Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies

Eun Kyoung Choe[1], Sunny Consolvo[1], Jaeyeon Jung[2] , Beverly Harrison[1], Shwetak N. Patel[1], Julie A. Kientz[1]

[1]University of Washington
{eunky, shwetak, jkientz}@uw.edu,
sunny@consolvo.org, beverly_harrison@yahoo.com

[2]Microsoft Research
jjung@microsoft.com

ABSTRACT

In-home sensing and inference systems impose privacy risks and social tensions, which can be substantial barriers for the wide adoption of these systems. To understand what might affect people's perceptions and acceptance of in-home sensing and inference systems, we conducted an empirical study with 22 participants from 11 households. The study included in-lab activities, four weeks using sensor proxies in situ, and exit interviews. We report on participants' perceived benefits and concerns of in-home sensing applications and the observed changes of their perceptions throughout the study. We also report on tensions amongst stakeholders around the adoption and use of such systems. We conclude with a discussion on how the ubicomp design space might be sensitized to people's perceived concerns and tensions regarding sensing and inference in the home.

Author Keywords

Privacy, sensing, inference, video camera, microphone, energy monitoring, accelerometer, interview, diary study, cultural probes, qualitative methods, domestic computing.

ACM Classification Keywords

D2.2 Design Tools and Techniques: User Interfaces; K.4.2 Computers and Society: Social Issues.

General Terms

Human Factors, Design

INTRODUCTION

Recent technical advances are accelerating the integration of sensors into consumer devices in the home. Microsoft's Kinect gaming accessory provides full-body 3D motion capture, facial recognition, and voice recognition capabilities [32]. This allows people to play games through gestures and voice. Energy sensing systems such as ElectriSense [9] and HydroSense [6] can provide device-level usage feedback. People can benefit from the sensor data in many ways—for example, to figure out whether hand washing or using a dishwasher is more energy efficient. Microphones, cameras, and wearable RFID have been embedded into home security systems and at eldercare facilities with the intention of more secure and safer living environments.

Despite the great advantages that sensor-rich environments and smart devices can offer, new challenges abound. Sensing and inference data captured in the home could be highly sensitive. A recent study [4] of activities that people do in the home that they would not want recorded included not only intimacy and secretive activities (e.g., confidential conversations) but also seemingly innocuous activities such as cooking and eating, depending on the context. In addition, in-home sensing and inference data may inevitably contain information about multiple stakeholders who may have different perspectives on what is acceptable and useful. This difference in perspectives may cause tensions among stakeholders—both householders and visitors—around the use of sensing and inference systems.

This study investigates householders' receptiveness to various sensing technologies in the home. A challenge we encountered in designing this early-stage investigation was that the general population is often not very familiar with how sensing technologies work and what might be logged. The risks and social ramifications of research prototypes and actual monitoring or recording technologies are unknown; they may capture sensitive data that participants would not realize. To address this challenge, we employed in-lab activities and in-home cultural probes using *sensor proxies* to situate participants in a context where they were encouraged to think through costs and benefits of various sensing and inference systems. In this way, we were able to collect contextualized feedback *without* deploying actual sensing devices that were potentially invasive.

Our research makes three contributions. First, we discuss technical and social issues that could impact people's perceived benefits and concerns of in-home sensing systems based on a contextually situated understanding. Second, we detail a method of investigating the acceptability of sensing and inference applications that can produce contextualized feedback without the need for deploying fully functional systems. Lastly, we offer a number of design insights, which technology designers can use to reduce some concerns observed in the study. However, many issues in resolving conflicting needs and desires by multiple stake-

UbiComp' 12, Sep 5 – Sep 8, 2012, Pittsburgh, USA.

holders remain open. We identify future research efforts that may help make progress toward these issues.

RELATED WORK

Langheinrich argues that there are inherent privacy issues in ubicomp systems due to their ubiquity, invisibility, sensing, and memory amplification [20]. To address some of these concerns, Langheinrich describes the concept of "privacy borders" and argues that designers of ubicomp systems should prevent unintended personal border crossings [21]. Jacobs and Abowd offer a legal perspective on these issues [16]; they introduce an analytic framework consisting of two dimensions—1) the size of the intended audience and 2) the motivation of the reasoning process. They demonstrate how this framework can be used to analyze a case where a family has a location service installed in the home, and the system collects data from multiple stakeholders (residents and guests). These [16,20,21] and other theoretical work [13,28] can help assess privacy aspects of ubicomp systems and explore their socio-technical implications. They also attempt to increase public awareness of privacy issues in ubicomp environments and provide general guidelines to inform design. While all these authors provide insights into how ubicomp systems should be more privacy preserving, they do not come from or reflect end user perspectives. Iachello and Abowd point out that it is unclear how the design guidelines can be directly applicable in designing a privacy-observant ubicomp system due to the lack of a design process model [14].

Several recent projects have focused on designing and deploying specific recording technologies for use in particular situations. Nguyen et al. argue that people may not fully understand the benefits and threats of technologies unless situated in a specific context [27]. Hayes and Abowd investigated privacy concerns and tensions of automated capture technologies in evidence-based care situations [11]. Iachello et al. used *paratyping*, an inquiry technique for event-contingent experience sampling [15]. They studied privacy concerns in the context of a mobile memory aid, the Personal Audio Loop [10], which raises issues around obtaining informed consent from others whose data might be captured by the user's device. Massimi et al. [24] employed the *Day Reconstruction Method* (DRM) and follow-up interviews to gather grounded reactions to the recording technologies people encounter throughout the day. Their study provides insights into designing notification elements of recording systems. Klasnja et al. recruited participants with substantial experience with sensing technologies so that participants could reflect on their experiences with their own data [17]. While our study shares similar goals to the work outlined above, our study investigates sensing and inference systems *in the home*. A few previous studies have examined privacy issues of a specific monitoring system in the home. Caine et al. designed the DigiSwitch, an elder-care home monitoring system that transmits three different data types (motion, sleep, and video) to healthcare providers [3]. They argue that providing a simple control over the transmission of monitoring data helps elders maintain their privacy. Investigating the impact of data processing techniques on privacy and awareness, Neustaedter et al. found that video blurring filters are not sufficient to balance awareness and privacy in the home media space where one's privacy may be at moderate to extreme risk [26].

