Exploring Smart Commercial Building Occupants' Perceptions and Notification Preferences of Internet of Things Data Collection in the United States

Tu Le[1,2], Alan Wang[1], Yaxing Yao[3], Yuanyuan Feng[4], Arsalan Heydarian[1], Norman Sadeh[5], and Yuan Tian[1,2]

[1]University of Virginia
[2]University of California, Los Angeles
[3]University of Maryland, Baltimore County
[4]University of Vermont
[5]Carnegie Mellon University

***Abstract*—Data collection through the Internet of Things (IoT) devices, or smart devices, in commercial buildings enables possibilities for increased convenience and energy efficiency. However, such benefits face a large *perceptual* challenge when being implemented in practice, due to the different ways occupants working in the buildings understand and trust in the data collection. The semi-public, pervasive, and multi-modal nature of data collection in smart buildings points to the need to study occupants' understanding of data collection and notification preferences. We conduct an online study with 492 participants in the US who report working in smart commercial buildings regarding: 1) awareness and perception of data collection in smart commercial buildings, 2) privacy notification preferences, and 3) potential factors for privacy notification preferences. We find that around half of the participants are not fully aware of the data collection and use practices of IoT even though they notice the presence of IoT devices and sensors. We also discover many misunderstandings around different data practices. The majority of participants want to be notified of data practices in smart buildings, and they prefer push notifications to passive ones such as websites or physical signs. Surprisingly, mobile app notification, despite being a popular channel for smart homes, is the least preferred method for smart commercial buildings.**

***Index Terms*—data collection, notification, privacy, IoT, smart building, smart devices**

1. Introduction

The Internet of Things (IoT), or smart devices, have increasingly made their way into various physical environments, transitioning them into "smart environments". These smart devices have introduced significant benefits to users and society at large. Continuous monitoring of indoor environmental conditions and user behaviors in smart devices-equipped buildings can help reduce energy consumption as well as enhance users' comfort and well-being [3], [44]. For example, Lu et al. [29] shows that using sensors to intelligently control the home's heating, ventilation, and cooling (HVAC) system can achieve a 28% energy saving. Figueiro et al. also shows how properly applied light exposures can increase alertness and circadian entertainment [20].

Problem. Despite the numerous potential benefits of making environments "smarter", the transition may also introduce great challenges due to the potential privacy issues [28]. Continuous data collection can expose more data than anticipated by the users, and the collected data can be shared with third parties [13], [35]. One particular privacy issue in these environments relates to occupants' awareness of these smart devices and their data collection and use practices. Research has shown that occupants in smart environments have significant privacy concerns, yet the level of transparency regarding the data practices in smart environments and their ability to control these data practices are limited [23]. To increase the transparency of data practices and raise occupants' awareness of data practices in smart environments, research has proposed various mechanisms, such as notifications via mobile devices, network monitoring through web apps, ambient lights, and sounds, etc. [14], [19], [27], [33], [43]. However, prior research primarily focuses on smart homes, with less focus on other more public smart environments. Several key differences exist between managing privacy in homes versus commercial buildings, making smart building privacy notification a novel and challenging problem. First, in a home, the same people affected by the potential privacy invasions are mostly capable of changing or removing the offending devices. In contrast, in a commercial building, the occupants might be less aware of the data collection and might feel they are less in control of their privacy. Second, the occupants might have a different mental model when facing the commercial buildings' pervasive data collection compared to their own homes. Finally, smart building data collection is multi-modal, pervasive, and large-scale. The privacy notifications, if not well designed, will cause user apathy or misunderstanding. As a result, there is a need to comprehensively understand users' awareness, perceptions of data collection, and privacy notification preferences in the smart commercial building environment to inform the design of smart building privacy notifications.

Research Goal. In this paper, we focus on smart commercial buildings, an understudied yet important smart environment in the privacy literature. We use "smart commercial buildings" to denote commercial buildings that

are equipped with smart devices (e.g., Internet-connected security cameras) and sensors (e.g., smart water meters), and use "occupants" to denote people who work in or regularly enter these buildings. We aim to understand occupants' awareness of smart devices in these buildings, as well as their preferences in receiving notifications about smart devices and their associated data practices. Our scope focuses on occupants in the US.

