Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy

IMTIAZ AHMAD, Department of Computer Science, Indiana University Bloomington, USA
ROSTA FARZAN, School of Computing and Information, University of Pittsburgh, USA
APU KAPADIA, Department of Computer Science, Indiana University Bloomington, USA
ADAM J. LEE, Department of Computer Science, University of Pittsburgh, USA

Sensor-enabled computers in the form of 'IoT' devices such as home security cameras and voice assistants are increasingly becoming pervasive in our environment. With the embedded cameras and microphones in these devices, this 'invasion' of our everyday spaces can pose significant threats to the privacy of bystanders. Because of their complex functionality, even when people attempt privacy measures (such as asking the owner to "turn the camera off"), these devices may still record information because of the lack of a 'real' off button. With the ambiguities of current designs, a bystander's *perceived* privacy can diverge from their *actual* privacy. Indeed, being able to assess one's actual privacy is a key aspect in managing one's privacy according to Altman's theory of boundary regulation, and current designs fall short in assuring people of their privacy. To understand how people as bystanders manage their privacy with IoT devices, we conducted an interview study about people's perceptions of and behaviors around current IoT devices. We find that although participants' behaviors line up with Altman's theory of boundary regulation, in the face of uncertainty about their privacy, they desire or engage in various 'tangible' workarounds. Based on our findings, we identify and introduce the concept of 'tangible privacy' as being essential to boundary regulation with IoT devices. We argue that IoT devices should be designed in a way that clearly and unambiguously conveys sensor states to people around them and make actionable design recommendations to provide strong privacy assurances to bystanders.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**.

Additional Key Words and Phrases: IoT; tangible design; privacy

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

1 INTRODUCTION

High-fidelity and often privacy-invasive sensor-enabled devices are becoming pervasive in our everyday environments — the number of internet-connected 'IoT' devices is estimated to reach

Authors' addresses: Imtiaz Ahmad, Department of Computer Science, Indiana University Bloomington, 700 N Woodlawn Ave, Bloomington, Indiana, USA, imtahmad@iu.edu; Rosta Farzan, School of Computing and Information, University of Pittsburgh, 135 North Bellefield Avenue, Pittsburgh, Pennsylvania, USA, rfarzan@pitt.edu; Apu Kapadia, Department of Computer Science, Indiana University Bloomington, 700 N Woodlawn Ave, Bloomington, Indiana, USA, kapadia@indiana.edu; Adam J. Lee, Department of Computer Science, University of Pittsburgh, 210 S. Bouquet St., Pittsburgh, Pennsylvania, USA, adamlee@pitt.edu.

2573-0142/2020/10-ART116 $15.00
https://doi.org/10.1145/3415187

more than 200 *billion* by 2020 [28]. At home, digital assistants such as Amazon's Echo[1] and Echo Look[2] can constantly 'listen' for instructions and even 'look' and comment on clothing choices after a visual inspection. Inside and outside of homes, security cameras such as the Nest Cam[3] can be on the lookout for unusual activities. The ubiquitous presence of such networked cameras and microphones 'peeking' into one's personal spaces has given rise to a range of electronic privacy concerns [21, 23, 48, 51, 71]. In addition to unauthorized recordings being stored in the cloud, researchers have highlighted privacy concerns related to inadvertent recordings and have argued for providing users with more control over their data [15]. With the proliferation of such IoT devices, casual conversations and encounters once thought to be private and ephemeral now may be captured and disseminated or archived digitally, and, at worst, can be used for malicious purposes, often without the knowledge of the user.[4]

Despite the various documented privacy concerns, designing these devices in a way that enhances privacy, especially for all stakeholders such as guests,[5] visitors, and passersby who are not the owners of these devices, remains a challenge [33]. We refer to this group of people in the vicinity as 'bystanders' of such devices, who are potentially affected by these devices but do not own or directly use them (i.e., they are 'indirect stakeholders'[6]). Although device owners may have some understanding of how and when these devices collect information, bystanders are particularly vulnerable and concerned about their privacy given their potential unfamiliarity with these devices and limited insight into the current configuration of nearby devices [17, 22, 69]. We posit that it is imperative that the IoT devices be designed in a way that assures the privacy of bystanders. Thus, an important goal of our research is ensuring that privacy – and people's sense of privacy – is improved for *all* stakeholders through adequate feedback (and where possible, control) mechanisms.

Norman [41] posited that feedback to users on the internal operations of systems is essential for awareness, reassurance, and anticipation of further actions. With the design of many of today's popular sensors, however, individuals often are not able to discern when and how they are being recorded. It is oftentimes unclear whether an audio or video sensor is, indeed, 'off' upon visual inspection by occupants of a space. In general, the lack of clear feedback about what is being recorded can lead to people forming inaccurate mental models of how and when the device collects information [67]. People do expect visual feedback [11, 14] from digital devices; yet, the feedback itself can be unreliable. For example, even though the Nest Cam has an LED indicator, the use of this indicator was optional until only recently[7] and controlled by software. Even for situations where camera LED indicators are controlled (ostensibly) through hardware, there have been demonstrated attacks disabling the LED indicator for some laptops [7]. Attackers in general can surveil victims without their knowledge [18, 19, 53, 63]; despite the use of LED indicators or software controls, users still cannot be confident that they are *not* being recorded. Designs of sensors should reliably convey the recording states of devices, and current efforts fall short in assuring people of their privacy. Interpreting the behavior of sensors should not require a high level of familiarity with or intimate knowledge of the sensors — the confusion and concerns about the recording states of devices are exacerbated when the person being recorded is a bystander of the device. Thus, the aim

[1]https://www.amazon. com/b/?ie=UTF8&node=9818047011l

[2]https://www.amazon.com/Amazon-Echo-Look-Camera-Style-Assistant/dp/B0186JAEWK

[3]https://nest.com/cameras/nest-cam-outdoor/overview/

[4]Gary Horcher. Woman says her Amazon device recorded private conversation, sent it out to random contact. https://kiro.tv/2J5QLwP.

[5]One timely example of such a concern is of guests discovering the existence of live streaming internet-connected cameras in their Airbnb apartment rentals [20] and not knowing if or when these cameras were recording their actions.

[6]Friedman et al. define 'indirect stakeholders' as "parties who are affected by the use of the system" as opposed to 'direct stakeholders' who "interact directly with the computer system or its output" [22, p. 239].

[7]https://www.techhive.com/article/3432337/google-nixes-the-ability-turn-off-the-status-light-on-nest-cameras.html

of our study is filling the existing gap in the current literature on how to design devices that assure bystanders of their privacy, i.e., provide them with a more 'tangible' sense of privacy.

In considering the design of sensors, theories of privacy can be helpful in understanding people's privacy concerns. Many theories of privacy focus on how information is *disseminated* among people (and their social networks). In the context of our inquiry, we consider two theories to be especially relevant to data *collection*: Nissenbaum's theory of Contextual Integrity [40] and Altman's theory of Privacy Regulation [1]. In her theory of privacy as 'contextual integrity', Nissenbaum discusses how privacy violations can occur when 'norms of appropriateness' are violated in the dissemination and collection of information. As IoT devices become more prevalent, the new forms of data collection and designs of sensors for the casual bystander can be vastly different from their expectations and what they assume as norms of data collection. We seek to understand how these deviations impact people's perceptions and expectations as they encounter such devices 'in the wild'.

Beyond people's perceptions of what may be (in)appropriate, people must manage their personal boundaries in the face of embedded IoT devices and regulate what information is captured by these sensors. From a 'boundary regulation' perspective, Altman's theory on privacy regulation in the context of one's *physical* privacy is particularly salient; Altman discusses how individuals manage the boundaries of their personal space as a dynamic process in negotiation with others in their space [1]. IoT devices, however, make the boundary-regulation process more complex as compared to managing interpersonal privacy in the (mere) presence of other people. Interpersonal interactions with other people within a physical space come with a high degree of certainty about the effectiveness of one's privacy-enhancing actions. For example, the presence of others listening or watching during one's conversations or actions can be evaluated with a high degree of certainty. However, it is unclear how people can evaluate the efficacy of their boundary-regulation behaviors with IoT devices given their software-controlled and display-limited nature. For instance, can a device's software-controlled 'off' button be overridden by other running software? This lack of certainty leads to a mismatch between one's *perceived* level of privacy (e.g., believing the sensor is off) and *actual* level of privacy (e.g., the sensor is still recording), making applications of frameworks like Altman's difficult. We seek to explore the relationship between the design of these devices and how people manage their privacy in *human-IoT* interactions.

In particular, we seek to answer the following research questions in this work:

R1 What are the current perceptions of people as bystanders of how and when IoT devices collect audio and video data? We seek to understand whether current designs of IoT devices match the perceptions of people not intimately familiar with the devices (i.e., those who are inexperienced with the functionality of the particular devices) and how deviations from people's expectations affect their assessment of privacy. Understanding such deviations can provide insight into intuitive designs that can bring people's perceptions in line with their expectations as they encounter such devices 'in the wild'.

R2 What kind of privacy-enhancing behaviors do bystanders use or conceptualize when encountering sensors? We seek to understand how people, particularly bystanders, try to manage their privacy both using current affordances as well as workarounds. These workarounds provide insights into the future design of privacy mechanisms as well as suggest how people manage their privacy while interacting with IoT devices in socio-technical spaces.

To answer our research questions, we conducted an interview study with 19 participants to uncover how bystanders can be assured of their privacy with improved sensor designs. Our study focused on two common smart connected devices: the Nest Cam[8] security camera and the Amazon

[8]https://nest.com/cameras/nest-cam-indoor/overview/

Echo Show[9] smart voice assistant. Both of these devices feature embedded cameras and microphones, with the Echo Show focused on microphone-based functionality and the Nest Cam focused on camera-based functionality. All participants were unfamiliar with the operation of these two devices and had never owned either device.