We explore multiple types of sensors to cover a broad range of sensing applications in the future home. We particularly examine four data types—video, audio, electricity use, and movement—each of which is captured by a camera, microphone, electricity monitor, and accelerometer. For each of these data types, we illustrate different data processing techniques ranging from raw data (e.g., raw video, raw electricity use data) to inferred data (e.g., presence information, physical activities). In designing our study, we strived to gather contextualized feedback without having to deploy actual sensing and inference systems.

STUDY METHOD

We conducted a three-phased study, which included an initial in-lab session, four weeks using sensor proxies in-situ, and exit interviews over the course of four to five weeks.

Participants

Couples living together across 11 households (10 females, 12 males, aged 28-54) participated in our study. All participants lived in the Seattle metropolitan area in the United States and were recruited by a market research agency. The participants included those who have (n = 16) and do not have child(ren) (n = 6), and those who rent (n = 8) versus own (n = 14) with an average length of stay of 7.7 years [Table 1]. The primary residence of all participants was a single family home, with two households having a home security system installed but not currently in use. Our participants had varying levels of education, ranging from high school (n = 4); some college/Bachelor's degree (n = 14); and some graduate work at Master's level/Master's degree (n = 4). All participants owned either a desktop or laptop with an average of 2.5 (Min = 1, Max = 5) computers per household. We compensated each participant with a $150 USD gift certificate. We conducted all interviews and surveys separately with each participant to uncover any conflicting views from people living in the same household.

First In-lab Session to Collect Initial Reactions

The first in-lab session consisted of a background survey and technology education session followed by a semi-structured interview. The background survey included questions about demographics, previous experience with various technologies, and privacy concern levels.

After participants completed the survey, we explained four sensing data types—video, audio, electricity use, and movement. For the *video* data type, we first played an original video clip [Figure 1, left], and then a processed version [Figure 1, right], which only contained the *depth* data of the original clip that is able to infer the number of people. Similarly, for the *audio* data type, we first played an original audio clip (i.e., raw audio) which contained a private con-

ID	Sex	Age	Occupation	Children (age)	Frequent visitors (non-household members)
H1a	F	41	Teacher	Yes	Babysitter
H1b	M	45	Tile contractor	(3, 7)	
H2a	M	31	Web team	No	Parent, relative, friend
H2b	M	43	Restaurant/dance captain		
H3a	M	47	Unemployed	No	Relative, friend
H3b	F	45	Customer service supervisor		
H4a	F	49	Homemaker	Yes	-
H4b	M	50	Manager	(15)	
H5a	F	35	Sales specialist	No	-
H5b	M	36	Server		
H6a	M	36	Director (non-profit)	Yes	Relative
H6b	F	30	Insurance agent	(6, 14, 14)	
H7a	M	28	Manager	Yes	Parent, relative, friend
H7b	F	28	Caregiver	(1, 4, 6)	
H8a	F	49	Realtor/Managing broker	Yes (18)	Adult child, parent, relative, friend, service people
H8b	M	49	Auto mechanic		
H9a	M	37	Unemployed	Yes	Adult child, relative, friend,
H9b	F	31	Bookkeeper	(9, 14)	neighbor's child, children's friends
H10a	M	51	Customer service	Yes	Adult child, parent, relative,
H10b	F	44	Owner / operator	(14, 16)	friend, wife's ex-husband
H11a	F	54	Supervisor	Yes	Adult child, parent, relative,
H11b	M	51	Iron worker	(23, 25)	friend, service people

Table 1. Demographics of the participants

versation of a couple, followed by a processed version (i.e., garbled audio) in which the details of the original conversation were difficult to understand but speakers could be distinguished. For the *electricity use* data type, we first showed a table containing raw numbers that the electricity monitor collected [Figure 2, left] and then a visualization of the raw data with the activity inference labels [Figure 2, right]. The labeled electricity monitor data showed that it could infer various activities (e.g., a washer turning on/off, a PC turning on/off). Similarly, for the *movement* data type, we showed raw accelerometer data [Figure 3, left] and then a visualization of the raw data with the activity inference labels [Figure 3, right] (e.g., vacuuming, tooth brushing).

After explaining each of the four data types and data processing techniques, we conducted semi-structured interviews, which lasted about an hour. We learned from our previous work [4] that people could only react meaningfully to questions with respect to certain positive properties that the system was supposed to have, and thus, we endeavored to find applications that might resonate with individual needs and interests. We encouraged participants to brainstorm possible application scenarios for each sensing technology and to consider the trade-offs (benefits/risks) of using sensing and inference systems in their home. When participants could not think of any, we provided them with several application scenarios and asked them what they perceived to be possible benefits and concerns of these applications. To ensure that the trade-offs were considered, if participants were too positive about the sensors or applications, we probed about potential risks (e.g., "what if a service provider has access to the data?") and vice versa. The in-lab session provided a frame of reference for the participants to understand sensor context for the rest of the study.

