi

[43] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo. 2014. 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*. ACM, New York, NY, USA, 1283–1288. https://doi.org/10.1145/2638728.2641709

[44] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. 2016. You Are Being Watched: Bystanders' Perspective on the Use of Camera Devices in Public Spaces. In *Proceedings of the 2016 ACM Conference on Human Factors in Computing Systems (CHI '16): Extended Abstracts*. ACM, New York, NY, USA, 3197–3203. https://doi.org/10.1145/2851581.2892522

[45] Manya Sleeper, Sebastian Schnorf, Brian Kemler, and Sunny Consolvo. 2015. Attitudes Toward Vehicle-based Sensing and Recording. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 1017–1028. https://doi.org/10.1145/2750858.2806064

[46] Daniel J. Solove. 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 1880 (2013).

[47] John Vines, Stephen Lindsay, Gary W. Pritchard, Mabel Lie, David Greathead, Patrick Olivier, and Katie Brittain. 2013. Making Family Care Work: Dependence, Privacy and Remote Home Monitoring Telecare Systems. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. ACM, New York, NY, USA, 607–616. https://doi.org/10.1145/2493432.2493469

[48] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in the US. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 172 – 190. https://content.sciendo.com/view/journals/popets/2016/3/article-p172.xml

[49] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. 2017. "Privacy Is the Boring Bit": User Perceptions and Behaviour in the Internet-of-Things. In *15th International Conference on Privacy, Security, and Trust (PST 2017)*.

[50] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart Homes and Their Users: A Systematic Analysis and Key Challenges. *Personal and Ubiquitous Computing* 19, 2 (Feb. 2015), 463–476. https://doi.org/10.1007/s00779-014-0813-0

[51] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and Risks of Smart Home Technologies. *Energy Policy* 103 (April 2017), 72–83. https://doi.org/10.1016/j.enpol.2016.12.047

[52] Jenifer Sunrise Winter. 2015. Citizen Perspectives on the Customization/Privacy Paradox Related to Smart Meter Implementation. *International Journal of Technoethics* 6, 1 (2015). https://doi.org/10.4018/ijt.2015010104

[53] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices. In *Proceedings of the 2017 ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 6789–6793. https://doi.org/10.1145/3025453.3026049

[54] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6777–6788.

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