Sensing or Watching? Balancing Utility and Privacy in Sensing Systems via Collection and Enforcement Mechanisms

Adam J. Lee
University of Pittsburgh
Pittsburgh, PA, USA
adamlee@cs.pitt.edu

Jacob T. Biehl
FXPAL
Palo Alto, CA, USA
biehl@fxpal.com

Conor Curry
University of Pittsburgh
Pittsburgh, PA, USA
clc231@pitt.edu

ABSTRACT

Devices with embedded sensors are permeating the computing landscape, allowing the collection and analysis of rich data about individuals, smart spaces, and their interactions. This class of devices enables a useful array of home automation and connected workplace functionality to individuals within instrumented spaces. Unfortunately, the increasing pervasiveness of sensors can lead to perceptions of privacy loss by their occupants. Given that many instrumented spaces exist as platforms outside of a user's control—e.g., IoT sensors in the home that rely on cloud infrastructure or connected workplaces managed by one's employer—enforcing access controls via a trusted reference monitor may do little to assuage individuals' privacy concerns. This calls for novel enforcement mechanisms for controlling access to sensed data.

In this paper, we investigate the interplay between sensor fidelity and individual comfort, with the goal of understanding the design space for effective, yet palatable, sensors for the workplace. In the context of a common space contextualization task, we survey and interview individuals about their comfort with three common sensing modalities: video, audio, and passive infrared. This allows us to explore the extent to which discomfort with sensor platforms is a function of *detected states* or *sensed data*. Our findings uncover interesting interplays between content, context, fidelity, history, and privacy. This, in turn, leads to design recommendations regarding how to increase comfort with sensing technologies by revisiting the mechanisms by which user preferences and policies are enforced in situations where the infrastructure itself is not trusted.

CCS CONCEPTS

• **Security and privacy → Access control**; **Privacy protections**;

ACM Reference Format:
Adam J. Lee, Jacob T. Biehl, and Conor Curry. 2018. Sensing or Watching? Balancing Utility and Privacy in Sensing Systems via Collection and Enforcement Mechanisms. In *SACMAT '18: The 23rd ACM Symposium on Access Control Models & Technologies (SACMAT), June 13–15, 2018, Indianapolis, IN, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3205977.3205983

SACMAT '18, June 13–15, 2018, Indianapolis, IN, USA

ACM ISBN 978-1-4503-5666-4/18/06…$15.00
https://doi.org/10.1145/3205977.3205983

1 INTRODUCTION

The world is becoming an very connected place. Advancements in the Internet of Things (IoT) and wearable technologies are extending the reach of technology into daily life. This is resulting in the collection of huge amounts of data about people, instrumented spaces, and the interactions between people and spaces. One promising class of technologies within this space is workplace awareness tools. The development, deployment, and study of these types of systems is a rich space within the intersection of the IoT and sensing research communities. By leveraging instrumented spaces, these types of systems are able to provide details and assistance about co-workers' location and availability, as well as contextualize how shared spaces are being used. Deployments of these technologies have shown their value in increasing timely communication among peers and promoting a greater sense of community in the work environment (e.g., [7, 11, 21, 23, 34]).

However, these systems also expose workers to a variety of potential security and privacy risks, especially when users are suspicious of the operators of the system. For instance, a vengeful manager could use data that was collected to help foster collaboration in ways that were not envisioned and are potentially detrimental to the employee. These concerns are legitimate, and are often reported as a major barriers to adoption or widespread use in the studies of these systems. As Patil et al. [31] noted, *"user opposition due to privacy concerns can translate into minimal use or even the abandonment of the system."* Similarly, Biehl et al. [6] found that *"Violations of their model [of data use], or even uncertainty as to how the data are being used, negatively impacts use"* of these types of systems. Interestingly, standard approaches to access control are unlikely to increase user comfort if the system enforcing these controls is not trusted by the user specifying preferences or policies regarding the collection and use of their information.

This presents an interesting tension: namely, balancing appropriate uses of these technologies while protecting individuals' privacy. There are many approaches that have been proposed for mitigating this tension, ranging from the use of formal policies, to controls for reciprocity and awareness. An alternate take on this issue appeals to Saltzer and Schroeder's oft-cited principle of least privilege: *Every [component] of the system should operate using the least set of privileges necessary to complete the job* [36]. Viewed through this lens, it is unsurprising that privacy and sensing are intrinsically linked: systems that have an imbalance in the amount, fidelity, or type of data that is collected to support a given sensing task can lead to actual (i.e., realized) or perceived (i.e., potential) privacy violations. For instance, a system that counts people in a space using video will always have the potential to collect and, in the worst case, share the broader—and perhaps sensitive—contexts of

and goings-on within that space. These violations can be malicious or, more likely, accidental.

This exposes an important technical challenge: preserving some notion of least privilege by mitigating privacy concerns at the sensing level, while supporting functionality and usability at the application level. We explore three modalities of presence sensors typically found in the workplace: those built using video, audio, or motion monitors. Given minimal performance differences between sensors built using each of these modalities in common workplace scenarios, we carry out a broad and representative evaluation exploring user-level discomfort arising from privacy concerns with these technologies across a variety of contexts of use.

In this work, we show that the privacy and utility gap can be narrowed such that there is better alignment between the technologies deployed and individuals' concerns over privacy. We conclude that complex policy controls may not be the best solution to the challenge of balancing privacy and utility in these workplace awareness scenarios, and perhaps broader IoT contexts. We further posit that these controls should be supplemented by the careful selection of sensing technologies used, in accordance with the principle of least privilege. We support this conclusion through a series of lessons for the design of future systems for enabling workplace awareness that balance accuracy with the privacy needs of individuals within an instrumented space.

2 RELATED WORK

We now highlight key areas of related work that provide context for the class of sensing problems that we study, raise privacy issues associated with ubiquitous and social systems, or propose solutions to the privacy problems emergent in these types of environments.

2.1 Awareness Technologies

Sensor driven awareness systems have a rich history in this research community. Early work on Portholes [11], a tool for sharing video feeds of colleagues' offices, pioneered the concept of workplace awareness tools. This work has inspired researchers to better understand the importance and conveyance of rhythms and activities in the workplace. For instance, Begole et al. [2] and Reddy and Dourish [33] both observed that workers exhibit periodic, predictable behaviors, or rhythms, and these signals become well understood in long term co-working environments and are often used in deciding how or when to establish contact.

Many systems have been developed to transition these findings into technological solutions. These include BlueSpace [28], ConNexus [40], MyVine [16], SideShow [7], InteruptMe [21], MyUnity [46], and many more. Many of these systems have been studied through broad deployment. Throughout the findings, there is consensus from this body of work that awareness systems are perceived by workers as useful tools in workplace. Further, their use has also been shown to effect many positive workplace communication behavior changes such as decreased time spent on email and an increase in more productive face-to-face meetings [7, 21, 46].

2.2 Privacy Issues in Ubiquitous and Social Systems

Ubiquitous and social computing systems are home to unique privacy problems [24]. These systems differ from traditional computing systems in that information is gathered continuously, rather than being created by individuals in distinct editing sessions. Further, individual users must behave as policy administrators and govern their own data sharing, rather than relying on trained security administrators to set policy for them. This pervasive collection of information and near seamless sharing make it easy to accidentally post information to unintended audiences [12], which can lead individuals to harbor feelings of regret [32, 44], cause feelings of embarrassment or humiliation [39], or even loss of employment [38].