Figure 1. Video data types—raw (left) and depth (right)

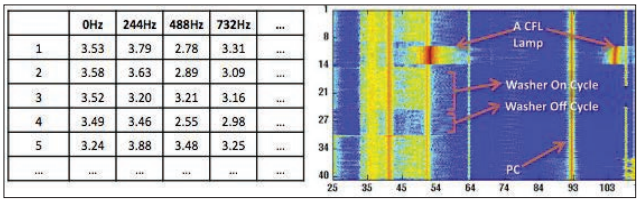

Figure 2. Electricity use data type—raw data (left) and visualization with activity inference caption (right)

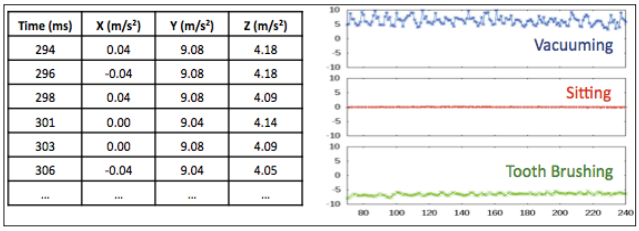

Figure 3. Movement data type—raw accelerometer data (left) and visualization with activity inference caption (right)

In-situ Phase for Collecting Contextualized Feedback

To help ground participants' responses in situated phenomena, we used the *Cultural Probes* [7] method. We provided participants with a take-home package to help them imagine living in a home with sensors that monitored their activities and surroundings. The in-situ phase lasted for four weeks and consisted of at-home activities with the cultural probe. The take-home package contained two diaries, a digital camera, a guestbook, and four "sensor proxies" [Figure 4]. The sensor proxies were off-the-shelf motion sensor lights wrapped in decorative paper, which turned on whenever motion was detected by the built-in sensor. After 30 seconds of not detecting motion, the light turned off. We gave one take-home package to each household and told participants that they were free to discuss the study with their partners, other household members, and visitors.

Participants were instructed to set up the sensor proxies in four different places in the home—kitchen, master bedroom, family room, and child's or guest bedroom/study—where the sensor proxies would be frequently triggered and visible. To assess the effectiveness of the light from the sensor proxies, we asked participants not to turn on the sensor proxies during the first week; participants turned on the sensor proxies at the beginning of the second week. We asked them to use the sensor proxies to think about the sensing and inference contexts that we talked about during the initial in-lab session. To collect contextual feedback, we asked participants to keep the diaries near the sensor proxies and jot down situations *"where sensing would have been helpful, undesirable, convenient, or inappropriate,"* and their *feelings, thoughts,* and *reactions* as they related to the

Figure 4. The take-home study package contained 4 sensor proxies (off-the-shelf motion sensor lights wrapped in decorative paper), 1 digital camera, 2 diaries, and 1 guestbook.

study. These instructions were provided as prompts in the diary. If an entry was about something that happened, we asked them to include *when* and *where* in the home it happened. Participants had an option to share the same diary with the partner. We also asked participants to take pictures of the sensor proxies to get a sense of how and where they were set up [Figure 5]. Lastly, participants kept a log of all visitors (e.g., guests and service people) in the guestbook.

It was not our intention to imitate an actual sensing environment with the sensor proxies. Rather, this was an exploratory and exaggerated way to frequently prompt participants to imagine in-situ what it might be like to have sensing and inference systems in their home. We used probes mainly as a provocative, experimental, and inspiring means of getting participants to think about sensors operating in the context of their real homes and everyday activities [2].

Exit Interview

After the 4-week in-situ phase, participants returned to our lab for a review of the sensing technologies and an exit interview. As with the initial in-lab session, the exit interviews were conducted one participant at a time. To remind participants, we played the same video and audio clips from the first session and showed a printout of the electricity use and accelerometer data. We asked participants about their perceptions toward different data types and data processing techniques, utility of the potential applications, and issues regarding data access, retention, and notification methods.

Analysis

Our study produced a rich dataset. We audio-recorded and transcribed all initial and exit interviews (34 hours of recordings). Participants completed a total of 79 diary entries (7.2 entries per household), which we digitized. All participants submitted the photographs of each sensor proxy to show how and where they were placed [Figure 5]. We employed cross-case analysis of the 44 interview transcripts and diary entries using a grounded theory approach [8]. During the interpretation phase, we took multiple passes of half of the data, thereby creating a codebook which contained high-level themes centered on: application scenarios, benefits, risks, and concerns of using sensing and inference in the home, device control, data ownership, data access, data retention, data sharing, notification method, technology adoption decision, and tensions among the stakeholders. The research team held several meetings to iterate on and refine the themes and corroborate findings. Then, the first author read through the rest of the data and tagged instances that dealt with the identified themes. We kept a record of which participant responses stemmed from which phase of the study, thereby disclosing the role and effect of the in-situ extended probe phase. This approach also helped us identify conflicting perspectives between couples, which allowed us to observe the tensions between householders. We also looked for any participants' change of opinions throughout the study period and strengths and limitations of our study methodology.

IN-HOME SENSING: PERCEIVED BENEFITS AND RISKS

As expected, the application, more than the sensor itself, became a determinant when participants assessed costs and benefits of sensing systems. For example, householders may find it acceptable to use a video camera in their living room for a video game system, but not for a home security system even though it may use the same type of video camera. In what follows, we detail what participants perceived as benefits and motivators as well as risks and concerns of using in-home sensing. Oftentimes, participants' perceptions shifted dramatically according to different applications and contexts. We describe how their perceptions evolved throughout the study by indicating from which phase the results were derived; however, we observed different patterns for each individual, and thus we do not intend to generalize results to an entire population.