We find that people engage in similar boundary regulation behaviors as described by Altman's theory, but the mismatch between one's 'perceived' and 'actual' privacy makes it more difficult for bystanders – who use more familiar interpersonal boundary regulation mechanisms – to manage their privacy with IoT devices. Our results highlight the importance and need for design solutions that provide clear privacy assurances to bystanders to reduce uncertainty with regulating their privacy. That is, not only should people have a strong perception of privacy (these perceptions could be misplaced, as often happens in phishing attacks), but this perception should be aligned with reality, providing a strong assurance of privacy as well.

Based on our findings, we identify and define 'tangible privacy' mechanisms as those privacy control and feedback mechanisms that are 'tangible', i.e., manipulated or perceived by touch, and of 'high assurance', i.e., they provide clear confidence and certainty of privacy to observers. Camera lens caps and the common use of stickers on laptop cameras are examples of tangible privacy mechanisms. On the other hand, an LED indicator is not (since it lacks the certainty provided by a lens cap: a bystander may worry the camera could still be recording with the LED off). We argue that 'tangible privacy' is an important property for the design of sensors to address the privacy concerns of bystanders and aligns well with the theories of contextual integrity (by providing more appropriate forms of data collection) and boundary regulation (by providing a better assessment of one's privacy). *Based on our findings, we advocate for sensor designs that allow for intuitive, tangible ways of manipulating data collection and convey a clear and definite sense of privacy to bystanders so they can be assured of their privacy.*

2 RELATED WORK

In this section, we start by discussing the theoretical framing of our work. We then discuss research in the context of IoT security and privacy, bystander privacy concerns, and privacy notices and other feedback mechanisms currently used for conveying privacy to the users of IoT devices.

2.1 Theoretical framing: Contextual Integrity and Boundary Regulation

Two theories of privacy are particularly salient to our work: Nissenbaum's work on 'contextual integrity' [40] and Altman's model of 'boundary regulation'.

Contextual Integrity. Contextual Integrity (CI) defines privacy as 'appropriate information flows' according to norms specific to social contexts.[10] Three key concepts constitute CI: (a) Social contexts – which define the appropriate norms; these are not formally constructed but rather discovered as parts of social life. (b) Contextual norms – which govern information flows and people's privacy expectations in a given context depend on them. (c) Contextual purposes – which help comprehend the purpose of respective contexts. Privacy as contextual integrity is respected when all these concepts are respected and the 'entrenched informational norms' are followed. One important aspect of information flows relates to norms of data collection. In particular, if the means of data recording by IoT devices deviate from expected norms of data collection, people's privacy can be violated. Such discord between one's expectations and the actual behavior of sensors is particularly heightened for bystanders, who may not be familiar with the specific devices and may

[9] https://en.wikipedia.org/wiki/Amazon_Echo_Show

[10] Social norms are implicit (informal) rules that are unspoken, not formally written or recorded but generally understood, and considered as acceptable behavior by a social group [9, 39].

make incorrect assumptions about the devices based on data collection norms familiar to them. The incorrect mapping of such norms based on the data collection contexts could also lead people to underestimate their privacy risks.

Boundary regulation. Altman's theory of privacy regulation has been a seminal work with respect to regulating social interactions in physical spaces. Altman conceptualized privacy as "an interpersonal boundary process by which a person or group regulates interaction with others" [1]. Altman's model of privacy regulation starts with an individual's desire to achieve a certain level of privacy (defined as 'desired privacy' in the model), which is derived from a combination of personal, interpersonal, and situational factors. Then, to regulate their privacy, individuals go through an iterative process where they use different control mechanisms to move toward their desired level of privacy. In each iteration, after using the control mechanisms, people achieve a certain level of privacy which may or may not be equal to their expected initial level of 'desired privacy'. The model defines this certain level of achieved privacy as 'achieved/actual privacy'. They assess the effectiveness of the used control mechanisms by comparing their initial 'desired privacy' with the 'actual privacy' they achieved by using the control mechanisms. If their attempt at controlling their privacy is insufficient (i.e., their actual privacy is less than their desired privacy), they can experience a feeling of 'crowding' in their space. If their attempt in managing their privacy is more than sufficient (i.e., their actual privacy is more than their desired privacy), they can experience 'social isolation'. When individuals experience either of the two (crowding or social isolation), they re-adjust their 'desired privacy' and go through the same iterative process until they reach 'optimum privacy'; i.e. the actual privacy is equal to the desired privacy. The privacy control mechanisms involve verbal and nonverbal behaviors (such as body language) and consideration of personal space and territories.

2.2 Privacy and security concerns with IoT devices

Security and privacy for IoT devices have been identified as major research challenges by The EU Commission in a recent report [62]. Accordingly, a growing body of work has sought to understand the privacy concerns of users in the context of ubiquitous sensing devices. They have investigated privacy and security concerns associated with internet-connected devices in the home [3, 57], connected children's toys [37, 61], assistive and monitoring technologies for senior citizens [10, 31], and household robots [19].

Interview studies with smart home users have shown that although users might express general concerns about physical security and home privacy, their mental models of privacy threats are often incomplete [71]. People tend to trust IoT manufacturers, and their desire for convenience and connectedness often influences their desired level of privacy. Further, people are not always aware of the privacy risks associated with the data collected by smart devices [72]. In the case of surveillance, Oulasvirta et al. found that although people may initially be anxious and concerned about their privacy, they gradually become accustomed to the presence of security cameras [42]. The authors also studied people's privacy-seeking behaviors under ubiquitous surveillance and found four kinds of privacy-seeking behaviors: ceasing a behavior entirely, hiding it from sensors, acting privately under surveillance, and manipulating the sensors. Research has also shown a power imbalance between owners of smart voice assistants and other family members. The primary users often restrict control of IoT devices and check how other family members are using their devices. At the same time, studies of users' privacy-seeking behaviors around smart devices, such as smart speakers, highlight that users believe existing privacy controls do not meet their needs [32]. Roman et al. emphasizes the necessity of improving peoples' awareness on how sensor-based devices collect, store, and share their information [50]. In a co-design study Yao et al. explored user-centered

privacy designs for smart homes and identified key design factors including data transparency and control [68]. Furthermore, users often expressed concerns about how companies handle their data and they strongly opposed the use of their data by third parties [34, 49].

These prior works have investigated privacy and security issues related to IoT devices and smart homes, both from devices' and end users' perspectives. The privacy and security issues identified by these works show the importance of providing people with control and awareness about their privacy as they interact with these devices. In line with these prior studies, in our work, we investigate bystanders' current perceptions and behaviors related to sensor data collection. Based on an understanding of how current design affordances fail to provide enough control and feedback, we derive design implications to provide bystanders with a more 'tangible' sense of privacy about their data *collection*.

2.3 Bystanders' privacy concerns about smart devices

The pervasiveness of smart sensor devices has introduced a distinct privacy concern, i.e., the privacy concerns of bystanders around smart devices and what is now discussed as the line between 'smart' security monitoring and being 'creepy' [45]. Smart home security cameras now have 'ample opportunities for casual peeks into the lives of others' [45, p. 5]. 'Indirect stakeholders' have indeed expressed the concern of being "watched" by cameras they do not own [22]. Bystanders' privacy perceptions of drones with cameras have also been studied. Bystanders expressed their concerns of being peeked at, stalked, and surveilled by drones in public places [66]. Yao et al. studied drone bystanders' and drone controllers' perceptions of different privacy mechanisms. They found that the two privacy mechanisms most supported by both the groups are owner registration and automatic face blurring [70]. Besides, research has been conducted on bystanders' privacy concerns in the presence of lifelogging wearable devices both from lifeloggers' and bystanders' points of view [13, 27].

In the context of augmented-reality glasses, bystanders show an interest in ways to block recording devices while also being concerned about "the logistics of such capabilities" [17, p. 2385]. As a result, recent research has been focusing on identifying design suggestions to specifically support the privacy of bystanders and advocate for the 'transparency' of the behavior of such devices [69] [45, p. 5]. Such design suggestions include providing bystanders with ways to detect sensors in a space or to limit their data collection [69]. In their study of privacy behaviors with lifelogging cameras, Hoyle et al. reported some participants (as owners) taking the camera off when entering a bathroom because they did not trust the software controls (to pause collection of photos). In the context of bystanders, participants reported instances of other people requesting the camera not be used. In general, this work found evidence for the importance of physical 'camera covers' and bystanders requesting owners to limit collection.

Motivated by this line of research, our work focuses on a deeper understanding of bystanders' perceptions of smart devices equipped with multiple sensors and their privacy behaviors (such as workarounds) around them. Our goal is not to investigate bystanders' privacy concerns. Instead, building on the prior works, we aim to clearly convey to bystanders when the devices are – and are not – recording information and allow for suitable controls with predictable outcomes to advance the discussion around how bystanders' privacy needs can be supported by incorporating 'tangible privacy'.

2.4 Privacy notices: use of indicators

Privacy notices are important in making people aware of data practices of the personal information gathered by a system. Prior work has shown that perceptive interaction with a device increases peoples' understanding of and engagement with the devices [16]. Traditionally, LED

status indicators have been heavily used in video recording devices such as laptops, first-person cameras, and security cameras for conveying privacy notices. For example, in their recent work, Song et al. made use of LEDs to create low-cost locators to help people find nearby IoT devices [59]. Voice-based devices, such as Google Home and Amazon Alexa, have also made use of status lights to communicate the device's state to people in the vicinity.

Although such indicators might seem like a good way of announcing a device's current status, prior research has shown that it is not an optimal strategy for several reasons. The lighting behaviors of LEDs are often ambiguous to people [25] or people can miss the indicators when they are engaged in the tasks at hand [46]. In response to these concerns, more recent work has explored possible ways for body-worn cameras to effectively convey privacy notices [30]. Researchers discuss how when it comes to the ubiquitous presence of devices with the ability of speech recognition, the design of devices should involve questions like whether the devices should contain obvious visual cues when transmitting data [24]. In some cases, people may need to rely on other timing (when it is provided) technologies (e.g., a mobile app) to understand the meaning of the flashing LEDs [70].

We extend this body of work by studying bystanders' perceptions of LED indicators and how they interpret the different colors shown, as well as positing the insufficiency of other firmware/software-based indicators (e.g., displaying messages on the screen or providing audio feedback). We also show that typical IoT device indicators lack a sense of trustworthiness that our participants identified as necessary to have in order to understand what is being collected by their devices.