Much research has been conducted into the factors leading to discomfort with the sharing of contextual information. Many studies have shown that a user's relationship with the data consumer to impact their comfort in sharing information (e.g., [9, 29]). The granularity at which information is accessed (e.g., city- vs. GPS-level access to location) has been found to be an important factor governing comfort (e.g., [6, 9, 30]), as has the frequency with which data is accessed by others (e.g., [6, 37]). Whether or not data is stored historically or simply shared ephemerally has also been shown to contribute to individuals' comfort with these systems [6]. Similarly, the purpose with which information is accessed has a major impact on individuals' comfort with sharing (e.g., [6, 9, 41]). These and other factors lead to a myriad of potential privacy issues in context sharing systems.

Of particular note are studies of sensing within the context of smart homes. The literature contains general discussions of privacy as being an important factor to consider in the design of smart homes (e.g., [27]), survey studies of behaviors in the home (e.g., [8]), and the development of purpose-built sensors for detecting home activities (e.g., [15]). Like our work, the above highlight the important role that context and fidelity play in perception of privacy. However, this body of work tends to focus either on privacy in a general sense, or the perceived implications of a particular sensing technology. Our work assesses the privacy implications of a variety of sensing technologies for a single type of sensing task across multiple contexts: to our knowledge, this is a unique contribution.

2.3 Privacy Controls for Ubiquitous and Social Systems

Given the complexity of issues surrounding privacy in these types of systems, a diversity of work has been done on developing solutions to provide users with some measure of control over their data sharing. Much work has gone into designing access controls and policy languages that can be used to govern data and context sharing in these types of systems, many of which provide controls for the above types of factors influencing individual comfort (e.g., [10, 17, 19, 22]). Others, however, recognize that individuals are often not trained as policy administrators, and instead seek to use machine learning to automate the process of setting privacy policies for location or social networking systems (e.g., [14, 35]).

Systems that make use of reciprocity in sharing are becoming more prevalent in this space. For instance, the privacy settings on

LinkedIn[1] allow users to see who has viewed their profile only if they are willing to share their identity with individuals whose profiles they visit. Similar efforts have been explored in the context of location sharing [3]. Other systems like Facebook Messenger[2], WhatsApp[3], and Google Hangouts[4] provide notifications to senders when messages are read by their recipients, making for reciprocal data sharing between the sender and receiver.

In addition to controls for who can access information, others have looked at building awareness regarding *when* information is accessed. This has a long history in the ubiquitous computing space [4], and has recently been explored in the context of social [43] and location sharing [37, 42] systems. These systems may make use of explicit, log-like records of accesses to an individual's data [42], or make use of summary techniques in an effort to preserve the privacy of individuals requesting information [37].

Finally, we note that the types of privacy controls explored our work occur at the sensor level, before the data to be shared with a system is even computed. As such, the resulting awareness information is amenable to any of the above-described approaches to further protect individual privacy.

3 WORKPLACE ACTIVITY SENSORS

In this paper, we seek to study the utility and privacy attitudes that people harbor towards sensing technologies that have application in the workplace. To this end, we describe a particular sensing task that enables a variety of smart-space functionality, identify three sensor modalities that are typical in today's workplaces, and explore the relative trade-offs between these types of sensors. These sensing modalities will form the basis of a survey and interview study aimed at understanding the design space for sensing systems that people trust to balance these types of trade-offs.

3.1 Scenario and Technologies

A key functionality of awareness platforms, and smart offices in general, is the ability to automatically assess the occupancy or utilization of a space. This functionality can help individuals locate colleagues for the purposes of interaction or collaboration (e.g., *Is Chris in his office?*), as well as contextualize spaces (e.g., *Is Chris alone in his office, or holding a meeting? Is anyone using the 4th floor conference room?*). For the purposes of our investigation, we focus on the following sensing problem:

Problem (Space Contextualization). *Given a space S, determine whether S is unoccupied, in use by a single individual, or being used by multiple individuals.*

In the event that (some) spaces are controlled by individual users, the above problem can help with certain classes of localization: e.g., if Chris' office is occupied, Chris is probably in it. Furthermore, presence sensors are used in a variety of tasks including security monitoring, building automation, energy conservation, space-based analytics, etc. A principle aspect of building smart workspaces is understanding whether and to what degree spaces are occupied. As such, the space contextualization problem is a foundational enabler for a variety of applications.

[1]http://www.linkedin.com/
[2]https://www.messenger.com/
[3]https://www.whatsapp.com/
[4]https://hangouts.google.com/

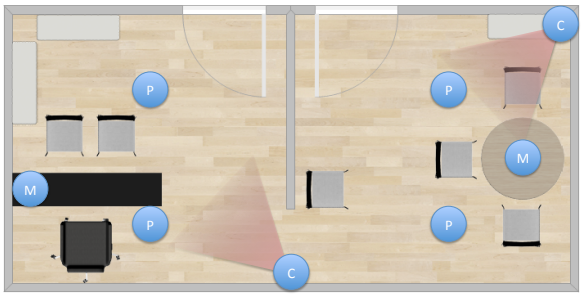


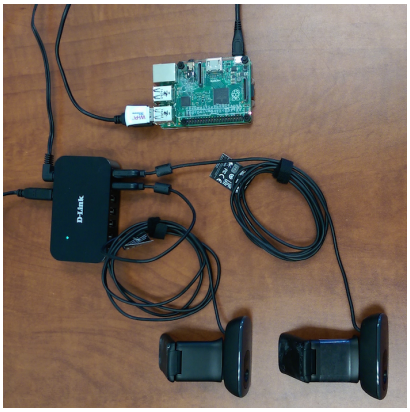
Figure 1: Office floor plan with sensor placements (C = Camera, M = Microphone, P = PIR housing)

We note that locating a single user is easily accomplished via the use of indoor localization techniques (e.g., based upon ultrasonic sound [18], infrared [45], RFID [20], WiFi/Bluetooth [5], or coded light [13] transmissions). However, leveraging indoor localization techniques to address the space contextualization problem is tricky. First, this requires buy-in from *all* individuals that may potentially use a space; this is likely unreasonable in situations with individuals not deriving value from this tracking (e.g., customers at a bank, or undergraduate students attending office hours). Second, these systems can enable persistent employee tracking in ways that other sensing platforms may not.

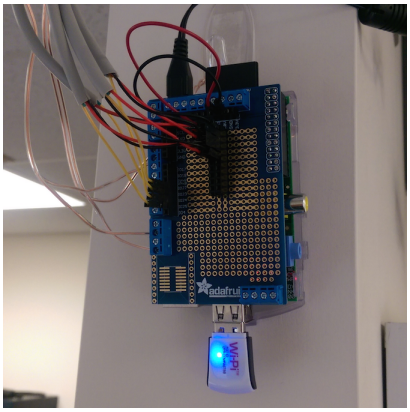
3.2 Prototypical Sensor Platforms

Rather than surveying user perceptions of purely hypothetical sensors, we sought to ground our study in reality. We began by carrying out an informal assessment of the types of sensors commonly deployed in office environments. In the end, three sensing modalities emerged as pervasive in these environments: video, audio, and passive infrared (PIR). The use of both video and audio processing date back to early work in presence literature (e.g., the Portholes system [11]), and readily support object and conversation detection. Further, these three sensing technologies are widely deployed in existing workplaces: cameras are deployed in many workplace security systems; microphones are increasingly deployed as part of networked meeting spaces and voice assistants (e.g., Apple's Siri, Google Home, or Amazon Echo); and most office spaces use PIR sensors to automatically control lighting and other environmental systems. Although individuals may not have each of these technologies in their personal workspace, it is likely that their pervasiveness means that individuals have a general sense of familiarity with these technologies.