Importance. This research is significant for two reasons. First, due to the nature of occupants' tasks and activities in smart commercial buildings, the privacy implications can be different from those in other environments, such as smart homes. Particularly, how to appropriately handle privacy notifications in smart buildings remains an open issue. In addition, existing techniques for maintaining privacy in other IoT environments such as smart homes are unlikely to apply in the smart building context. For example, the power dynamics in smart commercial buildings (e.g., employers vs. employees, administrators vs. tenants) may influence how occupants perceive privacy. Second, recent privacy regulations around the world have also mandated the disclosure of certain data collection practices in public places. For example, both the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) protect users' control over any personal information a business collects about them [11], [21], [22], [32]. As a result, it is important to understand occupants' privacy expectations and study their privacy notification preferences in smart commercial buildings. It is also timely for building owners to understand the mechanisms underlying privacy expectations and build a fiduciary relationship with their occupants.

Research Questions. In this paper, we aim to answer the following research questions:

- **RQ1:** What are the occupants' perceptions of data collection in smart commercial buildings?
- **RQ2:** What are the occupants' notification preferences for data collection in smart commercial buildings in different contexts?
- **RQ3:** What potential factors affect occupants' notification preferences for data collection in smart commercial buildings in different contexts?

Our Study. To answer these research questions, we conducted an online study of 492 participants in the US. Our participants are people who have worked in smart commercial buildings. We use the term *(smart) commercial building* throughout the paper to indicate our participants' indoor workplaces that deploy IoT devices/sensors other than their homes. In our study, we explored the participants' awareness and perception of data collection in the buildings and used a series of questions to identify whether they want to be notified on the different modalities of data collection, why or why not to be notified, what type of information should be communicated, and how they would like to receive these notifications. We design three hypothetical scenarios based on common IoT devices in smart buildings (i.e., Bluetooth beacons, cameras, smart meters) to ask about participants' privacy notification preferences.

Key Findings. Our results suggest that many participants are unaware of or have misunderstandings of the data collection in smart commercial buildings. Even participants who are highly confident about their knowledge of IoT devices, still have misunderstandings about data collection purposes and data access of smart devices in smart commercial buildings. For example, few people understood that Bluetooth beacon's data would be used for localization even though localization is in fact its primary data purpose. One participant even incorrectly assumed that Bluetooth beacon could get unauthorized access to his/her phone. In terms of their notification preferences, the majority of our participants (91%) indicated their willingness to receive notifications about the data practices regardless of their prior knowledge of smart devices. We also found that email was the most desired channel to deliver privacy-related notifications, while some participants preferred other channels (e.g., physical signs) depending on the scenarios. Our data helps us identify several factors that may impact our participants' notification preferences, such as their awareness of data collection and confidence in their knowledge of smart devices.

Contributions. This work contributes to privacy research and human-centered computing in several aspects:

- We provide a comprehensive user study to understand occupants' awareness and perceptions of data collection in smart commercial buildings, generating important empirical evidence in this area of research.
- Our study provides a systematic understanding of occupants' preferences for privacy notifications in smart commercial buildings and the potential factors that impact their preferences.
- We draw implications for designing a transparent data collection framework for future generations of smart commercial buildings.

Paper Outline. The rest of the paper is organized in the following way. We first introduce the related work in Section 2 and then explain the design of our user study in Section 3. We present our data analysis and results about the user study in Section 4. We then discuss the privacy law implications, the suggestions for improving smart building data collection transparency, the limitations of our study, the potential future work in Section 5, and conclude the study in the end.

2. Related Work

This section discusses the previous work and how our work is different. The related work is presented as three themes: IoT in Smart Buildings, IoT Privacy, and Privacy Notifications for IoT.

2.1. IoT in Smart Buildings

While there are many types of sensors deployed in buildings to collect information about the occupant and the surrounding environment, our study mainly focuses on the three types of smart devices that are popular and have been demonstrated to be privacy-invasive, i.e., Bluetooth beacons, cameras, and smart meters.