3 METHOD

To answer our research questions, we conducted a semi-structured interview study of participants recruited from in and around our university. We used two IoT devices equipped with both audio and video recording sensors for our study: the Nest indoor camera and the Amazon Echo Show. We chose two types of IoT devices with both audio and video recording abilities for two reasons: 1) this choice represents a realistic setting because most smart devices these days are equipped with both video and audio recording sensors; and 2) these sensors are used in two different contexts (personal assistant vs. a security camera) but have the capabilities of capturing the same kind of information about bystanders. This choice allows us to study users' perceptions of privacy and their privacy enhancing behaviors when in proximity of devices that are equipped with multiple sensors as well as study differences in perception based on the primary purpose of the device (home security vs. smart assistant). The study was approved by the affiliated university's ethics board.

3.1 Recruiting and Screening

We recruited our participants through flyers posted in and around a university campus, on the university's internal online advertisement forum, and several university mailing lists. The advertisement invited individuals to "Participate in a Research Interview about IoT devices"; to avoid biasing our recruitment, we did not include any specific terms about privacy in our advertisement.

We sought to recruit 'bystander' participants who were not intimately familiar with the Echo Show and Nest Cam. Interviewing participants less familiar with such devices helps us to better reflect what the physical designs of the devices convey to people – bystanders – about their states of collection. This was encouraged by including a statement in the recruitment advertisement that no prior background experience was needed to participate in the study. We confirmed their prior inexperience with these devices during the interviews. In addition, we screened for owners of such devices during the interview. Only two participants indicated they had prior experience as owners of a security camera and an Amazon Echo. We continued the interview and paid the participants to collect data for a potential future study of owners. We do not include their data in our analysis for this work. In the end, we were successful in recruiting 19 participants with no prior experience

with these devices. Participants explicitly confirmed they were unfamiliar with the operation of these two devices.

3.2 Participants

We interviewed a total of 19 participants. We interviewed 15 participants in September, October, and November of 2018. Although a point of saturation was reached in this set of interviews (after 13 interviews), we recruited and interviewed four additional participants (using the same recruitment strategy) in October 2019. The second round of interviews was conducted mainly to confirm the initial set of themes. Our coding and analysis process involved the first step of one author (the interviewer) creating the initial code book by analyzing the transcriptions of the interviews. These initial codes were then finalized through regular meetings of all co-authors and discussion of the codes to reach consensus. To ensure that the themes generated through this process were overarching and comprehensive, we complemented our initial set of interviews with additional interviews and confirmed and updated our codes. Another reason for conducting these additional interviews was to obtain additional qualitative insights for some of the themes in Sections 4.3 and 4.5.

Our participants represented a range of different educational backgrounds, including Computer Science, Game Design, Education, Mathematics, Human Biology, Marketing, Linguistics, Music, Kinesiology, Media, Human Computer Interaction, Photo Journalism, Telecommunication, Cybersecurity, Pre-Nursing, Law and Public Policy, Media Advertising, Chemistry, Optometry, and Microbiology. Seven of our participants identified as males and 12 as females. In terms of the age, 16 were in the age range of 18–24 years, one in 24–30, and two in 30–35. Ten of them had not completed their college degree, three of them were high school graduates, four had completed their bachelor's degree, and two had completed their master's degree.

3.3 Interview Protocol

The interview process started with an introduction to the devices including an official promotional video of the devices. The participants were also given the opportunity to examine the devices to understand them and the different functionality of each device before we started the interview questions. The participants were also allowed to interact with the devices throughout the interview session. The introduction was then followed up with a short, six-question demographic survey, a series of 16 semi-structured interview questions, a series of scenario-based questions, and design-related questions. An overview of our interview protocol is provided in the appendix.

Each interview lasted about 45–90 minutes (with an average of 56 minutes). Participants were compensated with $15 cash or gift card. The first four participants were paid by gift card, and the rest were paid in cash at the end of the interview. The interviews were conducted by one of the authors. The interview questions were divided into two parts. In the first part, we focused on understanding participants' perceptions of the devices: how they think these devices function and how they perceive the role of such devices in various personal spaces. As bystanders, people may not know when a device is on or off, how to turn it off if they encounter such a device, and what it means for a device to be on or off; a number of questions thus focused on asking the participants to identify the 'on' and 'off' state of the devices, and studying participants' interaction with each state of the device, i.e., asking them to turn the device on or off, and whether they were certain about the on/off state of the device.

In the second part of the interview, we provided the participants with different scenarios related to each of the devices to explore their privacy concerns. To avoid priming individuals' responses, we did not use the term 'privacy' in our scenarios. For example, we asked the participants about how they would feel about presence of these devices during their next doctor visit. However, in

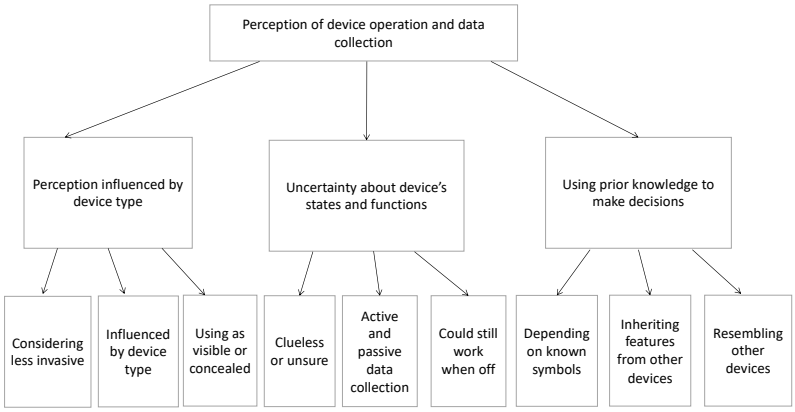

Fig. 1. Example of low-level codes and high-level categories in our coding

almost all cases, participants' raised privacy concerns with such devices. If they stated any privacy concerns, we then asked about their privacy-enhancing behaviors.

We ended the interview by asking them about their preferred design modifications of the devices that would make them more confident about their privacy.

3.4 Analysis

All the interviews were audio recorded, and a professional transcription service provider (REV) was used for transcribing the recordings. We made sure that no personal identifiable information was mentioned during the interview that could be linked to our participants.

A combination of open, axial, and selective coding was used to extract important themes from the interview data [6, 29, 55]. Initially, the first author of the paper analyzed the data inductively using open coding and identified a large list of relevant codes. Through subsequent group discussions in our research team, the large list of low-level codes was grouped into higher level codes using axial coding with minimal a priori assumptions. Figure 1 shows an example of our coding process. The bottom row represents the codes generated in open coding, the middle row represents codes generated using axial coding, and the top row represents the code generated using selective coding.

Using this iterative process of identifying codes and clustering the codes into categories based on the content of the first five interviews, we then developed a code-book. Based on the code-book, we coded each of the interview transcripts. The research team held weekly meetings where the coauthors discussed and revised these codes until consensus was reached. A total of 84 codes were identified at the initial coding stage. Examples of some initial codes include 'Certainty of States', 'Feedback Modality', 'Incomprehension of Microphones', 'Relying on Existing Affordances', and 'Privacy-Enhancing Strategies'.

Finally, selective coding was used to group codes, and we identified five overarching themes that emerged from the annotation of the interview data. The themes are described in the Findings section. Themes were generated and then refined as content was added under each theme. Regular discussions were held between the first author (the interviewer) and other authors about the codes and themes throughout the analysis period. We note that since we focus on a thematic analysis based on multiple iterations of meetings and refinement of the codes to determine emergent themes, we did not seek to compute inter-rater reliability, a decision that is in line with common practice [4, 36].

3.5 Limitations

As a qualitative study, this work sheds light on various recurring themes that we identified in our interviews and should not be seen as generalizing to the population in a statistically significant sense. Although the scenarios used in the interviews are taken from familiar real-world situations (i.e., visiting friends or doctors), they are hypothetically described to our participants. Thus, there might be some differences between our participants' responses (privacy enhancing behaviors) and their real-life behaviors. However, our findings show that some of the reported behaviors were, in fact, real-life behaviors (e.g., covering the device, turning the face of devices, etc.) indicating that although hypothetically presented, some participants had actually been in such scenarios (e.g., with other devices) and had practiced those privacy-enhancing behaviors. We also note that in real-life scenarios bystanders might not notice the devices and be oblivious to data collection. For this study, we assume bystanders will notice, or be notified about, the presence of such devices. However, further exploration is needed to make sure the sensors themselves are noticeable and recognizable. Our participants represent a younger population. Older participants may have different privacy concerns as well as different interpretations of IoT designs and indicators. Although one worry may be that younger populations are less concerned about their privacy, we note that Singh et al. [58] found that when it comes to sharing information with smart devices, younger adults are more reluctant than older adults. Thus, interviewing a younger population may reveal several interesting reasons for not sharing data with smart devices.

4 FINDINGS - RQ1: PERCEPTIONS OF DEVICE OPERATION AND DATA COLLECTION

In response to a set of interview questions that were designed to assess our participants' perception of the functionality of the devices, the following themes emerged:

4.1 Uncertainty about the device states

As a bystander and the indirect stakeholder who has not been in charge of the device, the first need is being able to make clear and correct determinations of the state of devices and their functionality under each state. Central to this is the ability to understand whether a device is 'on' or 'off.' Assessing the on/off state of devices has typically been straightforward for users of most devices: there is an on/off button that turns the device on and off, and once the device is off, all the functionalities of the device are completely disabled. However, as devices have become 'smarter', on and off states have become much more complicated. For example, with the Echo Show and Nest Cam devices, we observed that our participants understood the 'on' state with a high level of certainty. However, they often were not clear about the characteristics of the 'off' state. As highlighted below, participants used a number of strategies to assess the on/off state of the devices. Although these approaches allowed them to indicate effectively that a device was on, the same approaches were insufficient for convincing them that the device was actually off. For example, participants stated that the device could still be collecting data when perceived as 'off', as highlighted in the quotes below:

> "If the LED is on, I cannot tell that the device is on or off. I will have to look at my phone." (P8, Nest Cam)

> "Looking at it, I see a screen with data. Now if the screen is blank, that doesn't necessarily mean she's not on, because like I said, there could be a screen saver or something going across." (P6, Echo Show)

In both cases, the participants were unclear whether the device was actually off.