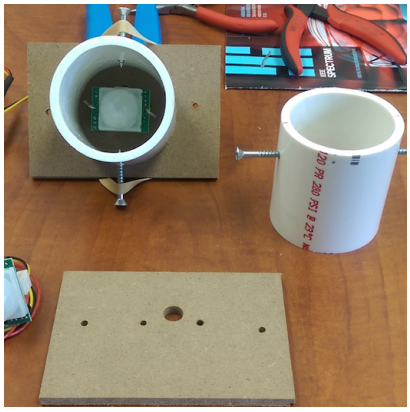
One thing that was unclear from our assessment was the degree to which these sensing modalities might differ in terms of accuracy for the sensing task at hand. If this were the case, accuracy differences between technologies would likely dictate deployment decisions, thereby overriding ancillary benefits of one technology over another (e.g., user privacy considerations). To explore this, we ran a small experiment in which we instrumented an office (Figure 1) with three prototype sensors (one per sensing modality). These prototypes were informed by the presence literature, and



(a) Camera-based sensor (Raspberry Pi v2)



(b) PIR Sensor (Raspberry Pi v1)



(c) PIR sensor housing

Figure 2: Prototype sensor hardware. The camera- and PIR-based sensors were developed using the Raspberry Pi platform to allow for easy incorporation into the physical environment. The housings used in the PIR sensor package allow for the monitoring of smaller office sub-regions, rather than the office as a whole. The audio sensor (not pictured) was a software-only implementation installed on computers already existing in the space.

are shown in Figure 2. We evaluated sensor accuracy in this context over the course of a typical work week, and found only minor variations in accuracy across a variety of workplace activities. This indicates that, even at the prototype level, accuracy alone should not, solely, dictate sensor selection.

3.3 Trade-offs

These types of sensors represent a range of utility and privacy affordances. The camera-based sensor package provides easy deployability in spaces already outfitted with cameras. However, processing high resolution images of a space to detect a three-value state carries a high potential for privacy "collateral damage" if the camera feed is compromised or stored. Audio sensor packages would likely require slight modifications to room-based microphone systems, as the microphones must sample continuously, rather than only when activated by the user. The audio sensor that we deployed was designed to prevent the capture of entire conversations via sampling, although we have not formally studied whether it is possible to reconstruct words (or even emotional states) from the snippets that are captured and processed. Finally, the PIR sensor package has the lowest potential for privacy violation, although this comes with the most overhead in terms of deployment. Typical PIR sensor configurations in office spaces are designed to scan the entirety of the space, not the targeted areas used by our application.

The literature (e.g., [4, 6]) highlights the need for tunable participation in awareness systems to help balance privacy and utility. This is in terms of enabling opt-in or opt-out of various sensors, as well as balancing the frequency, fidelity, and archival of information captured. Clearly, providing more information leads to higher quality presence states. However, privacy must be considered, otherwise invasive sensors will simply be turned off, reducing the quality of data brokered by the system. Despite this observation, the research community has largely been focused on understanding and improving the performance of individual technologies. Our hope is that reducing the privacy collateral damage associated with sensing by appealing to the principle of least privilege will lead to greater sensor opt-in, which increases the quality of information provided by the system. *That is, we believe that sensors designed for privacy can actually beget utility.* In support of this sentiment, we now turn our research towards understanding how the selection of these potential technologies could impact workplace privacy expectations and sentiments.

4 SURVEY OF CONTEXT SENTIMENT

In the previous section, we examined various technologies for workplace presence detection tasks. While this effort provides a good grounding for gaging trade-offs of one technology over another for a given context of use, it also raises many meta-level questions about how sensing technologies are *chosen* for deployment. Specifically, the varying tension between ease of deployment and accuracy vs. perceived invasiveness could help guide the deployment of awareness systems that balance the need for high quality information with the privacy of the individuals using monitored spaces. Towards building a broader understanding of this tension, we conducted a large-scale survey that examines user sentiment and concerns across a variety of contexts of use.

4.1 Contexts of Use

With breadth as the goal, we designed our survey to gage user sentiment regarding presence sensing technologies across four broad contexts of use. Three contexts were situated within a workplace setting. In each context, the workplace was introduced in the following way: *"Consider that you work in a workspace where each worker has his/her own office, and a presence system is in use to help facilitate person-to-person communication within the workplace."* We further specified the context of use into three categories, described to users as follows:

- **Personal office (PO):** *Consider the use of [presence] technologies within your own office.*

- **Colleague's office, work (CW):** *Consider the use of [presence] technologies while you are visiting a colleague's office to attend a work related meeting.*
- **Colleague's office, social (CS):** *Consider the use of [presence] technologies while you are visiting a colleague's office for the purpose of a brief social interaction.*

A fourth context of use focused on use in workplaces a person may visit as a **Customer to a Business (B)**. It was defined to users as follows: *"Consider you are visiting a place that you do business with (e.g., a bank or insurance office), and a presence system is in use to manage the distribution of incoming clients to representatives of the business. Consider the use of these technologies while you meet with a representative in his/her personal office."*

4.2 Presence Technologies

In the survey, we asked about the same technologies explored in the previous section: video camera (C), audio microphone (A), and motion sensor (M). As noted before, our motivation for selecting these technologies is that they are already in pervasive use in workplaces today and, perhaps as a result, are technologies that everyday users are likely to understand.

We prepared a series of short video explanations to (i) explain the purpose of data collection, (ii) situate how the technologies are used, and (iii) provide details about what information each technology collected, and the events that it could detect. These videos showed a typical office workplace (see Figure 1) and illustrated how each specific technology would be deployed in that environment. A short explanation was then given to demonstrate how each sensor collected and processed information. We note that the order in which technologies were presented in these videos was dictated by a 3x3 Latin Square (see "Participants, Calibration, and Counterbalance," below). We believe that these videos were important to ensure that our survey respondents all had the same understanding of not only the technologies' capabilities, but also the context in which they were deployed and used. The video for the C-A-M ordering condition can be found online[5]; the other videos are identical, modulo technology ordering.

4.3 Survey Questions

Our survey contained a mix of free-form and Likert rating questions. Questions were organized so that participants were asked to give their opinion and sentiment for each of the technologies (C, A, and M) across the various contexts of use (PO, CW, CS, and B). This provided an in-depth understanding across various dimensions, which included:

- Comfort with each technology and specific context of use
- Differences in comfort with the technology across contexts of use
- Differences in comfort with the technology when sensed data may be stored for historical or archival purposes
- Differences in comfort with the technology as a factor of respondents' overall privacy concerns
- Expectation of notification and/or awareness that technologies are deployed and in use
- Differences in notification and/or awareness preferences across contexts of use

A copy of our survey instrument (ordered for the C-A-M condition) is available in the Appendix.