For Bluetooth beacons, Caesar et al. [7] demonstrated that Bluetooth technology can be used maliciously to track occupant location. For example, a smartphone can be used to secretly monitor nearby Bluetooth Mesh activity and reference user location through transmissions, or an app

installed on smartphones can be used to track a user within a Bluetooth Mesh network.

For cameras, besides being able to identify users directly, cameras also reveal information that might be difficult or impossible to detect with the naked eye. For example, Davis et al. [15] showed that audio signals could be extracted through motion magnification of video data. The same motion magnification technique has also been shown to be able to extract health-related information from users such as blood circulation [38].

For smart energy meters, Jazizadeh et al. [25] demonstrated how Non-Intrusive Load Monitoring (NILM), or measuring electricity consumption using an energy meter at the circuit level instead of the appliance level, can still be disaggregated to extract signals of specific appliance use in households and occupant behaviors. Although network communications among IoT devices can be encrypted to ensure privacy, Acar et al. [2] showed that an adversary can exfiltrate sensitive data from the encrypted traffic. Rondon et al. [36], [37] demonstrated different attacks on different layers of enterprise IoT systems in smart buildings.

Besides, Babun et al. [1] provided an analysis of popular IoT platforms in terms of how they handle vulnerabilities and possible solutions for these platforms. Our work focuses on the occupants' perspectives on IoT devices and their data collection in smart buildings.

2.2. IoT Privacy

There has been considerable literature investigating the privacy preferences and factors that affect users' privacy decision-making in IoT scenarios. Yao et al. [46], [47] conducted co-design studies to identify key factors for designing smart home privacy controls. In a broader context, Naeini et al. [30] showed that participants were more comfortable with data collection in public rather than private settings and were more likely to share data for uses that they find beneficial (e.g., find public restrooms). The collection of biometric data is considered less comfortable than environmental data, and the participants wanted to be notified about the data practices of such information being collected. Different from these previous studies, we focus specifically on smart commercial building occupants rather than the general users and consider participants' background knowledge/confidence in IoT technology. We also explore more detailed perceptions regarding notification preferences and how occupants want to be informed of data collection. Via in situ studies, some previous work found users' privacy concerns or misunderstanding of the facial recognition technology [48], [49] and fitness tracker [42]. In particular, Zhang et al. [48], [49] studied people's notification preferences, including the frequency of notifications. However, they did not explore modality preferences such as emails versus mobile apps because people might not have an email address in the scenarios they considered. Harper et al. [23] conducted an online survey of 81 participants to understand their privacy concerns in the smart building context, focusing on environmental data collection. Our work considers a larger pool of participants, more types of smart devices, and occupants' preferences for different notification schemes.

Other work looked into the influence of friends and experts on privacy decisions [18]. These studies showed that participants were more influenced when their friends denied data collection than when their friends allowed data collection. In contrast, the participants were more influenced when experts allowed collection than when experts denied data collection. However, after being exposed to a set of scenarios in which friends and experts allowed or denied data collection, the participants were less likely to be influenced in subsequent scenarios. Barbosa et al. [6] presented machine learning models to predict personalized privacy preferences in smart homes and identify factors that could change such preferences.

Several frameworks were proposed to help users to enforce privacy protections on IoT devices. Apthorpe et al. [4] presented a framework to discover the privacy norms in the smart home context. IoTWatch [5] allows users to specify their privacy preferences at install time and ensure IoT apps' behaviors match the selections. Kratos [40] provides smart home users with access control settings that consider multiple users and devices in a shared space. Cejka et al. [8] presented potential countermeasures for privacy issues of smart meters. Wu et al. [45] proposed a privacy-preserving framework to support sensor applications such as occupancy detection while ensuring user privacy. In contrast, our work contributes new insights into smart building data collection from occupants' perspectives to support future designs of systems and frameworks.

2.3. Privacy Notifications for IoT

Privacy notifications are a type of privacy notice that informs people or users about the data being collected and using practices of a system, product, or service. They are often provided by entities responsible for the disclosed data practices (e.g., data collection, sharing, and processing), as increasing requirements by privacy regulations around the world (e.g., GDPR [11], CCPA [32]). Although privacy policies are the most common type of privacy notice, they are lengthy and difficult to read [12], [31]. Instead, researchers and practitioners have proposed more effective ways to notify people about data privacy practices, such as concise privacy notices [16] and privacy nutrition labels [17]. Moreover, Schaub et al. outlined a design space for more effective privacy notices [39].