When explaining what it meant for a device to be 'on', the majority of our participants focused on whether it was actively collecting audio or video data:

> "When you say it's on, you probably mean that it's listening to what you say and it's listening for the keyword." (P15)

> "I imagine on would be like recording and audio and video at the same time." (P13)

With respect to explaining the 'off' state, some participants defined 'off' as being powered off and thus being unable to record anything.

> "I'd say, like, no power running through it, period. Like, it's not video recording, it's not taking sound, it's incapable of anything without actual, like, energy." (P9)

> "Powered completely off, and nothing's recording, nothing's on. Yeah. So it's just the opposite [of 'on']." (P11)

Our participants, however, had a less definite understanding of what it means for a device to be 'off' and were more likely to assume that the device was in an intermediate 'stand-by' state. According to these participants, when a device is not 'on', it could either be totally 'off' (i.e., not collecting any data and not connected to any power source) or it could potentially be in a third state, which they defined as a 'stand-by' or 'sleep' state.

In this state, the device visually appears to be off, but it could be listening or it could be triggered (willingly or accidentally) to start recording at any time. Participants assumed when a device is turned off through a third-party application, such as a mobile application but it is still connected to a power source, it enters the 'stand-by' state. The following quotes highlight the indication of the 'stand-by' state.

> "Just like a standby. So, like, it could be active, but it's not actively recording per se. Until, like, I say, okay, I want it to start recording." (P9)

> "I think when you press this button she's still on but maybe like it doesn't take in what you tell her. She's like sleep[ing]." (P14)

> "They're always listening. Sleep would be not collecting visual, but still collecting sound, location, But off would be totally unplugging it to where it couldn't collect anything." (P10, Nest Cam)

Furthermore, they were uncertain about how selectively disabling collection of audio vs. video affected the collection of the other data. For example, one of the participants said that an Echo Show could continue to record visuals even when it is muted.

> "When the audio is off, it could be recording visual, I don't know, it could be. I don't see why it would but it could." (P15, Echo Show)

In the end, albeit a simple request, participants wanted a reliable, physical 'off' button in their interactions with sensors:

> "I don't like that there's not an off button. Even if you unplug it, I would still like there to be an off button for it." (P15)

> "Definitely, put an on and off button for the actual recording settings of the microphone and the camera. And, I think that would help a lot." (P12)

In summary, participants were not clear when a device was actually 'off' in the sense of being completely powered down. They considered the uncertain status of 'stand-by' mode as the more likely state a device might be in when turned 'off'; it was expected that devices in this state could still be collecting data. Participants expressed desire for a physical 'off' button that would completely power down the device.

4.2 Reliance on existing mental model of indicators

The uncertainty about the device states propelled us to ask the participants to identify the features of the devices that they would use as cues to determine the device's current state. For the Nest Cam, participants used the LED indicator as the primary way of inferring the device's state. In other cases, participants manually checked the video feedback from the mobile app. For the Echo Show, they used the audio feedback and the display screen as the primary means of confirming the device's state.

In interaction with the LEDs to infer the device's state, our participants used their existing mental model of traffic lights to interpret the meaning of LED indicators when green and red lights were shown. They interpreted a green LED as a 'Go' signal, meaning the device is on and it's recording, and a red LED as a 'Stop' sign, meaning the device has stopped recording.

> "I see the green light, I go. If I see green, I can go out and say it's fine, it's working fine. I mean, I'm just guessing. Probably if I unplug it, I will see the other side of it." (P4)

> "Cause usually a green light means on, red means off." (P5)

Moreover, comparing the Nest Cam to a webcam, participants expressed their expectation of seeing a green LED while recording because a standard webcam shows a green LED whenever it is recording.

> "I have a webcam back home, if it's recording it shows some green light or something. I think this probably would, too. 'Cause this to me is not a camera, it's just a webcam." (P7)

In some cases, applying this prior mental model did not match the operation of IoT devices. For instance, when a Nest Cam's status light is red, it does not mean that the device is not recording any video; rather, this indicates that the *LED* is not functioning properly, and the device itself may continue to function "as expected."[11] On the other hand, if the LED is off, it means either the device is off or potentially recording if the LED indicator was turned off in the settings.[12]

Interestingly, some participants did not rely on the existing visual cues and said that they would use the heat signature of a device to determine it's state.

> "Maybe like a heat signature? 'Cause you can usually tell if something's on if you can feel the heat." (P9)

> "I mean, it's [the device] pretty toasty, like warm" (P15)

Because LEDs did not provide participants with an ironclad assurance of whether a device is on, our participants specifically wanted a shutter-based mechanism for cameras, which clearly conveys when a camera is able to record and when it is not, and a mute button to make sure that only video is recorded without any audio.

> "Maybe put a shutter feature over the lens ... because then I'd be sure that it's not recording me." (P1)

> "First of all, shutters. Like an eyelid, close when its fully closed and then open when its fully open." (P7)

For microphones, however, our participants did not have many ideas. Only a handful said that they would physically disable a microphone by muffling it with another object like a blanket – which is likely not effective at blocking sound completely.

[11] https://www.nest-community.com/s/question/0D51W00005Fp6MHSAZ/what-does-the-red-light-on-my-nest-cam-mean

[12] It was only in Aug. 2019 that Google announced new interpretations of the LED light so that some form of lighting showed – including blinking – when the camera was on.

> "As far as sound goes, like I said, you really don't have much options, because it's just there, so you have to just put it somewhere else where it's not near you." (P9)

> "Put something over it like, a blanket for example. That would help muffle any sound getting through." (P2)

In summary, we observed that our participants, as bystanders who are not intimately familiar with devices, relied on their existing understanding of well-known devices to interpret affordances of these new devices such as LED indicators and visual and auditory feedback to assess the on/off state of the devices. Similarly, they relied on their existing mental model of devices when thinking about possible designs to better afford their desired certainty. As we argued, without our explicit prompt, their workaround solutions involve tangible interaction with the devices such as camera shutters instead of relying on LEDs.

4.3 Perceptions are guided by primary function of devices

We observed that participants' perceptions of a device were often influenced by the primary function or role of that device. Both the Nest Cam and Echo Show have a camera and a microphone. However, the primary function of the Nest Cam as a security camera is collecting video, whereas the primary function of Echo Show is collecting audio as it is understood to be an audio-based command-processing device. As a result, participants' perceptions influenced how they assessed features of the devices and their concerns with the devices. For example, P15 reported having fewer concerns regarding Echo Show because Echo Show's main purpose is not watching but interacting with people.

> "This one less so than the camera only because its main purpose is not to watch, it's to interact with." (P15)

Similarly, even after knowing that Echo Show has an embedded camera, P8 admits to having no privacy concerns regarding video recording because the "nature" of the Echo Show makes video recording a secondary function compared to audio recording.

> "I guess it is to do with the nature of the device. Even though it has a camera and everything, I see it as very secondary to the audio function." (P8)

The primary function of Echo Show made P7 think that the device cannot 'record' anything, it can only listen to audio cues and act accordingly.

> "Personally, I don't think this can record [video]. So I wouldn't have too much of a concern. That one [the camera] I know it's for recording, this one, for me, it's just a chore, doing a job. It can't do anything...'cause I'm pretty sure it can't record, I just think it's just here to hear the audio cues and act." (P7)

As we learned about this specific bias toward the main function of the device, in later interviews, we ensured to prompt the participants to elaborate on this issue. We continued to observe a similar trend. For example, P17 and P18 expressed that they were comfortable with the presence of an Echo Show in a bedroom as they believed that unlike the Nest Cam, Echo Show's primary function is not recording video.

> "This one[Nest Cam] its sole or the only thing it can do is record and that one has a lot of more other functions so I don't really think about it as much.." (P17)

> "Yeah. Because this one[Echo Show] doesn't record." (P18)

In fact, almost all participants' perception of the primary function of the device was indicated as a factor regarding their comfort with the presence of the device in a particular location. Although almost all of the participants were not comfortable with the presence of a Nest Cam in a bedroom because of privacy reasons, only three out of 19 participants expressed concern about the presence

of an Echo Show in a bedroom, and of these three, only two mentioned privacy as the reason. Similarly, 10 of the participants said that they wouldn't be bothered with the presence of an Echo Show in a bathroom, and out of nine participants who were uncomfortable with the presence of an Echo Show in a bathroom, only three cited privacy risks (e.g., the presence of a camera, the chances of eavesdropping) as the reason. The others mentioned reasons such as the device might be demolished by the excessive humidity or by the presence of water around it.

Our participants were more comfortable with the presence of voice assistants compared to security cameras in places generally deemed as private. This is a particularly interesting finding considering that the reasons they were citing (e.g., hacking, secretly watching) for being uncomfortable with the Nest Cam are also possible with the Echo Show as both devices have a camera sensor. This, again, can be attributed to the influence that the primary function of a device have over a bystander's perception, as mentioned by P16 when talking about the reason of being less hesitant about the Echo Show's presence in a bathroom.

> "I think that there's a little less hesitation with this one[Echo Show]. I don't know if it's stupid or not, I guess, but just because, like I said, the functionality of this device isn't just to be a camera." (P16)

In summary, we continued to observe how the existing mental models of our participants as indirect stakeholders of these devices not only influenced their perceptions regarding the functionality of the devices but also their privacy concerns associated with the devices.

4.4 Mistrust for software

When probed about possible design of sensor control mechanisms, all but two participants said that they preferred 'more physical' designs (e.g., shutters and physical 'off' buttons) . From our interviews, we identified two main reasons why participants did not trust software-based controls. First, many participants said that they feared that software-based controls could be vulnerable or compromised by adversaries.

> "Because I think it would be trusted more because there might be a glitch in the software and you might not be able to tell." (P2)

> "If it was software, you could know from your phone, there could be some flaws in it, where somebody could still hack that server." (P12)

The second reason is related to the perception of a stronger sense of empowerment and control over a device through hardware designs. Participants said that tangible mechanisms gave them their desired control over a device, which in turn gave them an extra level of assurance.