4.4 Interviews

For a subset of survey participants, we conducted follow up in-person interviews. To ensure that responses were still fresh in the minds of participants, these interviews were conducted within 24 hours of the survey being completed. The format of the interview generally followed a process of reviewing responses with participants, and then asking them to verbally provide a rationale or explanation for their rating. Through these interviews, we were able to a gain an even deeper, more contextual explanation for what motivated users concerns and preferences.

4.5 Participants, Calibration, and Counterbalance

Participants who only participated in the survey were recruited using the internal Amazon Mechanical Turk worker solicitation tools. Workers were restricted to being from the United States and over the age of 18. A total of 240 participants participated in the survey, which was conducted over a two day period in the spring of 2015. 50% were female. We did not collect absolute age of participants, but had them respond based on range: 15.4% 18-24, 32.9% 25-34, 26.3% 35-44, 15.4% 45-54, 8.8% 55-64, 1.3% 65+. Education level was also diverse; 11.3% high school or less, 10.0% attended college but no degree, 6.6% attended trade schools or programs, 10.4% earned associate degree, 35.8% bachelors, 7.1% masters, 2.0% professional degree, and 0.4% doctorate. Upon competition of the survey, participants received $1.

Nine of these participants were recruited using convenience sampling using organizational-level email solicitations in two organizations: a computer science department and a corporate research laboratory, both of which have sensor deployments to support the use of awareness systems by employees. These participants participated in the survey and follow-up interviews. The average interview time was 15:06 (SD=3:04). The age distribution for this group was comparable to the broader group, 22.2% 18-24, 55.5% 25-34, 11.1% 35-44, 11.1% 55-64. Given the additional time commitment of participating in the follow-up interview, these participants received $5 compensation.

All participants also completed a qualitative rating survey [25], categorizing them on Westin's three-level privacy sensitivity scale [1]. Across all participants, 29.6% categorized as Privacy Fundamentalists, 67.9% Privacy Pragmatists, and 2.5% Privacy Unconcerned. Compared to prior large population privacy studies (e.g., [25]), this distribution is similar except for a slightly lower than normal proportion of Privacy Unconcerned individuals. This difference is likely attributed to two factors. First, past research has shown that Mechanical Turk workers trend more privacy conscious than the broader population [26]. Second, during the time that the survey was administered, the United States NSA phone tapping and tracking activities were popular national news. We, however, believe this population to still be valid and representative, given the nature

[5] http://bit.ly/1R36Ldu

of our investigation. Higher attention and interest to privacy concerns will likely lead to more articulate and detailed explanations in survey responses.

To prevent ordering bias, the presentation of the technologies and the ordering of the scenarios of use considered were counterbalanced. At the beginning of the survey, the ordering of technologies described in the short introductory video was counterbalanced using a 3x3 Latin Square. For each participant, the ordering of technologies in their video was preserved through all of the context of use scenario questions. The ordering of the four context of use scenarios was randomized using mechanisms in the Qualtrics survey software[6]. In our analysis, we checked for ordering effect on all responses. No significant differences were found, and we do not report on this further.

5 RESULTS

From our broad survey, we found several consistencies in the responses across the variety of technologies and scenarios of use that were investigated. An unsurprising, but important, high-level result showed that comfort ratings were neutral to slightly negative as a whole. Specifically, collapsing across use and scenario conditions, the mean comfort score was 2.87 (SD=1.43, n=2880) on a 5-point scale ranging from very uncomfortable (1) to very comfortable (5), with a neutral condition (3).

Demographics, specifically the respondents' gender, age, and education level did not have a significant effect on comfort rating. While not significant (p=0.060), the data showed a small, negative trend between level of education and comfort rating. That is, respondents with higher levels of education trended lower in their ratings.

Also, perhaps as expected, we found that the Westin Privacy response had significant impact on comfort ratings ($F(2,237)=10.999$, $p<0.0001$, participant as random effect). A post hoc Tukey HSD test (α=0.050, Q=2.359) revealed significance between each Westin category. Privacy fundamentalists were most concerned (M=2.56, SD=0.11), followed by pragmatists (M=2.95, SD=0.07) and unconcerned (M=4.13, SD=0.36).

A two-way ANOVA was performed with scenario and technology as independent variables and participant as a random effect. Technology ($F(2,2629)=489.312$, $p<0.001$) and scenario ($F(3,2629)=48.677$, $p<0.001$) both had main effects. Interaction was just short of significance ($F(6,2629)=2.061$, $p=0.0546$). In short, technology and scenario both showed significant differences, when accounting for participant variance. That is, it is not the case that one explains the outcome of the other, it is likely these two factors contribute uniquely to a person's privacy concerns. Thus, in this investigation, we look at both factors in detail.

To better situate the results, we organize further analysis of the main effects within broader categorizations of our findings, including context provided by the qualitative measures.

5.1 Sensor Fidelity Matters

As the above main effect indicates, technology had a large and significant impact on participants' ratings of comfort. A post hoc Tukey HSD test (α=0.050, Q=2.345) revealed significance across all technologies. Microphone was rated lowest (M=2.42, SD=0.06). Followed closely, but significantly different from, camera (M=2.53, SD=0.06). Motion sensors, interestingly, were rated *above* neutral (M=3.64, SD=0.06).

Participants were asked in the survey to provide explanation for each of their comfort ratings. This qualitative channel provided some context for the difference in ratings. Many indicated that a large amount of discomfort with microphones and cameras stemmed from the fact that they captured data that could reveal a person's identity. As one participant stated, *"I would be uncomfortable with any technology that would collect and/or store any information that is identifiable or traceable back to any specific person."* This person further explains, *"I'm comfortable with the motion sensor because there is no identifying information tied to it other than simply motion was detected or not."*

While similar, others expressed discomfort because microphones and cameras could detect actions. For instance, one participant stated, *"I tend to talk to myself when I'm alone, I may say inappropriate things out loud that [could be captured]."* Similarly, another participant noted, *"Maybe [if] I fall asleep and snore briefly. Maybe I'm overwhelmed and sit and rest my head as I pull together from a busy task. This can be [captured] and taken out of context."*

5.2 Personal vs. Professional Personas

Scenario was also observed to have a main effect on participants' comfort ratings. A post hoc Tukey HSD test (α=0.050, Q=2.571) revealed significance across all scenarios. Personal office (PO) was rated lowest (M=2.61, SD=0.06). Followed by colleague's office for social interactions (CS) (M=2.74, SD=0.06), colleague's office for work (CW) (M=2.95, SD=0.06), and external business as a customer (B) (M=3.17, SD=0.06).

While scenarios were significantly different from each other, the quantitative results revealed that participants were less comfortable with the presence of sensing technology when the space was being used for personal or non-professional activities. In contrast, for true work-related interactions, the concerns were more neutral.