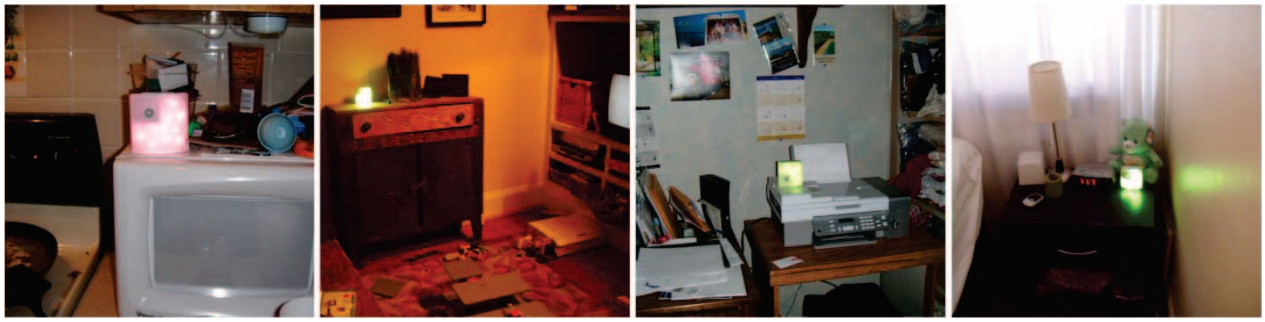

Figure 5. Setup of the sensor proxies—(from left to right) kitchen [H7], living room [H1], study [H11], and bedroom [H2]

Perceived Benefits of In-Home Sensing Applications

People may be willing to accept invasive technologies if perceived benefits outweigh potential risks [19]. Our data revealed a number of instances where participants thought of benefits and motivators for using in-home sensing and inference despite its potentially invasive and risky nature. Participants saw value in applications that could help family members who need special care (e.g., a child with special needs, elderly parent, spouse who has medical condition), or lead to monetary benefits (e.g., saving on electricity bill).

Applications of Interest to Participants

When in-home sensing applications were directly related to household members' health and safety, participants were more willing to accept sensing and inference. For example, one participant who was opposed to the use of a sensing and inference system at the beginning of the exit interview (*"I feel pretty strongly that I don't think I would want something like that in my home"*) later explained,

> *"My dad has passed away (...) my dad fell. You know, it would have been a great thing for one of us to have known that my dad had fallen (...) Anything can be used for good or evil, I guess, but in that particular situation when someone needs to be monitored for their own health and safety, I think that is important. But I do think that their privacy needs to be respected as well."* [Household 8, participant a, or "H8a," exit interview]

As such, many participants sympathized with the use of sensing technology designed for eldercare purposes despite its invasive nature. Participants recognized that sensors may be used in a place like the bathroom, and that they would need to have difficult conversations with their elderly parents about this. The bedroom was another place where there was initially a strong resistance to sensor placement. However, when prompted with a sleep application usage scenario where a video camera is used to record sleep behaviors, all participants said that it would be okay to record them and their bedmate then share the data with a doctor if either of them had a sleep problem:

> *"If the issue was a sleep issue and we knew that this was some way to resolve it and they told us that then that would be absolutely fine."* [H6b, exit interview]

On the other hand, many participants were reluctant to the use of recordings for home automation systems (e.g., voice command for controlling appliances, detecting who is in which room to save electricity). They thought of home automation applications as supplements or luxuries rather than necessities, which may lead them to express cynical thoughts, such as "*I don't need things that are going to make me more lazy than I am* [H4b, exit interview]," or "*I think these sensors are weird and creepy. How many times would someone need to know I walk in and out of a room* [H8a, diary entry—thought/idea]."

Monetary Benefits and Incentives

A monetary benefit or incentive seems to make people feel more comfortable about adopting in-home sensing systems and sharing the sensing data with 3rd party providers. For example, during the initial interview, the majority of participants were excited about the idea of an electricity monitor that could provide real-time feedback on appliance-by-appliance electricity use. They could see the value in using the real-time feedback to experiment with the energy efficiency of competing behaviors (e.g. hand washing dishes vs. using the dish washer), to decide whether or when to replace an old appliance (e.g., from CRT TV to LCD TV), to plan a budget, to convince other household members to change their behavior to save on the energy bill, or to convince their landlord to replace an old appliance:

> *"I would give him* [landlord] *the evidence to say "look, this is what, how much we could be saving (...) The appliances really aren't efficient," and so in order to show my landlord that yeah, we could be saving a lot of money, and it's a selling point when you're trying to rent the house."* [H3b, initial interview]

However, some participants who were initially excited about the technology came back with reservations after the 4-week in-situ phase. One participant contemplated a 3rd party provider having access to household data:

> *"...this has been on my mind all week. The fact that the electric company can tell when I've turned on the dishwasher or a light bulb or the TV—that's pretty fascinating to me. I don't know how they do that, but do I want them to know that? Well it's not a bad thing. It's still a private thing. (...) I mean it's alarming and surprising, it's fascinating. I don't know if it's good or bad. I'm undecided."* [H10a, exit interview]

As with H10a, a few participants acknowledged that service providers might already know this type of information. Indeed, cable companies [30] and utilities are already making these inferences. We further prompted participants by saying that it may be possible to infer activities such as which TV program someone is watching [18], what appliance is being used [29], and whether somebody is at home [25] from the real-time electricity use data. Many participants said that this was fine *as long as the data stays in the home*. When we asked participants about sharing this data with a service provider (e.g., an electricity or cable company) without receiving any incentives, many participants felt uncomfortable and somewhat unnerved. One participant was concerned that the electricity company might restrict their electricity use; some felt that it was not the business of non-householders to know that type of detailed information; others felt that the electricity company would not have time to review this data on a daily basis anyway. However, participants who were initially opposed to the idea of sharing such data with a 3rd party provider became more favorable when they thought they might receive a discount on their utility bill. As with many other participants, the aforementioned participant thought that he would be willing to share TV watching behavior or electricity usage data with 3rd party providers in exchange for a utility bill discount: *"Well,* [half-priced] *cable would be nice. Something like that I would carefully weigh the proposal* [H10a, exit interview]*."*

Perceived Risks and Concerns of In-home Sensing

We now describe participants' perceived risks and concerns that could deter them from adopting in-home sensing appli-

cations. We discuss issues regarding the private nature of the in-home sensing data, unintended consequences of recording and playback, and the possibility of data leaks.