> "It's kind of empowering to the person to be able to physically turn it off, I think. I think it's frustrating for consumers to not be able to physically turn off the device." (P11)

> "Because you usually have control over hardware. Other people can remotely control software. You can't really remotely control hardware." (P13)

> "Do you really know it's off? 'Cause I don't know anything about the technology built. Someone who designed it could have a backup system or something. So the only way I feel in control is if I manually do it myself." (P7)

In general, our participants expressed strong trust issues with privacy indicators and controls that can be controlled by software. We found that 'tangibility' is implicitly present in their coping mechanisms and it gives them a better sense of assurance and control over the device.

4.5 Degree of visibility of sensors influences the perception of the sensor

Our participants were quick to identify camera sensors as compared to microphones since microphones are often not visible enough. Often, they mistook microphones for speakers.

> "That's probably the speaker. And I don't know where the microphone is. But it could be in both, it could be both. This also looks like there's a little bit of a speaker portion on the top." (P11)

And in some cases, not identifying a microphone in a device made the participants perceive the device as not having a microphone. For example, even though the Nest Camera has an embedded microphone, P3 went on to conclude that the device does not have one.

> "Actually I'm not sure. Like, if I can see some hole or something that I can see that it's listening, but I don't see something like that ... So it has a speaker, but I don't think it has a microphone." (P3)

The lack of visibility and transparency about the existence of microphones is particularly threatening to the privacy of bystanders who may not be aware of the possibility of being recorded. Participant P10 went a step forward and said that he would mark, i.e., put some kind of identifying symbol around the microphone, to know of its existence.

> " I'd mark wherever the mic is, 'cause I'm not sure if the mic is there." (P10)

5 FINDINGS - RQ2: BYSTANDERS' COPING AND CONTROLLING MECHANISMS

To address our second research question on bystanders' privacy-enhancing behaviors, we sought participants' concerns when interacting with the devices and their coping mechanisms to manage their concerns. As mentioned before, we did not specifically prompt participants with privacy questions, but privacy concerns were naturally raised in many participant responses. In this section, we focus on such concerns and participants' approaches in managing them. Following Altman's theory of privacy regulation [1], we also define coping mechanisms as the set of 'workarounds' [47] or privacy-enhancing behaviors outside of the scope of privacy controls supported by the devices (e.g., 'Mute' functionality) which participants utilized in an attempt to maintain their desired level of privacy. We observed that participants' coping mechanisms closely followed Altman's categorization: 'filtering', 'ignoring', 'blocking', 'withdrawal', and 'aggression', which are used to reduce emotional stress and anxiety when individuals are in a state of social 'crowding' or 'isolation'. Below, we discuss examples of each of those mechanisms. We discuss how each of these mechanisms happens in the context of interaction with smart connected devices in physical spaces.

Filtering the intensity of inputs: Filtering as described by Altman is the "reduction of intensity of inputs" [1], which people often use for regulating their privacy preferences in social interaction. In interaction with the devices, our participants considered a number of strategies to filter out the undesirable impact of the devices, such as playing loud music to mask a private conversation, having the device on at certain times only, or avoiding certain tasks in the presence of the devices to filter out some of the available information. Examples of such statements from our interviews are highlighted below:

> "I would probably play super loud music to block it out. So that way, it will only hear the loud music and not what I'm saying." (P19)

> "Play some music. So, the conversation is not as clear." (P5)

> "If somebody's going to analyze my data, then I would want to be sure that this thing is on and off at certain times." (P15)

> "I think in private scenarios, if you know there's a camera at, you might limit your conversations. You might not talk about things." (P11)

Participants tried to drown out inputs or exercised discretion around such devices to reduce the relative intensity or availability of sensitive information to sensors.

Ignoring low-priority inputs: Altman considers ignoring low-priority interactions and being selective in which interactions to pay attention to as a strategy to deal with being overwhelmed with too much social interaction [1]. In interaction with devices, especially for bystanders and indirect stakeholders, ignoring the interaction can be more complicated. However, we observed the indication of attempts to ignore the presence of devices as an approach in coping with the inflicted distress. As highlighted in the quotes below, our participants stated how they considered audio collection to be lower priority than video and would try to ignore issues related to audio collection to reduce their sense of being overwhelmed by them.

> "It could still be recording like audio or something but that's fine. Audio is not that much of a concern as visual." (P7)

> "I wouldn't be too concerned, because I don't know. Like, the voice part doesn't really get to me. It's the video part that I would be worried about." (P12)

> "I feel like that's [video data collection] really personal. Audio is definitely evasive too. I feel like video is a lot more invasive than audio. I feel like when it comes down to it, there's not a lot of audio that I wouldn't care. Not that I wouldn't care, but that would get me in trouble. Yeah, I would definitely say video is more invasive and concerns me more." (P17)

Although some participants decided to simply not worry about certain modalities of collection, these workarounds point to the need for better ways to convey assurance to bystanders whether a sensor is recording or not so that they don't have to 'prioritize' their privacy concerns and behaviors in a way that still leaves them vulnerable to privacy risks.

Blocking of stimulus: Another coping mechanism for social crowding is described as "blocking of stimulus inputs by means of unlisted telephone numbers, doormen and guards who control entrances to buildings, and even an unfriendly countenance to discourage others" [1, p. 178]. When individuals feel filtering and ignoring are not adequate strategies, they opt for blocking. In responses provided by our participants, we also observed indication of blocking as a strategy to deal with concerns with the devices, such as covering the camera lens or the microphone with a blanket, a towel, or a cup to muffle the device.

> "I would put something over it like, a blanket for example. That would also help muffle any sound as well getting through." (P2)

> "I'd put a little cover on top of it just to make sure it wasn't collecting sound or something." (P10)

> "I think I could just get like a towel and put it over it, so it can't see, it can't hear as well." (P13)

However, although the participants had several ideas about blocking the camera, they were more skeptical about effective approaches in blocking the microphones and expressed feelings of helplessness in doing so, as highlighted in the quotes below:

> "I don't know. I was thinking maybe cover that up, but I feel like they would still be able to hear me." (P10)

> "Definitely more ideas come to mind with a camera than a microphone because I just can't really think of anything for a microphone." (P17)

These workarounds particularly highlight the need for tangible strategies to assure that sensors are not collecting data, particularly with respect to microphones. The workarounds and participants'

frustrations show how the lack of mechanisms, such as a lens cap, in today's sensors forces workarounds related to covering cameras.

Withdrawing oneself from interactions: Withdrawing is characterized as a coping behavior where an individual draws out oneself from a group physically and socially [1]. In interaction with devices, withdrawing can be represented as individuals distancing themselves from the perceived threats posed by devices. Indeed, a number of participants indicated such a strategy in dealing with devices, such as withdrawing themselves from the center of action or withdrawing the device from the room where they are present.

> "[If I don't want it to record me I would] Leave the room, probably go somewhere else." (P1)

> "So, only ways [are] to remove the camera totally, cover it up or stop doing what you're doing or go do it somewhere else. Those are only ways to be sure that the camera's not watching you." (P6)

> "I can probably take it to another room or remove it from the environment that I was in." (P12)

Although these are simple strategies they point to extreme measures because of the lack of trust and tangible ways to block collection.

Aggression toward the source of intrusion: In extreme cases, individuals might use aggressive or extreme coping mechanisms to deal with crowding in social situations and to achieve their desired level of privacy [1]. In interaction with the devices, we observed that, in most cases, participants utilized coping mechanisms that are more defensive in nature; however, if they found those mechanisms insufficient in achieving their desired privacy, they also considered more extreme approaches, such as turning off a device completely or even destroying a device.

> "I will switch off everything. My device, internet, everything else that you can turn off, I'd unplug and switch it off because I don't want it to be on. If I'm at my friends house I would ask my friends to turn it off." (P4)

> "Just one way you could make sure that it's not recording is destroying it. That's definitely one way." (P2)

> "I mean, if it's still collecting audio. It's just concerning. So I don't know what you would do to that. I guess I could break it. Just hit it a couple of times with a baseball bat." (P11)

> "Like the device has value, but if worst came to worst and I'd need no one to hear what I was saying I'd just break it." (P13)

These coping mechanisms point to the degree to which uncertainty about device operation can push people to extremes. Albeit humorous, these quotes suggest closer attention to designs that can assure people of their privacy instead of them having to destroy the device 'just to be sure'.

In summary, we observed that the coping mechanisms described by Altman in the context of interpersonal social interactions also manifest in the context of interaction with IoT devices. In many cases, the coping behaviors point to the need for sensor designs that provide clear and unambiguous information about the state of the device. The coping mechanisms also highlight the need to empower bystanders' interactions with these devices, both in terms of awareness of devices' states as well as a sense of control over the functionality of the devices. Participants' workarounds – often tangible in nature – further support the need for designs that support 'tangible privacy'.

6 DESIGN IMPLICATIONS: DESIGNING FOR TANGIBLE PRIVACY

Our findings point to a number of practical design considerations for future iterations of IoT devices to complement security best practices [38]. We start by defining 'tangible privacy' followed by several design implications.

6.1 Defining 'Tangible Privacy'

Our findings highlight the importance of a design approach to support more comprehensive assessment of peoples' privacy in the context of IoT devices. To this end, *we define 'tangible privacy' mechanisms as those privacy control and feedback mechanisms that are 'tangible', i.e., manipulated or perceived by touch, and of 'high assurance', i.e., they provide clear confidence and certainty of privacy to observers.* This concept of 'tangible privacy' builds upon the well-established concept of 'tangible' user interfaces, which support interaction with the digital world through physical affordances [64] and the need for feedback to understand system operation [26, 65] as further discussed in Section 7.1. More recently, Angelini et al. proposed a framework for building an "Internet of Tangible Things (IoTT)" [2]; their focus, however, is not on privacy, and our proposed concept of tangible privacy fills an important gap in designing for privacy. We posit that tangible privacy designs can provide the missing certainty in regulating privacy with such devices, a mode of interaction people are accustomed to when regulating their personal boundaries in inter-personal interactions.