This observation also emerged in the qualitative data. One participant articulated his comfort ratings in this way: *"It would depend on how intimate and private of a situation I would be facing. If I were talking about something personal, I would need more privacy."* Many participants were very direct about the personal interactions that concerned them the most: family. For instance, one participant stated *"Personal visits from family/friends are more private and demand greater protections, making these technologies more intrusive."* Another stated, *"If I have my friend or family visiting, presence of these technologies would be considered like personal invasion, espionage."*

5.3 Content and Context

Despite not having a true statistical interaction, there are aspects of the data that point to an interesting relationship between scenario and technology. In line with a weak interaction effect, we found that despite the overall comfort scores across scenarios being significantly different (as noted above), the variance of comfort scores within a particular scenario are quite similar (SD=1.44, 1.40, 1.42,

[6]http://www.qualtrics.com/

1.37, for PO, CW, CS, and B scenarios, respectively). Indeed the differences between the highest rated technology (motion) and lowest (audio) have similar mean distances across all scenarios (1.26, 1.24, 1.22, 1.18, for PO, CW, CS, and B, respectively). That is, the spread of comfort ratings across technologies was consistent across scenarios, but not the means (overall, or individually by technology).

It is likely that this result emerges based on the influence that a scenario has on the type of conversations and interactions that occur within it. For instance, the higher comfort with all technologies in the external business scenario is likely the result of participants believing they are less likely to have sensitive interactions within these spaces. As one participant stated, *"an office is a setting where professionalism is always the expectation."* Another participant was even more explicit, stating *"Whether I was visiting the CEO or another associate at the same level as myself I wouldn't be bothered by these technologies. When a person is at work all interactions should be professional."*

In contrast, not all participants expressed this relationship. For instance one participant stated, *"It matters not the office of the person I am visiting. What matters is the purpose of the visit."* Another expressed, *"It depends on what kind of meeting it is and what kind of conversation we're going to have."*

5.4 History Matters

When asked about their overall comfort when sensing technologies are used in situations where information would be kept for historical use, participants' overall comfort ratings (collapsed across scenarios and technologies) were lower (M=2.40, SD=1.08, n=2880) compared to the mean comfort score reported above. A paired t-test (with user as grouping) showed a significant difference (paired t(2879)=-23.9615, p<0.0001). That is, across the board, historical use of sensor data negatively impacted users' comfort.

We saw a similar pattern in the regression tests on comfort ratings for historical use as we did for the question where historical use was not identified in the question, albeit with lower means. We conducted a two-way ANOVA with scenario and technology as independent variables, and participant as a random effect. A main effect was observed for technology (F(2,2629)=247.621, p<0.0001) and scenario (F(3,2629)=30.566, p<0.0001). No interaction effect was observed.

A post hoc Tukey HSD test (α=0.050, Q=2.345) showed significant differences between motion sensor (M=2.83, SD=0.05) and the other technologies. Interestingly no difference existed between audio (M=2.18, SD=0.05) and camera (M=2.20, SD=0.05). Similarly a post hoc Tukey HSD test (α=0.050, Q=2.571) showed a significant difference between the external business (B) scenario (M=2.59, SD=0.05) and other scenarios, a difference between colleague's office for work interaction (CW) (M=2.45, SD=0.05) and other scenarios, but no difference between colleague's office for social interaction (CS) (M=2.28, SD=0.05) and personal offices (PO) (M=2.28, SD=0.05).

Over all of these statistics, the means are all below the neutral mark. Further, the post hoc comparisons show less contrast between technologies and scenarios. These result suggest that historical use of data likely eliminates any neutral to mild comfort participants could have with any workplace sensing deployment. This is overwhelming supported by the qualitative feedback as well. One user

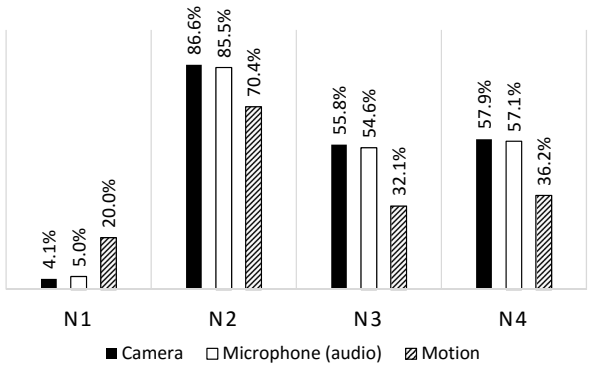


Figure 3: Agreement rates for N1–N4.

stated, that if the data *"was being collected then there is a possibility it could be used in the future, that makes me uncomfortable."* Similarly, another stated *"the amount of social interaction could be tracked [over time] and used to judge me negatively as being idle."* One participant stated *"… [historical] camera data scares me, images can be fatal to careers."*

5.5 Benevolent Sensing

Finally, we wanted to understand whether participants harbored any expectation that notifications should be provided if these types of technologies were in use in their own workplace, or in workplaces that they visited. For each of the three sensing technologies, participants were asked for binary agreement with each of the following statements:

- **N1:** No notification necessary for [cameras, microphones, motion sensors]
- **N2:** Signs in the space indicating [cameras, microphones, motion sensors] are in use
- **N3:** Signs indicating the position of [cameras, microphones, motion sensors] in the space
- **N4:** Light or other indicator that the [camera, microphone, motion sensor] was current in active use

In addition, the participants were given an "other" option in which they could fill their own statement regarding notification. A free form section was also provided to allow participants to explain or summarize their agreement ratings across all the technologies. A summary of our results is shown in Figure 3.

In relation to overall comfort scores, it was not surprising that very few participants agreed with N1 (No notifications necessary). Only 4.1% and 5.0% of respondents felt that no notification was necessary for camera and microphone sensors, respectively. 20.8% of participants indicated no notification was necessary for motion sensors, perhaps a reflection of their greater overall comfort with this sensor technology. The difference across technologies was significant (F(2,478)=36.430, p<0.0001). Post hoc Tukey HSD (α=0.050) revealed motion sensors were significantly different from camera and microphone. No other differences were observed.

Agreement with N2 (Signs) was very high for camera (86.6%) and microphone (85.8%). Motion sensors had comparatively lower

agreement at (70.4%). The difference across technologies was significant ($F(2,478)=26.699$, $p<0.0001$) and post hoc Tukey HSD ($\alpha=0.050$) showed the difference between motion and the other technologies was significant.

With respect to N3 (Position indicators), 55.8%, 54.6%, and 32.1% of participants agreed for camera, microphone, and motion sensors, respectively. The result was significant across technologies ($F(2,478)=44.464$, $p<0.0001$) with post hoc Tukey HSD ($\alpha=0.050$) showing significance between motion and other sensors. N4 (Lights or other indicators) followed a similar pattern, with 57.9%, 57.1% and 36.2% agreement for camera, microphone, and motion sensors, respectively (also significant $F(2,478)=34.972$ $p<0.0001$ across technologies with post hoc significant between motion and other sensors).

Qualitative feedback from participants provided a very clear concern to inform suspecting colleagues and visiting family. Comments from participants capturing this sentiment included statements like *"I would want to make sure that the individual in the office is aware of the presence of these devices."*; *"I feel the person visiting me would feel uncomfortable, and that in turn would make me feel uncomfortable."*; and *"I would like to know it was there when visiting any office. I feel like I am ok with this but think there should be a way to make sure people know these things are there."*

6 DISCUSSION AND IMPLICATIONS

We now reflect upon and interpret our findings in the context of designing more effective workplace sensing technologies and mechanisms for enforcing user preferences in a trusted manner.