User-facing privacy notifications, in addition to or in lieu of privacy policies, are very common in the digital world. For example, websites have increasingly adopted GDPR-compliant cookie banners, which automatically pop up when websites detect new users. These banners usually contain a concise privacy notification describing how the website uses cookies to track user data and how users can disable some of them [10]. Another common example is the app permission management framework on smartphones. Both iOS and Android platforms send users just-in-time notifications when apps are trying to access certain sensitive permission on smartphones, along with the choice to allow or deny. The notifications in both examples are delivered to users through primary channels, which is the same platform or device a user interacts with. Huang et al. [24] presented a tool that examines

network traffic in a smart home and informs the user of vulnerabilities or tracking services.

However, in IoT-embedded smart buildings, providing people with effective privacy notices is extremely challenging. First, since smart buildings have countless IoT devices and sensors collecting data (e.g., energy sensors, lighting, temperature, air quality, etc.), it is possible that the number of notifications can overwhelm building occupants and visitors. This may lead to privacy fatigue [9] if users receive too many irrelevant privacy notices. Second, IoT devices and sensors in smart buildings lack traditional user interfaces (e.g., screens), so it is difficult to deliver privacy notifications through the most intuitive primary channels (i.e., IoT devices and sensors themselves). This means privacy notices need to rely on secondary or public channels (e.g., a website, or physical signs), causing an additional barrier for residents or visitors to receive them. Researchers have recently developed a location-based mobile app, IoT Assistant, capable of notifying people about nearby IoT data privacy in public places [14], [19]. However, little research has examined what types of IoT privacy notices people would like to receive and how to receive them. Therefore, our study aims to understand people's notification preferences for smart building scenarios to inform the design of more effective privacy notices in smart buildings.

3. Methodology

Figure 1 shows an overview of our study workflow. We describe our study protocol in detail in this section. In this study, our survey design aims to investigate the awareness and perceptions of data collection (RQ1), the notification preferences (RQ2) of occupants in smart commercial buildings, and the factors that affect occupants' notification preferences (RQ3).

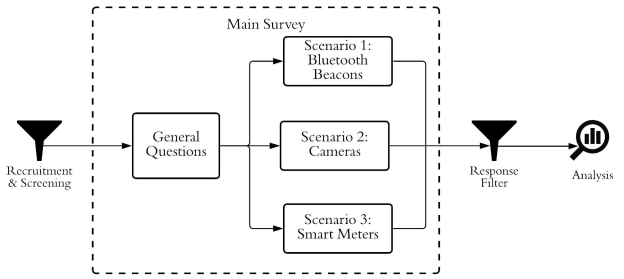

Figure 1. Overview of the study protocol.

3.1. Recruitment & Screening

Our study was built via Qualtrics and posted on Prolific to recruit participants. To ensure the quality of the responses, only people with at least a 95% approval rate on Prolific were able to view our study. We also set up Qualtrics to disallow retaking the survey. The participants were required to be adults who are 18 or older, fluent in English, live in the US, and have or are working in a commercial building physically (e.g., offices or retail stores). We further conducted a screening to determine participants' eligibility. If the participants had worked in an indoor workplace other than their home, they were eligible to participate in our study.

We paid each participant $0.5 for completing our 1-minute screening and followed up with 597 eligible participants for our main survey. Our main survey (presented in Section 3.3) took approximately 9 minutes to complete, and each participant was paid $1.5 for completing it. The longest completion time was 52 minutes. The completion time included the time it took to read and sign the consent form. Prolific allowed a minimum payment rate of $8/hour and a recommended rate of $12/hour. Our payment rate was set to $12/hour, which matched the recommended amount on Prolific. Note that Prolific may request extra payments based on the completion time. We also asked our participants to leave feedback (if any) for our study and we received no complaints from our participants regarding the payment and survey length.

3.2. Study Pretest

Cognitive pretesting and pilot study are two common practices to identify potential issues and biases in surveys, such as priming wording or confusing questions, prior to deployment [34]. We followed an iterative review process in which we repeated the process of running pilot studies to get preliminary results as well as feedback and improving our survey design accordingly until no issues arose.