6.2 Toward tangible designs for assured privacy

In designing for 'tangible privacy', each sensor must have:

- tangible affordances to allow people to unambiguously control the sensor's data collection.
- high assurance feedback mechanisms that provide a clear and definite sense of awareness of what data is being collected to people in the sensor's vicinity.

We now expand on key design insights that emerged from our interviews.

Clear and unambiguous feedback. In response to our findings about participants' uncertainty about device states (Section 4.1), we posit that as a general design principle, devices must strive to provide *clear and unambiguous* feedback. Although it has been recognized that feedback should be 'clear' and easy to understand for effective privacy management [5], such feedback may not reflect the reality of what is being sensed (as discussed for LEDs next). Our participants expressed a general *disbelief* toward software-controlled indicators and mechanisms, arguing that there is a high probability of software being compromised and used surreptitiously for monitoring people even when feedback was provided. Instead, they sought less or unambiguous mechanisms such as lens caps to cover the camera. These mechanisms provided a stronger assurance of privacy beyond simply being easy to interpret. It is also worth reiterating that not all tangible affordances (e.g., physical buttons) convey unambiguous feedback, and designers need to focus on tangible affordances that also *assure* bystanders of their privacy.

Reliable 'off' buttons. Many of our participants indicated (Section 4.4) that knowing a device can be physically turned off gives them a sense of control and a better sense of privacy. In the past, many digital devices featured a physical and intuitive on/off switch. Modern designs, however, have been eschewing physical buttons for 'simpler' designs with fewer physical buttons that have multiple assigned functions. For example, turning a modern smartphone 'off' can require a multipurpose button to be held continuously for a few seconds. In general, the lack of clear and trustworthy 'off' buttons, where one is assured the power is indeed cut off, has a negative effect on people's sense of privacy. Of the two devices used in our interviews, the Nest camera did not have a physical off button. Throughout our interviews, participants were looking for an off button on

the device, and the absence of this button forced them to unplug the device from the power source when they wanted to completely turn off the device.

Based on our findings, we therefore advocate a return to the practice of including a physical and reliable off button to provide stronger privacy assurances to users. We note that there might be multiple ways to 'assure' bystanders that power is cut off by such a button. These might range from a physically visible break in a connection or an internal hardware design that ensures the breaking of a circuit. Such features may be communicated in various ways to users, but it is important for such a switch to *not* be software controlled to provide strong assurances to users as many of our participants declared a lack of trust in software controlled mechanisms.

Clarity on 'on/stand-by/off' states. Related to the previous design principle, the responses of our participants demonstrated confusion about the devices' operational status (Section 4.1). Participants demonstrated different interpretations of what it means for a device to be 'off', ranging from 'sleep', 'stand-by', or 'a complete shut off' state. Current devices make it difficult to ascertain whether a device is in an 'off' or some intermediate state still capable of 'seeing' or 'listening'. From a bystander's point of view, this lack of certainty and trust about the sensors can lead to confusion about how and when to manage one's privacy as was evident in responses from our participants. Thus we posit that a device must have a clear and tangible way of declaring whether it is in a stand-by or off state. Some of our participants made use of tactile feedback, such as touching the device, to see if the device was warm to make sense of whether the device was off or in stand-by. Based on such responses, one design approach could be a periodic vibration of the device or a periodic motion of a physical artifact whenever the device is in a stand-by state to remind the people around that it is not off. One approach may be to use LED-based communication mechanisms that are hardwired and not disabled through software. Unfortunately recent work has shown we cannot take such assurances for granted [7], and firmware-based attacks can be a threat against 'hardware'-controlled LEDs.

LEDs necessary but not sufficient. Recent attempts have been made to design effective feedback mechanisms for IoT devices that are more physical in nature.[13] However, these attempts are focused on providing people with visual LED-based feedback to indicate when the device's sensors are actively recording data. LEDs have served as a tangible notion for a device's state for years now. We posit that LEDs alone cannot provide users with tangible privacy as we have seen in our findings that LEDs can be misleading at times. LEDs, when 'on' convey useful information that the camera or microphone is indeed recording. Thus, these are necessary indicators for IoT devices with cameras and microphones. But as we have argued, they may not be sufficient for communicating 'off' states. Furthermore, even if they are trustworthy, they *may not be noticed* by users [46]. For bystanders, as evident from the responses of our participants, the situation is even worse (Section 4.2). They reported when in the vicinity of a smart device owned by others, even if that device is using LEDs to communicate its state, as bystanders they typically do not know how to correctly interpret the LEDs. Participants during our interviews demonstrated this state of confusion about the meaning of the LEDs displayed in Nest Cam and Echo Show. We advocate that bystanders may need a more tangible mechanism, such as opaque covers or physical disconnects, to be assured recording is not possible at certain times. Beyond 'tangibility', future interfaces could also explore making stronger emotional or "visceral" connections as has been suggested in the context of data privacy [60], as a possible way for further assuring users about the device's state.

Clearly declaring types of sensors in the device. IoT devices are increasingly adopting multiple sensors into their designs. Sometimes these sensors might catch consumers by surprise; for example, Google's Nest Secure home-security hub was found to include a microphone that

[13] http://www.signifiers.io/

was previously unadvertised.[14] As we have found in our interviews, participants' privacy attitudes revolved around the *primary* sensor's data collection, and they tended to overlook the presence of other sensors on the device (Sections 4.3 and 4.5). Moreover, participants were uncertain about the presence and location of sensors on the devices. Most participants *assumed* that the Nest Cam had a microphone installed, but they could not locate it. Sometimes a device might contain sensors that are totally unrelated to the device's functionality (Google's Nest Protect is a smoke detector that also has an internal microphone.[15]). Yao et al. also sought for device transparency where, in a smart home application context, either the owner or the manufacturers need to provide information about the device to bystanders [69]. As suggested by our participants, we propose that instead of relying on the owners, the design of IoT devices should ensure that all sensors are visible to bystanders. These designs should not assume that educating the owner is sufficient (e.g., through stickers in the 'unboxing' process); designs should intuitively convey to bystanders that they are capable of being recorded through video and/or audio.

Shutter mechanisms for cameras. One of the most common responses of our participants talking about regulating their privacy in the vicinity of a camera was obscuring the camera's view; almost all of them talked about blocking the view with objects such as a towel or a piece of clothing (Section 5, 'blocking of stimulus'). Based on these findings, we recommend the incorporation of shutter mechanisms in camera-based devices. One consideration with shutters is whether these can be actuated electronically (e.g., via an associated smartphone app or by the device itself). If this is possible, then users may still have concerns about being recorded surreptitiously, as the device could temporarily open the shutter. For strong assurances, these shutters should be controllable only manually. One option could be to create designs that allow for electronic actuation for *closing* the shutter but require manually opening the shutter as needed.

Another tangible design suggestion that emerged from our interviews could be the use of a camera mount that can easily rotate on its axis. Bystanders can ask the owner or, when applicable, can rotate the camera lens by themselves towards the wall.

Disabling mechanisms for microphones. With the prevalence of 'always-on' IoT devices, microphones are considered to be one of the most privacy-invasive sensors [8, 42]. Our study shows that even when participants were concerned about microphones, they did not always feel they were provided with solutions to address their concerns, even if as a workaround (Section 4.2). For example, they could easily cover the camera to block visual recording but were less clear on how to block a microphone. This paves the way for future research on the design of microphones that are easy to be disabled and enabled in a way that is tangible to users. The current tangible practice is the use of a 'Mute' button but consistent with our findings, Lau et al. [32] found that users preferred unplugging the Amazon Echo compared to muting it. As argued before, to increase people's trust in the mechanism, it is important that the mute button is not just a software control but rather a hardware switch that can physically disable or disconnect the microphone's circuit.

Analogous to obscuring camera lenses, jamming mechanisms for disabling a microphone [12] can be effective at blocking the microphone temporarily; nevertheless, the concern about assured feedback (a part of 'tangible privacy') remains. Because ultrasound (naturally) does not provide any audible feedback, there is no way for a bystander to know whether the jamming mechanism is actually on. This, again, indicates the need for future research investigating how to incorporate tangible privacy mechanisms for embedded microphones.

[14] https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy

[15] https://store.google.com/product/nest_protect_2nd_gen_specs

Using detachable sensors. One possibility is for future IoT platforms to follow a modular approach in which each sensor can individually – and tangibly – be enabled or disabled. For example, in the case of Echo Show, our participants deemed that using the camera sensor is not the primary objective of that device and wanted to selectively turn off the camera and continue using the microphone. Using a modular approach would allow a user to selectively carry out preferred sensing without having to shut down or unplug the device as a whole. Seyed et al. [56] designed a modular smart phone and showed how people can lend different parts of a modular phone to others making temporary device lending more trustworthy and convenient. Some commercial smart phones use modularity to enhance device capabilities.[16,17] We posit that, given the availability of proper detachable sensors, following a modular design approach for IoT devices can more effectively ensure better privacy management in a truly tangible manner. In cases where bystanders may not have the ability to perform such 'detachments', they are still provided with tangible assurances when performed by the owner.

7 DISCUSSION

In this section we discuss a) why 'tangible privacy' is an important consideration in the design of sensors, b) theoretical implications for exploration in future work, and c) a discussion of how bystanders might navigate social norms with tangible designs.

7.1 The Importance of Tangible Design for Privacy

Our proposed concept of 'tangible privacy' is complementary to an array of solutions to control data collection and dissemination. Although other solutions can provide other forms of security 'guarantees' (e.g., validated software), our goal is to go further and provide users with an *assured* sense of privacy (versus a 'false sense of security') by leveraging the physicality of the devices.