6.1 Design for Assurance

The neutral to mildly positive valence for individual comfort with the PIR sensors across contexts of use is a potential indicator that unease with sensing in the workplace is not due to the deployment of presence systems in general, but rather with the specific sensing technologies deployed to support presence detection. For instance, when discussing the audio sensor, one interviewee noted *"... when you tell me that it's only 1 or 0 that's being uploaded from the microphone [indicating conversation], I wouldn't believe you."*, indicating doubts that sensed environmental data may actually be stored or misused by the sensor.

To explore this notion further, we asked interviewees more directly about their perceived trust of a hypothetical "unhackable" sensor that carried out image or audio processing within a trusted component and emitted only a presence state. Across the board, individuals reported that such a sensor would cause them to rethink their comfort with camera- and audio-based sensors. As one individual responded when asked about the value of this potential technology in her interview, *"... it would be a nice thing to do to increase peoples' trust in the system"*. This qualitative result combined with individuals' quantitative preference for PIR sensing as a technology, indicate two promising approaches toward designing sensor systems that provide individuals with high assurances regarding the privacy of their actions within a space: securing sensor components themselves, and further exploring the use of low-fidelity sensors.

While "unhackable" sensors may not be technically feasible, steps can be taken to design inexpensive sensor packages that make surreptitious access to the environmental inputs used to derive presence states markedly more difficult. For example, our camera-based sensor currently processes the video feeds from two webcams on a Raspberry Pi v2 single-board computer, transmitting the derived presence state to our awareness system via a USB WiFi adapter. An alternate—and only marginally more expensive—approach to this would be to remove the WiFi adapter, and instead leverage an output-only pin on the Raspberry Pi as a makeshift data diode that transmits computed presence states to a Bluetooth or WiFi system-on-a-chip (e.g., Electric Imp[7]). This SoC can handle relaying presence states to our awareness system, without having the ability to, itself, access raw environmental data. Such an architectural shift on the sensor side would make unauthorized access to raw environmental data much more difficult—likely requiring physical access to the sensor—and perhaps increase individuals' comfort with sensing technologies that are typically viewed as invasive.

A second approach worth studying is the design of other low-fidelity sensor packages for common presence sensing tasks. For instance, ultrasonic ingress/egress counters could be useful for spaces with clearly demarcated entrances or exits. Similarly, force sensing resistors could be used to instrument chairs in meeting spaces or common areas to register when individuals are using the space. Given the potential for privacy harm related to high-fidelity sensors that was noted by the individuals that we surveyed, the onus is on system designers to consider these less invasive—and often inexpensive—alternatives to rich sensing modalities like image processing.

6.2 Locality of Control

One possible explanation for the noted decrease in comfort with sensed data being stored for historical use, as well as the use of higher-fidelity sensing modalities (i.e., camera and audio), could be a perceived loss of control by individuals as they are monitored by these systems. This is reflected by many of the participant quotes in the "Personal vs. Professional Personas," "Content and Context," and "History Matters" subsections of the Results section.

As historical information has been shown to be a useful feature of awareness systems [2, 33], it would be worthwhile to explore the impacts that "opt in" policies for historical data collection and/or the ability for an individual to edit the historical information stored about them may have on individuals' comfort with these features. Similarly, it could be useful to provide users with the ability to temporarily shut off awareness sensors in response to their personal determination of a private context (e.g., having a sensitive discussion or a visit from a family member). Providing individuals with some (perhaps time- or task-limited) measure of control over *when* they are sensed may enable the use of higher fidelity sensing in certain situations, without impinging on individuals' comfort with their participation in an awareness system.

[7] https://www.electricimp.com/

6.3 Mixed Method Deployments

In the specific context of workplace sensing, our investigation of sensing modalities and survey findings indicate that a one-size-fits-all solution to the problem of deploying a highly-effective presence system that maximizes individual comfort across contexts is unlikely to exist. For instance, the PIR sensor package was shown to elicit the highest level of comfort from survey participants, as well as perform well in an office environment. This type of environment is often largely static, however, with individuals having seated discussions or working collaboratively using whiteboards within relatively small sensing zones. We expect that these types of sensors would perform poorly in environments where motion across large areas—and thus multiple sensing zones—is typical (e.g., kitchens or break rooms). By contrast, camera-based sensors handle motion well, but come at the cost of being a significantly more invasive technologies.

One potential solution to this problem that is worth investigating is the use of mixed method sensor deployments. Rather than relying on a homogeneous sensor deployment throughout an organization, the particular sensors deployed could be chosen to balance accuracy and comfort. For instance, PIR sensors would be reasonable to deploy in personal office spaces or small meeting rooms in which individual motion is typically limited and sensitive or personal topics may be discussed. Meanwhile, camera-based sensors could be used in common areas or larger meeting spaces where individuals are perhaps more mobile, but would likely have lower expectations of privacy, as supported by our findings. Such a deployment would allow system designers to balance the overall accuracy of the data used by the presence system system with the per-space privacy concerns of the individuals occupying these spaces.

6.4 Study Limitations

One limitation of our study is that we considered a single sensing problem within the broader context of workplace awareness, and a small set of sensing technologies for addressing this problem. This was an intentional choice, made to keep our survey short (≈10 minutes on average) and to allow respondents to give deeper attention to a specific problem, rather than considering "monitoring" in general. However, it would be worthwhile to explore individuals' sentiments towards other sensing tasks in the workplace, as well develop a deeper understanding of how a broader class of sensing technologies (including those noted above) impact individuals' perceptions of privacy loss.

Another limitation of our study is our use of Amazon Mechanical Turk for the recruitment of survey respondents. It has been shown that Mechanical Turk workers tend to be more privacy conscious than the general public [26], a fact that is reflected in the distribution of Westin scores reported on previously. However, there are also two potential strengths to soliciting more privacy-conscious respondents for this study. First, these individuals are likely to have more well-defined mental models of privacy, which could lead to more authentic responses to our hypothetical contexts of use. Second, this allows us to effectively lower-bound the comfort with these technologies that we would expect to see in a survey of the general population. For instance, that a more privacy-conscious population expresses a positive valence for comfort with low-fidelity sensing provides strong justification for further pursuing the use of these types of technologies in workplace awareness systems. Nonetheless, a broader survey of the general public would enhance our findings, and make for interesting future work.

7 CONCLUSIONS

Embedded sensors are here to stay: IoT devices, wearable computers, smartphones, and instrumented smart spaces have revolutionized the ways that people learn about themselves, interact with others, and manage spaces. Despite the benefits of these technologies, pervasive sensing has the potential for privacy harms if the collection, analysis, and dissemination of data is left unchecked. In the rush to maximize productivity and utility, this cannot be overlooked. To this end, we investigated the accuracy and comfort trade-offs that exist in common space contextualization tasks leveraged by workplace awareness systems in an effort to uncover design recommendations for sensing systems that provide users with a sense of agency when in instrumented spaces.