Private Nature of the In-home Sensing and Inference Data

The home is where private activities, intimacy, sociality, and mourning take place [23]. One participant who worked at a restaurant commented,

> *"I'm in public every night around hundreds of people. Most of my daily life—work life. So I'm always censoring myself at work and monitoring how I am, 'cause it's guest-related. So I like to go home and just be private and not monitor or think about what I'm gonna say or do."* [H2b, initial interview]

With in-home sensing and inference, it is highly likely that private activities may be captured by various technologies. Participants expressed concerns over the sensitivity of the data that might be captured from home such as picking one's nose or changing a baby's diaper. Even when we emphasized that the sensing technologies would be installed for the householders' own use (e.g., home monitoring) and no one other than the members of the household would have access to the data, some participants thought that they would be more self-conscious about what they say and do:

> *"I think there is a certain quality about, not preserving everything. Being a history person I am afraid to admit that but I think it's nice that some things are just left best unsaid…"* [H1b, exit interview]

There seemed to be an innate discomfort in being monitored or knowing that they could be monitored, even though participants understood the utility of the sensing devices. Some mentioned that sensors running in their home most of the time is such a foreign concept that they do not know how to respond and that after time, they might feel more comfortable or get used to the idea. Many participants did not seem to realize that they are already exposed to frequent sensing including CCTV cameras, alarm systems, credit card purchases, or use of telephone, Internet, or electricity.

Unintended Consequences of Recording and Playback

We discussed with participants that in-home sensing devices could run with or without saving data, but there would be trade-offs between the two approaches: saving more data over a longer time would allow people to review it later for the application's intended purposes, but it could be riskier from a privacy perspective. Not saving data would reduce privacy risks, but the technologies would be limited in what they could provide. For example, a video camera used for security purposes could either save data or not; a benefit of saving the data might be that it could be shared with police in the event of a burglary. In addition, we discussed other possibilities, such as setting a flexible retention period (i.e., recorded data remains in the system for a certain time period defined by the data retention policy), event-triggered recording (i.e., recording is initiated by a pre-defined triggering event), or rolling window recording (i.e., recordings older than a certain buffer length are automatically deleted) [10]. We assumed that all household members would have access to the recordings, but not outside people. Overall, the longer the retention period, the more uncomfortable participants felt about an application. The exception was when they were *not at home*; participants liked the idea of having recordings while all members of the household were absent.

Being able to playback the recording was seen as a double-edged sword because it might reveal potentially disturbing facts while providing useful information:

> *"When someone goes back and, 'Why were you here instead of over here?' You know, 'The dish broke, you said you didn't break it. Now I got it here.' It's just—you know, buy a new dish! Don't worry about the argument as to where and when and why."* [H4b, initial interview]

As participants thought further about the potential ramifications of recording, many of them commonly brought up a divorce scenario where partial recordings could be taken out of context and used for or against a case:

> *"I would hate to say this. Say you're in a divorce situation. And you wanted to use that as information, you know, to present your case. Then it seems like, "Well, I've got this all recorded here." But is that fair? Is that right?"* [H1b, initial interview]

Next, we discuss concerns around potential misuse of the recordings by non-members of the household.

Possibility of Data Leaks: Security and Data Storage

Although we assumed that no one other than the householders would have access to the data, many participants worried about outsiders getting access to the data. Householders with children tended to express more concerns; they worried that the data could be hacked or leaked someday, which could harm the safety or reputation of their children:

> *"It'd be my kids' safety. And if somebody got a hold of that, I don't know if I'd like that. And there's no way to guarantee–and if there is, great, but I would assume that there's, like, a 99.9% chance to guarantee, but there's still that one guy that's out there, the hacker, that's going to find his way in to see the image. So I wouldn't want that. Even if it did save on electricity, because I think safety is more important than saving a little bit on your electric."* [H6b, initial interview]

When we prompted participants with another scenario where data would be stored in the cloud so that users could access their data from anywhere, not many participants were favorable to this idea because of additional risks caused by server or network security vulnerabilities.

TENSIONS REGARDING SENSING AND INFERENCE

Recruiting pairs of adults living in the same household helped us investigate possible conflicts and tensions among householders around the use of sensing technologies. In addition, some of the participating households had frequent visitors such as family, friends, relatives, and service people, meaning that an in-home sensing and inference system would likely capture data about visitors. Participants had different tolerances and comfort levels toward what can be captured, how the data is used, and with whom the data can be shared. In this section, we discuss stakeholders' different perspectives around the use of sensing technologies.

Tensions between Couples

We encountered many cases where the two participants from a single household had different viewpoints about public and private places in the home and acceptability toward certain applications. For example, in response to a question about the *public* places in the home, one participant who worked from home stated, *"my wife will dispute that with me, but I'll say it's my bedroom. I conduct a lot of business out of my bedroom"* [H7a, initial interview]. As he predicted, his wife considered the bedroom to be a *mostly private* place. Participants' perceptions toward public and private places in the home were tightly related to where they would allow sensing and recording devices. This divergence of opinions and different tolerances toward what can be captured and where sensing and/or recording would be allowed were a source of potential conflict.

One couple had a child with special needs. The mother was the child's primary caregiver. She described herself as a very private person; she was very opposed to sensing until she realized that she could use the video to record incidents with her child and she could share it with a therapist:

> *"It would be nice to capture some of his* [son's] *behavior on video and then show it to, like, his therapist or something. 'Cause it's hard to explain—when you're in the moment, and then go to the therapist and try to explain exactly what went on, you know."* [H4a, initial interview]

However, when we interviewed her husband, he was overwhelmingly negative toward the use of any sensing devices whether or not they recorded data. He worried sensing would cause the family to quarrel over trivial matters, which would not happen otherwise.

> "*Conversations could get heated up if somebody was supposed to be doing chores, and we've got them videoed, you know, watching a TV program or something. I'd rather just not worry about that, and make sure the chores get done later, as opposed to have something that people would go back and start referring to. You know, I think at this point, you know, you're much happier not having that access.*" [H4b, initial interview]

In an earlier section, we pointed out that applications related to safety and health were far more likely to be acceptable to householders. However, we observed strong resistance toward sensing which H4b raised. Interestingly, after four weeks, H4a, his wife, came back saying that she changed her mind and would not want to have a video camera running 24/7 for the purpose of capturing her son's behavior. In this particular case (H4a and H4b), the couple's opinions converged in the end. However, for couples with contrasting opinions, conflict may arise with respect to competing values and priorities.