We also tested our survey by conducting cognitive interviews with four university students and staff outside of the research team who are from a variety of departments and backgrounds. During the interviews, the participants thought out loud when taking the survey. We noted their thought process and asked them to provide feedback for each survey question (e.g., fixing confusing questions or adding more answer choices).

As a result, we improved the wording and formatting of survey questions and added additional answer choices to some multiple-choice questions. For example, for questions asking about the context/scenario we give, we highlighted the context/scenario (e.g., "at your workplace" or "in the scenario") to avoid misunderstanding according to the suggestions from the pilot study. We excluded the pilot study data from our final results to avoid biases.

3.3. Survey Design

In this section, we describe how we design the survey to answer the research questions.

3.3.1. Structure and Goals. The survey includes three sections. In the first section, we started with questions to understand participants' general perceptions and preferences in smart buildings. These questions include:

- Participants' awareness of potential data collection in the smart buildings (answering RQ1);
- Background questions (e.g., confidence in IoT technology and knowledge of IoT), we analyze whether the answers to the questions influence people's privacy notification preferences (answering RQ3);
- Pre-scenario questions for occupant's general privacy notification preferences in the smart commercial building setting (answering RQ2).

In the second section, we randomly show the participants one of the three hypothetical scenarios of data collection. The three scenarios include common data collection sensors (i.e., Bluetooth beacons, cameras, and smart meters). We then ask the participants the following two sets of questions:

- Questions about their perceptions of data collection in the scenario (answering RQ1);
- Post-scenario questions about their privacy notification preferences for the scenario (answering RQ2).

Note that we use the same set of questions for the pre-scenario questions and post-scenario questions regarding their privacy notification preferences. The goal is to see whether participants' preferences would change after they are exposed to the scenarios.

In the last section, we ask demographic questions. The answers to these questions are used when we analyze the factors that impact people's privacy notification choices (answering RQ3).

3.3.2. Detailed Survey Flow. In the following, we will explain the flow of our survey and how we collect responses from the participants.

- Questions about participants' awareness of potential data collection in the smart buildings (answering RQ1) and background (answering RQ3): To understand the participants' experience of working in a smart building environment, we first ask them to self-report if they work in a smart building. We present a set of smart devices (e.g., cameras, sensors, smart TV, etc.) and ask the participants to select what devices they notice at their workplace. The participants are able to select multiple devices and have an "other" option to enter others. We then ask the participants to report if they are aware of the data collection at their workplace (Yes/No). Note that the answers to these questions are used for two analyses: (1) understanding participants' awareness of data collection (answering RQ1); (2) understanding if awareness of the data collection would impact people's privacy notification choices (answering RQ3).
- Pre-scenario questions for users' general privacy notification references (answering RQ2): To understand our participants' general notification preferences for data collection in smart buildings, we used a series of questions to identify whether they want to be notified, why/why not, what should be notified, and how they want to be notified. First, we asked them if they want to be notified about the presence of the devices collecting data (Yes/No). We followed up with a free-text question to let them explain their reasons. We then presented a list of information about data collection and asked the participants to select what they want to be notified of. Next, we presented a list of notification means (e.g., physical sign, email, mobile, etc.) and asked the participants to select the means of notification that they prefer. Note that for these multiple-choice questions, the participants can select multiple items and have the option to enter additional text answers. We later repeated this series of notification preferences questions after presenting the scenarios to understand the participants' preferences specifically for each scenario.
- Scenarios-based questions: To understand users' perception of data collection, and privacy notification preferences, we designed three common data collection scenarios for the participants to check during the survey. Each scenario represents a type and purpose of data collection with different devices typically found in a smart commercial building. We study three devices (Bluetooth beacons, cameras, and smart meters) because they are popular data collection devices in smart buildings and they collect personal data about individuals. Our goal is to study how the perceptions of data collection and notification preferences differ across scenarios. We randomly assigned the participants into three groups. Each group was presented with one of the three scenarios below:
  - Scenario 1 (Bluetooth beacons): Suppose your employer installs Bluetooth beacons (devices that wirelessly broadcast a unique identifier to nearby electronic devices) at your workplace. These beacons are used to collect location and movement information to understand how the space is used.)
  - Scenario 2 (Cameras): Suppose your employer installs video surveillance cameras at your workplace that collect photo/video footage to ensure workplace security.
  - Scenario 3 (Smart meters): Suppose your employer installs smart meters at your workplace that collect data about human activities and resource usage (e.g., energy consumption, bathroom usage) to monitor and optimize the resource consumption.
- Questions about participants' perception of data collections (answering RQ1): After presenting the scenario descriptions, we asked the participants about their perceptions of data access. In particular, they were asked to select from a list of entities that could potentially (e.g., building manager, supervisor, government, etc.) have access to data about them, who they are comfortable with, who they think will benefit from having access to this data, and select/add what purposes they think the data might be used for. We further reused the aforementioned series of notification preferences questions to understand their preferences specifically for the presented scenario.
- Post-scenario questions about participants' privacy notification preferences (answering RQ2): We repeat the questions about privacy notification preferences in the pre-scenario section to check if users' preferences would be different for specific scenarios.
- Demographics: Finally, we asked our participants a set of demographic questions, including gender, age, education, and income.