We surveyed and interviewed individuals to examine their comfort with sensors designed to use three sensing modalities often deployed in workplace environments (video, audio, and motion) across a variety of workplace contexts. Across all contexts, sensor fidelity and a sensor's ability to capture ancillary context were found to have a significant impact on user comfort with awareness technologies. In fact, the use of low-fidelity PIR sensors was associated with neutral to mildly positive comfort ratings, while higher fidelity sensors—which are more likely to capture private contexts—were associated with negative comfort ratings. This indicates that discomfort with awareness technologies may have less to do with specific sensing tasks, and more to do with the means by which these tasks are carried out.

Our findings signal an important message to researchers and developers in the access control space: the exploration of access control enforcement mechanisms that do not rely on a trusted reference monitor are of increasing importance as the amount of personal data processed by third-party and/or untrusted infrastructure increases. To this end, our qualitative findings show that individuals are significantly more comfortable with low-fidelity sensors in situations where raw sensed data could be accessible to the platform. Further, our qualitative findings indicate that users would be reasonably comfortable with high-fidelity sensors like camera-based platforms if they could be provided with strong assurances that only derived states (e.g., occupancy count) and not raw data (e.g., images) would be exposed to the broader platform, for instance via hardware isolation mechanisms. Given the increasing prevalence of instrumented spaces, incorporating these insights into the design of flexible sensor packages that isolate sensitive data from derived information will be instrumental in increasing the utility that can be derived from these spaces without overly impinging upon user privacy and agency.

Acknowledgments. This work was supported in part by the National Science Foundation under award no. CNS–1253204.

A SURVEY QUESTIONS (C-A-M ORDERING)

Introduction. Please watch the following short (2 minute) video further explaining how specific presence detection technologies may be deployed within a workspace.

[The video for the C-A-M ordering can be viewed at http://bit.ly/1R36Ldu.]

Personal Office. You work in a workspace where each worker has his/her own office, and a presence system is in use to help facilitate person-to-person communication within the workplace. Consider the use of these technologies **within your own personal office**.

- **Q1.** How comfortable are you with **camera sensors** being used for this specific context of use?
  - Very uncomfortable
  - Somewhat uncomfortable
  - Neutral
  - Somewhat comfortable
  - Very comfortable
- **Q2.** How comfortable are you with **microphone sensors** being used for this specific context of use?
  - Very uncomfortable
  - Somewhat uncomfortable
  - Neutral
  - Somewhat comfortable
  - Very comfortable
- **Q3.** How comfortable are you with **motion sensors** being used for this specific context of use?
  - Very uncomfortable
  - Somewhat uncomfortable
  - Neutral
  - Somewhat comfortable
  - Very comfortable
- **Q4.** In addition to using the sensed **camera data** (e.g., images) for determining current presence state, this data **may also be stored for historical or archival purposes**. Would this use change your comfort with a particular technology?
  - Very negatively
  - Somewhat negatively
  - Neutral
  - Somewhat positively
  - Very positively
- **Q5.** In addition to using the sensed **microphone data** (e.g., audio snippets) for determining current presence state, this data **may also be stored for historical or archival purposes**. Would this use change your comfort with a particular technology?
  - Very negatively
  - Somewhat negatively
  - Neutral
  - Somewhat positively
  - Very positively
- **Q6.** In addition to using the sensed **motion sensor data** (e.g., on/off readings for each sensor) for determining current presence state, this data **may also be stored for historical or archival purposes**. Would this use change your comfort with a particular technology?
  - Very negatively
  - Somewhat negatively
  - Neutral
  - Somewhat positively
  - Very positively
- Would your opinion about these technologies change depending on the **person visiting your office**? For instance, whether this person is a colleague, outside customer, friend or family? If so, please explain.
  - *[Free text input box]*

Colleague's Office (Work). You work in a workspace where each worker has his/her own office, and a presence system is in use to help facilitate person-to-person communication within the workplace. Consider the use of these technologies while you are **visiting a colleague's office to attend a work-related meeting**.

- *[Repeat questions **Q1–Q6**.]*
- Would your opinion about these technologies change depending on the **person whose office you were visiting**? If so, please explain.
  - *[Free text input box]*

Colleague's Office (Social). You work in a workspace where each worker has his/her own office, and a presence system is in use to help facilitate person-to-person communication within the workplace. Consider the use of these technologies while you are **visiting a colleagueâĂŹs office for the purpose of a brief social interaction**.

- *[Repeat questions **Q1–Q6**.]*
- Would your opinion about these technologies change depending on the **person whose office you were visiting**? If so, please explain.
  - *[Free text input box]*

Visiting a Business. Consider the scenario in which you are **visiting a place that you do business with (e.g., a bank or insurance office)**, and a presence system is in use to manage the distribution of incoming clients to representatives of the business. Consider the use of these technologies while you meet with a representative in his/her personal office.

- *[Repeat questions **Q1–Q6**.]*
- Would your opinion about these technologies change depending on the **type of business you were visiting**? If so, please explain.
  - *[Free text input box]*

Notifications.

- Do you feel that workspaces outfitted with presence sensing technologies should provide notification to individuals who may be monitored by these systems?
  - Yes
  - No
- Please select all notifications that you feel are appropriate if **camera sensors** are deployed.
  - No notification is necessary
  - Signs indicating the use of cameras
  - Clear indications of camera positions
  - Lights or other indicators of "record" status
  - Other (please specify)

- Please select all notifications that you feel are appropriate if **microphone sensors** are deployed.
  - No notification is necessary
  - Signs indicating the use of microphones
  - Clear indications of microphone positions
  - Lights or other indicators of "record" status
  - Other (please specify)
- Please select all notifications that you feel are appropriate if **motion sensors** are deployed.
  - No notification is necessary
  - Signs indicating the use of motion sensing technologies
  - Clear indications of motion sensor positions
  - Lights or other indicators of whether sensors are active
  - Other (please specify)

REFERENCES

[1] Privacy on and off the internet: What consumers want. Technical Report 15229, Harris Interactive, Feb. 2002. http://www.ijsselsteijn.nl/slides/Harris.pdf.

[2] J. Begole, J. C. Tang, R. B. Smith, and N. Yankelovich. Work rhythms: analyzing visualizations of awareness histories of distributed groups. In *Proceeding of the ACM Conference on Computer Supported Cooperative Work (CSCW)*, pages 334–343, 2002.

[3] P. Bellavista, A. Küpper, and S. Helal. Location-based services: Back to the future. *IEEE Pervasive Computing*, 7(2):85–89, 2008.

[4] V. Bellotti and A. Sellen. Design for privacy in ubiquitous computing environments. In *Proceedings of the Third Conference on European Conference on Computer-Supported Cooperative Work*, ECSCW'93, pages 77–92, 1993.

[5] J. T. Biehl, A. J. Lee, G. Filby, and M. Cooper. You're where? prove it!: towards trusted indoor location estimation of mobile devices. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 909–919, 2015.

[6] J. T. Biehl, E. G. Rieffel, and A. J. Lee. When privacy and utility are in harmony: towards better design of presence technologies. *Personal and Ubiquitous Computing*, 17(3):503–518, 2013.

[7] J. J. Cadiz, G. Venolia, G. Jancke, and A. Gupta. Designing and deploying an information awareness interface. In *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work*, CSCW '02, pages 314–323, 2002.