Regarding the electricity monitor that might be able to infer what TV program or movie someone was watching, H1b mentioned that there are *"gray areas which do not get discussed between husband and wife, and still not affecting each other to the best of their ability"* [exit interview]. H3a was particularly sensitive about the electricity monitor data:

> *"I guess, realistically, it* [electricity monitor's capability to know what program somebody is watching] *might still bother me because, for instance, even though my wife and I are a couple, there are still probably things that either one of us might do at any given time that is private that we wouldn't share with the other person. And so—like if I put in an X-rated thing, I wouldn't really want somebody to be able to tell – you've been watching these videos a lot, you know."* [H3a, initial interview]

Tensions between Parents and Children

About half of the participants were either parents or expectant parents. When we asked whether it would be acceptable to have video or audio recordings in their children's room, we received mixed responses. While participants wanted to be perceived as a "good parent" who respects their child's privacy and gives them freedom, they also wanted to be perceived as a "responsible parent."

> *"It* [video camera] *should not be there* [children's bedroom]. *Although, honestly, I would want it there. I could see reasons why I would want to know what's going on in those rooms at all times. I just—I probably wouldn't do it anymore than I would peek through the peep hole or look under the door."* [H6a—a parent with three children, initial interview]

Similar sentiments were expressed regarding the electricity data from which parents could possibly infer what TV program the child was watching and when. H5a stated that it seemed like crossing a line if she knew what her husband was watching when she was not at home, but she would feel differently if it were her child's data. She explained,

> *"I would never be one to read my kid's diary, but just to make sure they're not—you know, I mean, there's a lot of stuff on TV—violence and, you know. Make sure they're not—and I guess computers. Oh, my god. I worry about, like, how long they're on."* [H5a, initial interview]

Although all of the parent participants stated that they would talk to their children up front about the recordings wherever they are installed, not everyone agreed on including their child's opinion in deciding whether to adopt sensing and inference systems. In our study, it was the adults in the family (or "*those that are contributing to the mortgage*" [H8a]) who make such decisions. Parent participants were reluctant to give their children direct access to any recordings. Despite not having the opinions of the children in our study data, we could expect that they might resist sensing being in their bedrooms, which we learned from a diary entry about a conversation prompted by the sensor proxies:

> *"My son (7yr) asked if he was being recorded. I asked if he'd mind and he said he would not want to be recorded. Why? Because he might say something personal."* [H1b, a diary entry]

Tensions between Householders and Visitors

Most of the participants had guests come to their home during the study period. During the exit interview, we asked if visitors had noticed the sensor proxies or if the participants had discussed the study with anyone. Although the sensor proxies were not intended to imitate a recording device per se, the proxies prompted participants to think about how they might communicate such a system to visitors:

"My 30-year-old brother-in-law stopped by to visit. He was watching TV in the living room when I came home and activated the sensor as I passed it. He asked what the light was for and I explained that we are doing a study about sensing devices in the home. We told him that potentially video (raw/clear), glass shattering detection, and power (electricity) monitoring could be available in the future. He said that if the device was video recording him that he would feel very uncomfortable and would not want to visit." [H9a, diary entry]

Participants had different expectations about and strategies for how they might communicate an in-home sensing and inference system to a visitor. These expectations and strategies varied depending on the *relationship between the householder and visitor* and the *data processing techniques* that an application collects and retains. First, the relationship between the householder and visitor matters. If the visitors were close friends and family, most of the participants said that they would tell the visitors about such a system—for some, this was due to privacy reasons, but for others, it was due to their fascination toward technology. A few participants said that they would feel obligated to tell visitors about the recording and would expect the same if they visited another's home [H2a, H3b, H5a, H5b, H8a]; some said that they would simply post small signage outside of their home [H7b, H8b, H10a]; others thought that they would tell only when guests ask, because "*By the way, you're being taped"* [H3a, initial interview] is such a weird conversation to have whenever they have a guest come over [H3a, H6b, H10b]. However, if the visitors were service people such as a babysitter, caregiver, or plumber, participants said that they would notify them differently:

"If there was ever an outside babysitter that I didn't know, I surely wouldn't tell them there was a camera; I'd want to actually see, you know, what they'd do." [H7a, exit interview]

"I think the people that are closer to you are the people that you're more apt to tell than those that are strangers. (...) I wouldn't feel that I needed to tell the service guy that you're on candid camera." [H8a, exit interview]

Another strategy toward service people was to give a *subtle* notification—for example, telling them that the home had a sensing and inference system, but not providing details:

"I would say, "Just to let you know, we have a home monitoring system and, you know, we're not going to be like keeping tabs on you, but I want you to know that," because it would invoke fear in them, I think." [H5b, exit interview]

Second, the data processing techniques that reduce the sensitivity of recordings matter. A majority of participants thought that they should inform visitors of the system in one way or another if it captured raw data (e.g., raw video or audio). However, if it only captured filtered data (e.g., garbled audio, blurred video), several participants said that they would feel less obligated or not feel the need to tell visitors at all. They believed that filtered data was less identifiable and less sensitive, and hence, they expected that others would care less.

Not every participant would treat visitors to their home as they would want to be treated in someone else's home. A few participants who said that they *would not* feel obligated to tell visitors about a system in their home later mentioned that they *would* expect others to tell them in advance if the home they were visiting had a sensing and inference system. When we asked participants how they would feel if they found out after the fact that they had visited someone's home who had a sensing and inference system running, one participant remarked:

"'Hey, that's un-cool man,' you know (...) I might even be inclined to say, 'I'm not going over to Susan's house because she has that thing on and I don't like it.'" [H3a, exit interview]

Reciprocity ("if I see you, you see me") is considered as an important privacy control feature in the workplace media setting [1]. However, this was not always the case in the home setting. All participants said that they would let visitors review the data *only if* the visitor asked to rather than share it always. In terms of data ownership, most of the participants thought that the recording would belong to the householders, and the same policy would apply when they visit someone else's home. However, if a recording captured in someone else's home contained data about the participants, the participants would want to know the reason for the system.