3.4. Data Analysis

Our data includes multiple-choice (only 1 choice can be selected), multiple-response (multiple choices can be selected), 5-point Likert scale, and free-text data types. We used Chi-square test (for categorical data) and Kruskal-Wallis H test (for Likert scale data) to quantitatively analyze the responses across 3 scenario groups. We also conducted follow-up Bonferroni post-hoc tests for identifying statistical significance from pair-wise comparisons.

For multiple-response questions, we coded each item into its variable holding a Yes or No value. Yes value means the participant selected the item and No means otherwise. We then treated these new variables similarly to those of multiple-choice questions.

For free-text responses, 4 researchers in our group independently coded a subset of the qualitative data. We first developed and agreed on a code book to capture the themes. We then used this codebook to code the data independently. Each entry in the dataset was coded by 2 researchers. After finishing independent coding, we discussed the codes as a group to resolve conflicts and finalize the codes.

3.5. Ethical Considerations

We worked closely with our Institutional Review Board (IRB) and iteratively updated our study protocol. Our protocol did not receive any obligations or constraints from the IRB. Before the study, we asked the participants to read our consent form carefully and sign it to participate in the study. Participation in our study was voluntary and anonymous. When collecting the data, we did not collect any personally identifiable information except for their Prolific ID (a randomly-generated string of numbers and letters) for payment purposes. All data was securely stored and could only be accessed by the research team. Our survey instrument is attached in Appendix B.

4. Results

This section presents our findings from the user study and how they answer our research questions.

4.1. Overview

Our study contributes to a new understanding of people's awareness, perceptions, and notification preferences of IoT devices and the associated data collection behaviors in commercial smart buildings. In general, we found that about half of the participants reported being aware of the data collection by IoT devices at their workplaces while the other half were unaware. However, we observed variances among participants' perceptions regarding who may access their data, whether they are comfortable with their data being accessed, and who might benefit from their data.

Furthermore, we also unpacked our participants' preferences on whether they would like to receive notification about their data collection, and if so, what information they would like to know and how they want to be notified. Our results highlight the need for notifications as over 90% of our participants want to be notified. However, they have different expectations of the notification content and modality, suggesting the need for context- and device-dependent notification mechanisms.

Our study also suggested a few factors that could influence participants' preferences of what and how notifications should be delivered. For example, participants who were aware of the IoT devices' data collection would prefer to know how their collected data is used.

In the remainder of this section, we first summarize the demographics and backgrounds of our study participants, then we present our detailed findings based on the three research questions we listed.

4.2. Participants

Screening and validation: We received 800 responses from our screening. 597 participants qualified for our screening and received our invitation to the study. Eventually, we received 564 responses for our main survey. We filtered out invalid responses such as incomplete responses (including meaningless ones that the participant entered only white spaces into all free-text answer boxes), and responses that failed our attention checks. As a result, we removed 8 invalid responses from our dataset. These removed responses include 6 duplicates and 2 attention-check fails.