During our interviews, participants showed a clear preference toward privacy *control* mechanisms that can be manipulated physically. This unification of action and perception, which was sought out by our participants is an important theme in tangible interaction. Users must be able to perceive their action and the system's output simultaneously. In other words, 'tangibility' offers a seamless integration of representation and control which means the user can read the system state from the manipulated object [65]. Participants also expressed the importance of meaningful *feedback* from the devices. Tangible interaction systems can successfully raise awareness [52, 73], improve 'legibility' (the understanding of the system's states) [64], and convey meaningful information about the control and representation of data by making the information representation immediately available to the users [65]. Another reason for using tangibility is the *tactile* feedback that a user can receive by using tangible mechanisms. Tactile feedback is perceived by the sensation of touch and has been found to have several benefits through improved decision making [44], confidence in evaluating functionality [43], and enhanced task performance when interacting with devices [54]. Indeed, lacking tactile and tangible controls our participants showed a general lack of confidence while evaluating whether a device was 'on' or 'off' for example.

In sum, tangible design provides an immediate confirmation about an individual's actions. More importantly, it encompasses the feeling of 'sureness' by leveraging the richness of human senses, developed by interacting with physical objects on a daily basis. These properties are crucial when it comes to regulating one's privacy in the current socio-technical space.

[16] https://www.theverge.com/2016/7/21/12244300/motorola-moto-z-review-droid-moto-mod
[17] https://www.engadget.com/2016/02/21/lg-g5-modular-official/

7.2 Theoretical connections and implications

Our findings lined up closely with many aspects of Altman's theory of boundary regulation. At the same time, privacy concerns stemming from such devices relate to deviations from 'entrenched norms' of how information is collected or disseminated as described by Nissenbaum's theory of contextual integrity.

Although several aspects of our findings (such as participants' coping mechanisms) lined up well with Altman's theory, we did not set out to confirm or extend the theory. For example, we did not explicitly ask participants about their emotional state and did not confirm whether they felt 'social isolation' from certain privacy-enhancing behaviors. At the same time we did find indirect evidence of such a sense of 'isolation', where participants talked about isolating themselves from the physical space when left with no other choices or the use of tangible workarounds (such as covering a camera) to avoid isolation. Applying Altman's framework to our analysis shows that despite the lack of stronger assurances, people apply a similar set of boundary regulation mechanisms both in the context of human-human and human-IoT interactions resulting in an ambiguous sense of privacy or the use of tangible workarounds. Such feelings of ambiguity and behaviors highlight the discrepancy between one's 'perceived' and 'actual' privacy and the desire to resolve ambiguity, which is not explicitly differentiated in Altman's model. Although this discrepancy makes salient why tangible privacy mechanisms are desirable, further work is needed to understand how Altman's model for interpersonal boundary regulation can be updated to include components of 'perceived' vs. 'actual' privacy and how they interact with more nuanced boundary regulation. We leave this exploration for future work.

Connecting with Nissenbaum's theory of contextual integrity, we found that our participants' perceptions were guided by norms based on their conception of a device's *primary* function. Although the Nest Cam has an embedded microphone, participants were not concerned about the device secretly listening to them because, according to them, the device's primary function is to 'watch'. Similarly, despite having a built-in camera, participants were less concerned about the Echo Show as they see it as a device whose primary function was not to watch but rather to 'listen' for user commands. Our results provide evidence on how contextual integrity can play a part in shaping participants' privacy perceptions about the devices: where privacy violations in the context of interactions with such devices can occur, and when the collection of personal information can take place in ways that defy user expectations (e.g., Nest Cam collecting audio). We argue that incorporating tangible feedback into design of devices can help users to better assess the contextual factors, thus forming better contextual norms and better privacy expectations about IoT devices.

7.3 Social Norms and Tangible Privacy

Social norms guide behaviors in general [9, 39] and should be considered when designing mechanisms to shape interactions for managing privacy. Some of our suggestions for tangible designs may appear to conflict with prevailing social norms about who should control devices, e.g., whether it is appropriate for bystanders to 'disable' IoT devices owned by others. However, when our participants were asked about their privacy-enhancing behaviors, depending on the context, we recorded a variety of responses that were mindful of prevailing social norms. Participants' responses largely showed that they respected their interpersonal relationships with owners. For example, in the context of on/off buttons, they said that they would ask the owner to turn off the device using the off button instead of turning off the device themselves. Participant P2 said, "If it was my friends' house, I'd ask them to have some confidential conversation. For example, I'd ask them if they would turn the camera off." Moreover, when the owner is not known to them, for example in the case of a rented Airbnb, participants said they would contact the owner, ask them about the purpose of

using such devices, and ask their permission to turn the devices off. They considered turning the devices off by themselves as a socially awkward behavior but still wanted the assurance of an off button when the devices was permitted to be off.

In specific cases, however, participants were willing to override owners' intentions or violate social norms. For example, in situations where the owner of an Airbnb rental cannot be reached and the devices are placed in sensitive places (e.g., a bedroom or bathroom), participants said that they would turn the devices off by themselves to protect their privacy. Underscoring the need for tangible privacy mechanisms beyond software controls [35], participants were even willing to break or destroy devices in cases when they felt helpless; for example, when the devices do not provide any options of turning them off manually. We take these responses as evidence that bystanders, too, have expectations of what is appropriate in terms of how and when information about them is collected by owners.

While proposing suggestions for the design of tangible privacy mechanisms, one must consider the needs of both owners as well as bystanders. Based on our findings, the inclusion of 'turn off' and/or 'blocking' techniques, such as the incorporation of off buttons and the inclusion of shutter mechanisms, in devices strike this balance of allowing control by owners and providing tangible assurances to bystanders. In general, our participants showed a tendency of following the established social norms while regulating their privacy as bystanders when the devices were equipped with options to either turn them off or block collection. These responses form the basis of our proposal of designing devices with tangible privacy mechanisms, which would help bystanders regulate their privacy while maintaining social norms. Even though it might seem counter intuitive to provide an off mode for devices that are 'always-on' by nature, it was evident from our interviews that this 'always-on' nature generated several privacy concerns among participants who may not find the always-on feature desirable and would like to ensure these devices can indeed be turned 'off' at times. Indeed, some IoT devices, such as Amazon Echo Show and Google Nest Hub Max, have recently taken a step in that direction and have incorporated a physical mute button as well as an 'off' button into their designs, allowing any users in the vicinity to turn off the microphone or the device itself. However, more work is needed to make these designs convenient to use and to provide adequate assurances to users as to whether the microphone/camera or the device is, indeed, off.

8 CONCLUSIONS

Based on our study of how people manage their privacy around IoT devices, we identify and introduce the concept of 'tangible privacy' as an important consideration in the design of IoT devices. Tangible privacy mechanisms provide people with a way to clearly and unambiguously control and discern privacy states of IoT devices in their vicinity. Current designs do not provide adequate assurances to bystanders, who are unable to clearly ascertain whether they are being recorded by a camera or microphone. Through our interview study, we find that current designs lead to an uncertainty about device states (e.g., whether they are indeed 'on' or 'off' or in some intermediate 'stand-by' state and able to record data) and confusion about features such as what LEDs mean. This uncertainty, along with the mistrust of software controls, also lead people to improvise their own privacy mechanisms such as covering cameras with other objects and even attempting to muffle microphones. We also found that people can underestimate their privacy risks by overly focusing on the primary function of the device and sometimes not being aware of microphones on video-focused IoT devices and vice versa.

A major contribution of our work is the call for adopting hardware mechanisms in an attempt to provide bystanders with the required assurance of their privacy. Our findings inspire various design principles for the design of future IoT devices. Designers should strive to design mechanisms that

provide clear and unambiguous feedback through 'tangible privacy' mechanisms. Their devices should convey clarity on their 'on'/'off' states, and designers should recognize the limitations of LEDs (they should be seen as necessary but not sufficient). Cameras should support shutter mechanisms for obscuring the camera, and microphones, in particular, need special attention because their current embedded designs do not seem to offer any easy ways of being obscured. Future microphones need to be designed so that they can be easily – and tangibly – disabled on devices. Future, novel designs could consider modular designs where sensors can be easily removed or reattached based on people's privacy preferences. Finally, IoT devices should support a negotiation of privacy between people in the vicinity. Although much work has studied such privacy negotiation, more research is needed on how devices can be reconfigured for tangibility. Overall, we hope that our work inspires future research on designs for 'tangible privacy', which we posit is a necessary component for managing privacy in today's socio-technical physical spaces.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under grants CNS-1252697, CNS-1814513, and CNS-1814866. We would also like to thank Yasmeen Rashidi for her guidance.

REFERENCES

[1] Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Pub. Co.

[2] Leonardo Angelini, Elena Mugellini, Omar Abou Khaled, and Nadine Couture. 2018. Internet of Tangible Things (IoTT): Challenges and Opportunities for Tangible Interaction with IoT. *Informatics* 5, 7 (2018).

[3] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. 2015. Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems* 1, 2 (2015), 99–109.

[4] David Armstrong, Ann Gosling, John Weinman, and Theresa Marteau. 1997. The Place of Inter-Rater Reliability in Qualitative Research: An Empirical Study. *Sociology* 31, 3 (1997), 597–606.

[5] Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93.* Springer, 77–92.

[6] Lucia Benaquisto and L Given. 2008. The SAGE encyclopedia of qualitative research methods. *New York: Sage* (2008).

[7] Matthew Brocker and Stephen Checkoway. 2014. iSeeYou: Disabling the MacBook Webcam Indicator LED. In *23rd USENIX Security Symposium (USENIX Security 14).* San Diego, CA, 337–352.

[8] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC).* IEEE, 172–175.

[9] Gary Burnett and Laurie Bonnici. 2003. Beyond the FAQ: Explicit and implicit norms in Usenet newsgroups. *Library & Information Science Research* 25, 3 (2003), 333–351.

[10] Kelly E. Caine, Celine Y. Zimmerman, Zachary Schall-Zimmerman, William R. Hazlewood, Alexander C. Sulgrove, L. Jean Camp, Katherine H. Connelly, Lesa L. Huber, and Kalpana Shankar. 2010. DigiSwitch: Design and Evaluation of a Device for Older Adults to Preserve Privacy While Monitoring Health at Home. In *Proceedings of the 1st ACM International Health Informatics Symposium* (Arlington, Virginia, USA) *(IHI '10).* ACM, New York, NY, USA, 153–162.

[11] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens, and Volker Wulf. 2017. What Happened in My Home?: An End-User Development Approach for Smart Home Data Visualization. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17).* ACM, New York, NY, USA, 853–866.