We could not identify a single social norm for how to communicate recording practices in the home with which all participants could agree. The divergence of opinions and contradictory expectations indicate that in-home sensing and inference systems that record data could be a source of tension between householders and visitors.

DISCUSSION

Technical mechanisms could potentially lower some of the privacy risks of sensing and inference systems by limiting when and what types of data systems are allowed to capture in the home. However, a bigger challenge lies in the social tensions among householders as well as between householders and visitors. In what follows, we discuss privacy mechanisms that might reduce privacy risks and tensions around sensing status notification. We also reflect on our method for gathering grounded reactions in situ.

Mechanisms to Reduce Privacy Risks

Limited capability sensors for the home: Although technology trends push for richer and higher-fidelity sensors, we see opportunities for sensing and data processing techniques that can strictly limit what information can be inferred from sensed data in the home. For example, a recent study proposes a new microphone-based cough sensor that only sends the relevant features of coughing sounds to a central server in such a way that the features can only reconstruct the coughing sounds, but any speech would be unintelligible [22]. This technique would keep the cost of the sensors low (all the computation does not need to be done on the sensor) and still enable some recording in a privacy-preserving manner. Non-invertible audio pro-

cessing techniques are already being developed in the signal processing community (e.g., [31]). Similarly, one can imagine vision filters that can convert a general-purpose camera into a single event detector (e.g., fall detector) that could alleviate people's concern as to placing cameras in a private area of the house (e.g., bathroom or bedroom).

Context-aware sensing: While participants felt recording raw video data at home was too invasive, they clearly saw the need for it when household members were *not at home* (e.g., security cameras for capturing a burglar). Taking this a step further, participants expressed their desire to switch back and forth between high-fidelity (e.g., raw video) and low-fidelity (e.g., blurred video) sensing depending on the situation. For instance, one participant mentioned a dual-purpose camera in the living room: when the family is around, the camera operates with blurred video (that can still identify who is who) for automatically personalizing video content on the TV. However, the same camera can capture full-blown faces of intruders when the householders are not home. One could imagine building a two-level inference system that uses an unobtrusive sensor to detect household members' presence in the home and automatically switch between video feed types.

Secure recording with limited playback: As some of the participants mentioned, recording of sensed data, especially video and audio data, can be misused by household members at a later date out of the context (e.g., evidence for a divorce case). Requiring household members to set up access control policies could be challenging. Instead, we hypothesize that a reasonable default data use policy that limits playback of recorded data can reduce the risk without compromising the usefulness of sensed data in the home. For example, the sensing system can enforce recorded data to be automatically deleted after a certain time period or to be viewed only a pre-specified number of times.

Tensions between Aesthetics and Visible Notification

There is an inherent tension between maintaining the overall aesthetics of the home and making the status and the existence of the system obvious. While participants did not like to have sensing devices be visibly installed in their home, they also felt the need to have a proper status notification (especially for an *on by default* system) to clearly indicate when the sensing is off or a timely reminder (especially for an *off by default* system) in cases where the user forgets to turn it on. Moreover, the system sometimes needs to be hidden to fulfill its duty (e.g., supervising service people) or to avoid unnecessary conversation. Thus, making invisible sensing more visible may not always be an appropriate solution for the home, and yet we need to find better ways to gracefully communicate sensing and inference systems. Notifying visitors and service people about the system was a particularly thorny issue because it could influence existing relationships and established trust. Thus, designing a gentle notification system (e.g., a location-based reminder on a cell phone whenever a user enters a space with cameras) warrants future research efforts.

Methods to Gather Contextualized Feedback

It is difficult to study people's perceptions toward technology that is not yet prevalent. In addition to many technical, social, and pragmatic challenges of sensing system deployments (e.g., [5]), it takes effort for people to reflect on a new technology concept. People can meaningfully reflect on technology when they understand its benefits as well as the risks. Therefore, a specific sensing context that would resonate with their needs and interests should be established before asking people's perceptions. Our mixed-method approach using in situ probes with in-lab activities helped us collect contextualized feedback in three ways. First, the provocative nature of the probes helped participants articulate their thoughts during exit interviews. We observed many occasions where people were actively thinking about the benefits as well as the problems with the sensing in situ:

> *"It* [sensor proxy] *reinforced the fact that I wouldn't want anybody videotaping me or recording me doing everything I do during the day… like I'd walk past it and I'd chuckle to myself saying, 'Oh, now just think if they were videotaping me, they'd see that I entered the house four times as I was just trying to leave.'"* [H8a, exit interview]

Second, the probes and diary were effective in capturing participants' grounded reactions in context:

> *"Seeing the lights on reminds me of what they represent and I don't like it. I would not want cameras or recorders in the house. I notice the sensor all the time, but I try to ignore them."* [H4b, diary entry]

Third, the probes often became a conversation starter between householders and visitors:

> *"Same friend ask what the lights were doing in my room. I explained the project and he asked me if it was recording our data. I told him, nah… and explained he should relax as it is all good at my house. He agreed."* [H7a, diary entry]

However, as the study progressed, some participants reported forgetting the main purpose of the probes and started to use them as nightlights. Others were surprised by how quickly they got used to the probes (*"I forget they're there for the most part"* [H2a, diary entry]), which could mean that the probes did not always effectively force reflection or that forgetting could also happen in real world sensing contexts.