Considering participants whose workplace has IoT devices: As our study focuses on occupants in smart commercial buildings, we asked the participants to report what devices they noticed at their workplace. We included the "None" answer to filter out participants who had no experience with IoT devices at all. We excluded 64 such responses from our dataset. Our final dataset includes responses from 492 participants.

	Responses	Percentage
Gender		
Male	276	56.1%
Female	208	42.3%
Non-binary	7	1.4%
Prefer not to answer	1	<1%
Age		
18 - 24	95	19.3%
25 - 34	226	45.9%
35 - 44	118	24%
45 - 54	35	7.1%
55 - 64	14	2.8%
65 and above	4	<1%
Education		
Some high school	2	<1%
High school graduate	36	7.3%
Some college	87	17.7%
Associate's degree	40	8.1%
Bachelor's degree	207	42.1%
Graduate degree	117	23.8%
Prefer not to answer	3	<1%
Annual personal income		
Less than $10,000	42	8.5%
$10,000-24,999$	75	15.2%
$25,000-49,999$	125	25.4%
$50,000-74,999$	103	20.9%
$75,000-99,999$	55	11.2%
$100,000-149,999$	48	9.8%
$150,000 and greater	33	6.7%
Prefer not to answer	11	2.2%

TABLE 1. DEMOGRAPHIC INFORMATION (GENDER, AGE, EDUCATION, AND ANNUAL PERSONAL INCOME BEFORE TAXES) OF THE PARTICIPANTS IN OUR SAMPLE.

Demographic background: Among the 492 participants, 56.1% are male, 42.3% are female, and less than 2% non-binary. Our participants skewed towards young (45.9% are between 25 and 34), highly educated (42.1% have Bachelor's degree) people in the middle socio-economic class (46.3% have income between $25,000 and $74,999). Table 1 presents the descriptive statistics about the demographic background of our participants.

Regarding the background of IoT technologies in general, over 60% of our participants indicated a good level of confidence (i.e., above a rating of 3) with the IoT technologies (e.g., voice assistants, smart security cameras, smartwatches, virtual reality, etc.). Most participants reported that they have an average (34.96%) and above-average (40.04%) understanding of IoT technologies.

In Appendix A, we present additional details about participants' level of confidence with the IoT technologies and participants' understanding of the IoT technologies (Figure 5 and Figure 6).

4.3. Perceptions of Data Collection in Smart Commercial Building (RQ1)

Our goal is to understand occupants' perceptions of data collection in smart commercial buildings, identifying potential gaps between occupants' perceptions and the IoT data collection transparency. Our data suggested that the participants reported different levels of understanding in terms of the types of data collection at their workplaces. There is a discrepancy between what people think about IoT data collection and what it actually is.

4.3.1. Awareness of data collection. First, we want to understand if the occupants know of the data collection happening and what kinds of IoT devices they noticed at their workplace. 52.44% of participants reported being aware of the data collection at their workplace while the other 47.56% reported being unaware. We asked what devices they noticed at their workplace. Cameras were the most popular device (selected by 76.83% of participants) that they noticed at their workplace. Among different sensors, most of our participants reported noticing temperature sensors, while the energy sensor was the least noticed one. Figure 2 shows the percentage of responses for what devices the participants noticed at their workplace.

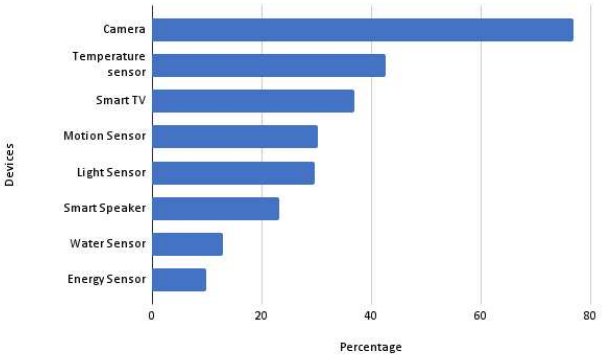

Figure 2. Participants' responses to what devices they notice at their workplace.