[8] E. K. Choe, S. Consolvo, J. Jung, B. L. Harrison, and J. A. Kientz. Living in a glass house: a survey of private moments in the home. In *13th International Conference on Ubiquitous Computing (UbiComp)*, pages 41–44, 2011.

[9] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the 2005 Conference on Human Factors in Computing Systems (CHI)*, pages 81–90, 2005.

[10] A. K. Dey. *Providing Architectural Support for Building Context-Aware Applications*. PhD thesis, College of Computing, Georgia Institute of Technology, Dec. 2000.

[11] P. Dourish and S. A. Bly. Portholes: Supporting awareness in a distributed work group. In *Conference on Human Factors in Computing Systems (CHI)*, pages 541–547, 1992.

[12] N. B. Ellison, J. Vitak, C. Steinfield, R. Gray, and C. Lampe. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy Online - Perspectives on Privacy and Self-Disclosure in the Social Web.*, pages 19–32. 2011.

[13] M. Fan, Q. Liu, H. Tang, and P. Chiu. Hifi: Hide and find digital content associated with physical objects via coded light. In *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, HotMobile '14, pages 6:1–6:6, 2014.

[14] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th International Conference on World Wide Web, WWW 2010, Raleigh, North Carolina, USA, April 26-30, 2010*, pages 351–360, 2010.

[15] J. Fogarty, C. Au, and S. E. Hudson. Sensing from the basement: a feasibility study of unobtrusive and low-cost home activity recognition. In *Proceedings of the 19th Annual ACM Symposium on User Interface Software and Technology (UIST)*, pages 91–100, 2006.

[16] J. Fogarty, J. Lai, and J. Christensen. Presence versus availability: the design and evaluation of a context-aware communication client. *International Journal of Humam-Computer Studies*, 61(3):299–317, 2004.

[17] Y. L. Gall, A. J. Lee, and A. Kapadia. Plexc: a policy language for exposure control. In *17th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 219–228, 2012.

[18] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster. The anatomy of a context-aware application. *Wireless Networks*, 8(2/3):187–197, 2002.

[19] U. Hengartner and P. Steenkiste. Protecting access to people location information. In *Proceedings of the First International Conference on Security in Pervasive Computing*, pages 25–38, Boppard, Germany, Mar. 2003.

[20] J. Hightower, R. Want, and G. Borriello. Spoton: An indoor 3d location sensing technology based on rf signal strength. Technical Report UW CSE 00-02-02, University of Washington, Department of Computer Science and Engineering, 2000.

[21] J. D. Hincapié-Ramos, S. Voida, and G. Mark. A design space analysis of availability-sharing systems. In *Proceedings of the 24th Annual ACM Symposium on User Interface Software and Technology (UIST)*, pages 85–96, 2011.

[22] J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of MobiSys 2004*, pages 177–189, June 2004.

[23] G. Hsieh, K. P. Tang, W. Y. Low, and J. I. Hong. Field deployment of *IMBuddy* : A study of privacy control and feedback mechanisms for contextual IM. In *9th International Conference on Ubiquitous Computing (UbiComp)*, pages 91–108, 2007.

[24] G. Iachello and J. I. Hong. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1(1):1–137, 2007.

[25] C. Jensen, C. Potts, and C. Jensen. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1–2):203 – 227, 2005.

[26] R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of Mechanical Turk workers and the U.S. public. In *Symposium On Usable Privacy and Security*, pages 37–49, July 2014.

[27] C. D. Kidd, R. J. Orr, G. D. Abowd, C. G. Atkeson, I. A. Essa, B. MacIntyre, E. D. Mynatt, T. Starner, and W. Newstetter. The aware home: A living laboratory for ubiquitous computing research. In *The Second International Workshop on Cooperative Buildings, Integrating Information, Organization, and Architecture (CoBuild)*, pages 191–198, 1999.

[28] J. C. Lai, A. Levas, P. B. Chou, C. S. Pinhanez, and M. S. Viveros. Bluespace: personalizing workspace through awareness and adaptability. *International Journal of Humam-Computer Studies*, 57(5):415–428, 2002.

[29] S. Lederer, J. Mankoff, and A. K. Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *Extended abstracts of the 2003 Conference on Human Factors in Computing Systems (CHI)*, pages 724–725, 2003.

[30] S. Patil, Y. L. Gall, A. J. Lee, and A. Kapadia. My privacy policy: Exploring end-user specification of free-form location access rules. In *Financial Cryptography and Data Security (FC) Workshops*, pages 86–97, 2012.

[31] S. Patil and A. Kobsa. Privacy considerations in awareness systems: Designing with privacy in mind. In *Awareness Systems - Advances in Theory, Methodology and Design*, pages 187–206. 2009.

[32] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Symposium On Usable Privacy and Security (SOUPS)*, page 5, 2012.

[33] M. C. Reddy and P. Dourish. A finger on the pulse: temporal rhythms and information seeking in medical work. In *Proceeding of the ACM Conference on Computer Supported Cooperative Work (CSCW)*, pages 344–353, 2002.

[34] N. Romero, G. McEwan, and S. Greenberg. A field study of community bar: (mis)-matches between theory and practice. In *Proceedings of the 2007 International ACM Conference on Supporting Group Work*, GROUP '07, pages 89–98, 2007.

[35] N. M. Sadeh, J. I. Hong, L. F. Cranor, I. Fette, P. G. Kelley, M. K. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[36] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[37] R. Schlegel, A. Kapadia, and A. J. Lee. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *Proceedings of the 2011 Symposium on Usable Privacy and Security (SOUPS)*, pages 14:1–14:14, July 2011.

[38] I. Simpson. Maryland prisons official fired for facebook joke about being groped, Feb. 2015. http://www.huffingtonpost.com/2015/02/20/maryland-prisons-official_n_6722366.html (Accessed 09/19/2016).

[39] B. Smallwood. Parents and oversharing on social media, May 2015. http://wivb.com/2015/05/19/parents-and-oversharing-on-social-media/ (Accessed 09/19/2016).

[40] J. C. Tang, N. Yankelovich, J. Begole, M. V. Kleek, F. C. Li, and J. R. Bhalodia. Connexus to awarenex: extending awareness to mobile users. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 221–228, 2001.

[41] K. P. Tang, J. Lin, J. I. Hong, D. P. Siewiorek, and N. M. Sadeh. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. In *12th International Conference on Ubiquitous Computing (UbiComp)*, pages 85–94, 2010.

[42] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. Who's viewed you?: The impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2003–2012, New York, NY, USA, 2009.

[43] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. Cranor. Privacy nudges for social media: an exploratory Facebook study. In *WWW 2013 Companion*,

2013.

[44] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor. "I regretted the minute I pressed share": a qualitative study of regrets on facebook. In *Symposium On Usable Privacy and Security (SOUPS)*, page 10, 2011.

[45] R. Want, A. Hopper, V. Falcão, and J. Gibbons. The active badge location system. *ACM Trans. Inf. Syst.*, 10(1):91–102, Jan. 1992.

[46] J. Wiese, J. T. Biehl, T. Turner, W. van Melle, and A. Girgensohn. Beyond 'yesterday's tomorrow': towards the design of awareness technologies for the contemporary worker. In *Proceedings of the 13th Conference on Human-Computer Interaction with Mobile Devices and Services (Mobile HCI)*, pages 455–464, 2011.