Since our participants were limited to middle-income families in the U.S., the results are perhaps mostly applicable to the specific demographic that was studied. However, we can further use our method to study other types of households (e.g., a single person, roommates), other groups (e.g., seniors), or specific sensing domains (e.g., simulating electricity sensing) for which the use of this method to understand people's needs and concerns could be valuable.

CONCLUSION

While in-home sensing and inference systems can provide numerous benefits, privacy risks and concerns exist. To understand what might affect people's receptiveness to in-home sensing systems, we conducted in-lab activities and

four-weeks in situ with a cultural probe that used sensor proxies with 22 participants from 11 households. Through our mixed-method approach, we gathered contextualized feedback on participants' perceived benefits and risks of in-home sensing applications, and identified tensions among stakeholders. Based on our results, we provide design insights to alleviate perceived privacy concerns and tensions among stakeholders. Our study calls for careful design and implementation choices of sensing system modalities based on an understanding of these concerns.

ACKNOWLEDGMENTS

We would like to thank the participants in this study as well as Sidhant Gupta for assisting with the study and Khai Truong for early reviews of the draft. This work was supported by Intel Labs Seattle and has been reviewed and approved by University of Washington's Institutional Review Board, protocol #38991.

REFERENCES

1. Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. *ECSCW '93*, 77–92.
2. Boehner, K., Vertesi, J., Sengers, P., Dourish, P. (2007). How HCI interprets the probes. *CHI '07,* 1077–1086.
3. Caine, K.E., et al. (2010). DigiSwitch: design and evaluation of a device for older adults to preserve privacy while monitoring health at home. *IHI '10,* 153–162.
4. Choe, E.K., Consolvo, S., Jung, J., Harrison, B., & Kientz, J.A. (2011). Living in a glass house: a survey of private moments in the home. *UbiComp '11,* 41–44.
5. Edwards, K., & Grinter, R. (2001). At home with ubiquitous computing. *UbiComp '01,* 256–272.
6. Froehlich, J., et al. (2009). HydroSense: infrastructure-mediated single-point sensing of whole-home water activity. *UbiComp '09*, 235–244.
7. Gaver, B., Dunne, T., & Pacenti, E. (1999). Cultural probes. *interactions, 6*(1), 21–29.
8. Glaser, B.G., & Strauss, A.L. (1967). The discovery of grounded theory: strategies for qualitative research. New York: Aldine Transaction.
9. Gupta, S., Reynolds, M.S., & Patel, S.N. (2010). ElectriSense: single-point sensing using EMI for electrical event detection and classification in the home. *UbiComp '10*, 139–48.
10. Hayes, G.R., et al. (2004). The personal audio loop: Designing a ubiquitous audio-based memory aid. *Mobile HCI '04*, 168–179.
11. Hayes, G.R., & Abowd, G.D. (2006). Tensions in designing capture technologies for an evidence-based care community. *CHI '06*, 937–946.
12. Hayes, G.R. et al. (2007). Physical, social, and experiential knowledge in pervasive computing environments. *IEEE Pervasive Computing, 6*(4), 56–63.
13. Hong, J.I., Ng, J.D., Lederer, S., & Landay, J.A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *DIS '04*, 91–100.
14. Iachello, G., & Abowd, G.D. (2005). Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing. *CHI '05,* 91–100.
15. Iachello, G., Truong, K.N., Abowd, G.D., Hayes, G.R., & Stevens, M. (2006). Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. *CHI '06*, 1009–1018.
16. Jacobs, A.R., & Abowd, G.D. (2003). A framework for comparing perspectives on privacy and pervasive technologies. *IEEE Pervasive Computing*, *2*(4), 78–84.
17. Klasnja, P., et al. (2009). Exploring privacy concerns about personal sensing. *PERVASIVE '09*, 176–183.
18. Kuhn, M. (2004). Electromagnetic eavesdropping risks of flat-panel displays. *Workshop on Privacy Enhancing Technologies,* 23–25.
19. Ladd, J. (1991). Computers and moral responsibility: a framework for ethical analysis. In C. Dunlop & R. Kling (Eds.), *Computerization and controversy: value conflicts and social choices* (pp. 664–675). Academic Press Inc.
20. Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. *UbiComp '01*, 273–291.
21. Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. *UbiComp '02,* 237–245.
22. Larson, E.C., Lee, T., Liu, S., Rosenfeld, M., Patel, S.N. (2011). Accurate and privacy preserving cough sensing using a low-cost microphone. *UbiComp '11,* 375–384.
23. Leonardi, C., Mennecozzi, C., Not, E., Pianesi, F., Zancanaro, M., & Gennai, F. (2009). Knocking on elders' door: investigating the functional and emotional geography of their domestic space. *CHI '09*, 1703–1711.
24. Massimi, M., Truong, K.N., Dearman, D., Hayes, G.R. (2010). Understanding recording technologies in everyday life. *IEEE Pervasive Computing*, *9*(3), 64–71.
25. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E. & Irwin, D. (2010). Private memoirs of a smart meter. *BuildSys '10,* 61–66.
26. Neustaedter, C., Greenberg, S., & Boyle, M. (2006). Blur filtration fails to preserve privacy for home-based video conferencing. *ACM Transactions on Computer-Human Interactions, 13*(1) (Mar 2006), 1–36.
27. Nguyen, D.H., Kobsa, A., & Hayes, G.R. (2008). An empirical investigation of concerns of everyday tracking and recording technologies. *UbiComp '08*, 182–191.
28. Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *CHI '03*, 129–136.
29. Patel, S.N., et al. (2007). At the flick of a switch: detecting and classifying unique electrical events on the residential power line. *UbiComp '07,* 271–288.
30. TV's Next Wave. (2011). http://online.wsj.com/article/SB10001424052748704288304576171251689944350.html
31. Wyatt, D., Choudhury, T., & Blimes, J. (2007). Conversation detection and speaker segmentation in privacy sensitive situated speech data. *Interspeech '07*, 586–589.
32. Xbox Kinect. http://www.xbox.com/en-US/kinect.