[12] Varun Chandrasekaran, Kassem Fawaz, Bilge Mutlu, and Suman Banerjee. 2018. Characterizing Privacy Perceptions of Voice Assistants: A Technology Probe Study. *ArXiv* abs/1812.00263 (2018).

[13] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M Jose. 2016. Bystander privacy in lifelogging. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Companion Volume.* BCS Learning & Development Ltd., 15.

[14] Yaliang Chuang, Lin-Lin Chen, and Yoga Liu. 2018. Design Vocabulary for Human-IoT Systems Communication. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18).* ACM, New York, NY, USA, Article 274, 11 pages.

[15] Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. 2016. Privacy mediators: Helping IoT cross the chasm. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. ACM, 39–44.

[16] Eva Deckers, Stephan Wensveen, Pierre Levy, and Rene Ahn. 2013. Designing for perceptual crossing: Designing and comparing three behaviors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1901–1910.

[17] 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* (Toronto, Ontario, Canada) *(CHI '14)*. ACM, New York, NY, USA, 2377–2386.

[18] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. 2013. Computer security and the modern home. *Commun. ACM* 56, 1 (2013), 94–103.

[19] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno. 2009. A spotlight on security and privacy risks with future household robots: attacks and lessons. In *Proceedings of the 11th international conference on Ubiquitous computing*. ACM, 105–114.

[20] Emily Dixon. 2019. Family finds hidden camera livestreaming from their Airbnb in Ireland. https://www.cnn.com/2019/04/05/europe/ireland-airbnb-hidden-camera-scli-intl/index.html.

[21] 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 *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[22] Batya Friedman, Peter H. Kahn, Jr., Jennifer Hagman, Rachel L. Severson, and Brian Gill. 2008. The Watcher and the Watched: Social Judgments About Privacy in a Public Place. *Hum.-Comput. Interact.* 21, 2 (May 2008), 235–272.

[23] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2018. Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats. In *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP), Baltimore, MD, August 12, 2018*. USENIX, Berkeley, CA.

[24] Stacy Gray. 2016. Always on: privacy implications of microphone-enabled devices. In *Future of privacy forum*.

[25] Chris Harrison, John Horstman, Gary Hsieh, and Scott Hudson. 2012. Unlocking the expressivity of point lights. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1683–1692.

[26] Eva Hornecker and Jacob Buur. 2006. Getting a grip on tangible interaction: a framework on physical space and social interaction. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 437–446.

[27] 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*. 571–582.

[28] Intel. 2014. Intel IoT Gateway. https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/gateway-solutions-iot-brief.pdf.

[29] Judy Kendall. 1999. Axial coding and the grounded theory controversy. *Western journal of nursing research* 21, 6 (1999), 743–757.

[30] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights-Design Requirements of Privacy Notices for Body-worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*. ACM, 177–187.

[31] Karen L Courtney, George Demiris, Marilyn Rantz, and Marjorie Skubic. 2008. Needing smart home technologies: The perspectives of older adults in continuing care retirement communities. *Intformatics in primary care* 16 (02 2008), 195–201.

[32] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 102.

[33] Adam J. Lee, Rosta Farzan, Apu Kapadia, and Imtiaz Ahmad. 2020. Making sense of risk in an increasingly cyber-physical world. *Critical Quarterly* 62, 1 (2020), 40–48.

[34] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250 – 271.

[35] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458.

[36] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages.

[37] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human*

Factors in Computing Systems. ACM, 5197–5207.
[38] B. Momenzadeh, H. Dougherty, M. Remmel, S. Myers, and L. J. Camp. 2020. Best Practices Would Make Things Better in the IoT. *IEEE Security & Privacy* 18, 4 (2020), 38–47.
[39] David M Newman. 2020. *Sociology: Exploring the architecture of everyday life*. SAGE Publications, Incorporated.
[40] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
[41] Don Norman. 2014. *Turn signals are the facial expressions of automobiles*. Diversion Books.
[42] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term Effects of Ubiquitous Surveillance in the Home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. ACM, New York, NY, USA, 41–50.
[43] Joann Peck and Terry L Childers. 2003. To have and to hold: The influence of haptic information on product judgments. *Journal of Marketing* 67, 2 (2003), 35–48.
[44] Joann Peck and Jennifer Wiggins Johnson. 2011. Autotelic need for touch, haptics, and persuasion: The role of involvement. *Psychology & Marketing* 28, 3 (2011), 222–239.
[45] James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, Article 45, 14 pages.
[46] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. ACM, New York, NY, USA, 1649–1658.
[47] 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 *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS '18)*. 143–157.
[48] Joel R Reidenberg. 2014. Privacy in public. *U. Miami L. Rev.* 69 (2014), 141.
[49] Tom A Rodden, Joel E Fischer, Nadia Pantidi, Khaled Bachour, and Stuart Moran. 2013. At home with agents: exploring attitudes towards future smart energy infrastructures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1173–1182.
[50] Rodrigo Roman, Jianying Zhou, and Javier Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57, 10 (2013), 2266–2279.
[51] Gilad Rosner and Erin Kenneally. 2018. Clearly Opaque: Privacy Risks of the Internet of Things. In *Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum*.
[52] Mike Scaife and Yvonne Rogers. 1996. External cognition: how do graphical representations work? *International journal of human-computer studies* 45, 2 (1996), 185–213.
[53] Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang. 2011. Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*. 17–33.
[54] Bertrand Schneider, Patrick Jermann, Guillaume Zufferey, and Pierre Dillenbourg. 2010. Benefits of a tangible interface for collaborative learning and interaction. *IEEE Transactions on Learning Technologies* 4, 3 (2010), 222–232.
[55] Irving Seidman. 2006. *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. Teachers college press.
[56] Teddy Seyed, Xing-Dong Yang, and Daniel Vogel. 2017. A Modular Smartphone for Lending. In *Proceedings of the 30th Annual ACM Symposium on User Interface Software and Technology (UIST '17)*. ACM, New York, NY, USA, 205–215.
[57] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks* 76 (2015), 146–164.
[58] Deepika Singh, Ismini Psychoula, Johannes Kropf, Sten Hanke, and Andreas Holzinger. 2018. Users' Perceptions and Attitudes Towards Smart Home Technologies. In *International Conference on Smart Homes and Health Telematics*. Springer, 203–214.
[59] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.
[60] Luke Stark. 2016. The emotional context of information privacy. *The Information Society* 32, 1 (2016), 14–27.
[61] Joshua Streiff, Olivia Kenny, Sanchari Das, Andrew Leeth, and L Jean Camp. 2018. Who's Watching Your Child? Exploring Home Security Risks with Smart Toy Bears. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 285–286.
[62] Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé. 2010. Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision* 3, 3 (2010), 34–36.

[63] Robert Templeman, Zahid Rahman, David Crandall, and Apu Kapadia. 2013. PlaceRaider: Virtual Theft in Physical Spaces with Smartphones. In *Proceedings of The 20th Annual Network and Distributed System Security Symposium (NDSS)*.
[64] Brygg Ullmer and Hiroshi Ishii. 2000. Emerging frameworks for tangible user interfaces. *IBM systems journal* 39, 3.4 (2000), 915–931.
[65] Elise Van Den Hoven, Evelien Van De Garde-Perik, Serge Offermans, Koen Van Boerdonk, and Kars-Michiel H Lenssen. 2013. Moving Tangible Interaction Systems to the Next Level. *IEEE Computer* 46, 8 (2013), 70–76.
[66] 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.
[67] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2016. The perfect storm: The privacy paradox and the Internet-of-Things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 644–652.
[68] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 198.
[69] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 59 (Nov. 2019), 24 pages.
[70] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. ACM, New York, NY, USA, 6777–6788.
[71] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80.
[72] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (Nov. 2018), 20 pages.
[73] Oren Zuckerman. 2015. Objects for change: A case study of a tangible user interface for behavior change. In *Proceedings of the Ninth International Conference on Tangible, Embedded, and Embodied Interaction*. 649–654.

A APPENDIX - INTERVIEW PROTOCOL

Assessing people's perception of smart devices.

Q1. How would you describe the word 'ON' for this device?
Q2. How would you turn this device ON?
Q2a. What made you think you could turn the device ON in this way?
Q3. When this device is ON, how do you know if it's actually ON?
Q4. When ON, what do you think the device is doing?
Q4a. What made you think that the device is doing this?
Q5. How would you describe the word 'OFF' for this device?
Q6. How would you turn this device OFF?
Q6a. What made you think you could turn the device OFF in this way?
Q7. When this device is OFF, how do you know if it's actually OFF?
Q8. When OFF, what do you think the device is doing?
Q8a. What made you think that the device is doing this?

Understanding people's concerns and their privacy enhancing behaviors.

Q9. Name some places in a house where you would be comfortable with the presence of this device.
Q10. What are the reasons people would have this device in these places for?
Q11. Name some places in a house where you would not be comfortable with the presence of this device.
Q12. What are the reasons that would make you feel uncomfortable?
Q13. We followed up device-specific questions with three different scenario-based questions for a more objective assessment of participants' behavior in relation to sensor-rich devices. All three scenarios were presented to all participants.

Example scenario 1: Suppose you have gone to visit your friend's house and decide to spend the night over there. You found out a device like this in the bedroom which is ON. How would you feel about that?
Example scenario 2: Suppose you have gone to visit your doctor. In the examination room you see a device like this. How would you feel about the presence of this device?
Example scenario 3: Suppose you have rented a house on Airbnb. You found out a device like this in the bedroom which is ON. How would you feel about that?
Q14. Based on the responses of Q4, Q12 and scenario-based questions, we then asked the participants

- In each of these situations, if you are concerned about being recorded/watched by the device, what would you do to deal with the devices in ways to make you feel more comfortable?
- If you are allowed to equip the device with (i) hardware based affordances or mechanisms (such as a mute button, lens shutters) and/or (ii) software based affordances or mechanisms (such as controlling the mobile apps) for better assurance of its states and functions, which type of affordance would you prefer?
- What are the reasons for choosing such affordance?

Received January 2020; revised June 2020; accepted July 2020