Takeaway 1: Even though people notice IoT devices at their workplace, they are not aware of these devices collecting data. Cameras are the most popular devices that people notice at their workplaces. This indicates that the camera's presences are very obvious to many occupants in a smart commercial building setting. We later present findings about occupants' perceptions and notification preferences of the camera's data collection scenario as compared to two other less obvious scenarios (i.e., Bluetooth beacon and smart meter).

4.3.2. Perceptions of data access. We further unpack people's perceptions of data collection from the following three perspectives: (1) who do you think will have access to your data, (2) who are you comfortable with having access to your data, and (3) who do you think will benefit from having access to your data. We provided a list of entities relevant to data collection in smart buildings, which included my building manager, my supervisor, the government, the manufacturer of the devices, my company, and myself. We used Chi-square test to identify the significant associations between the scenario and the selection of each entity. We also conducted a Bonferroni post-hoc analysis to identify the specific pairs of scenarios that have a significant difference.

First, we find that the majority of participants (94.5%) thought that their company would have access to data about them in all 3 scenarios. A few participants (11%) thought that they [themselves] would have access to their own data. We identify statistical significance for "My supervisor" ($p = 0.002$) and "The manufacturer of the devices" ($p = 0.000$) across 3 scenarios. Specifically, for the "My supervisor" selection, our pair-wise comparison test shows that in the Bluetooth beacon scenario, significantly more participants thought that their supervisor would have access to their data compared to the smart meter scenario ($p = 0.001$). For the "The manufacturer of the devices" selection, we find a significant difference between the camera scenario and each of the other two scenarios, i.e., significantly fewer participants in the camera scenario thought that the manufacturer of the devices would have access to the data as compared to the other 2 scenarios ($p = 0.000$).

Second, we find that most participants felt comfortable with themselves (62.4%) and their company (53.5%) having access to their data. For the Bluetooth beacon and smart meter scenarios, slightly more participants were comfortable with themselves than with their company having access to the data. For the camera scenario, the numbers are equal. We find statistical significance for "My building manager" ($p = 0.005$), "My supervisor" ($p = 0.027$), and "The manufacturer of the devices" ($p = 0.000$) across the 3 scenarios. For "My building manager", our pair-wise comparison test shows that significantly fewer participants in the Bluetooth beacon scenario felt comfortable with the building manager having access to their data compared to the smart meter scenario ($p = 0.003$). For the "My supervisor" selection, significantly more participants in the camera scenario were comfortable with their supervisor having access to their data compared to the smart meter scenario ($p = 0.022$). For "the manufacturer of the devices" selection, significantly more participants in the smart meter scenario were

comfortable with the manufacturer of the devices having access to their data compared to the camera ($p = 0.000$) and Bluetooth beacon ($p = 0.001$).

Lastly, when asked about who they thought would benefit from having access to their data, most participants thought that their company would. Only 15.4% of participants thought that they would benefit from having access to their own data. We find statistical significance for "My building manager" ($p = 0.002$), "My supervisor" ($p = 0.000$), and "The manufacturer of the devices" ($p = 0.002$). Our pair-wise comparison test indicates the significant difference between the smart meter and each of the other two scenarios regarding "My building manager" (camera: $p = 0.003$, Bluetooth beacon: $p = 0.012$) and "My supervisor" ($p = 0.001$) selections. Noticeably more people in the smart meter scenario thought that the building manager would benefit from having access to the data while the percentages were similar between the other two scenarios. In contrast, significantly fewer people in the smart meter scenario thought that their supervisor would benefit from having access to the data as compared to the other two scenarios. For the "the manufacturer of the devices" selection, we find a significant difference between the camera and each of the other two scenarios (smart meter: $p = 0.004$, Bluetooth beacon: $p = 0.013$). Significantly fewer people in the camera scenario thought that the manufacturer of the devices would benefit from having access to the data.

Takeaway 2: In a smart commercial building setting, occupants feel more comfortable with having access to their own data over other entities. However, most people do not think that they have access to their own data, yet they would benefit from having access to their own data. Besides, depending on the type of devices that collect data, they have significantly different perceptions about what data are collected and who will benefit from such information. Building managers, supervisors, and the manufacturers of the devices are the three entities that have significant differences in terms of occupants' perceptions across the 3 scenarios (i.e., Bluetooth beacon, camera, and smart meter).

4.3.3. Perceived purposes of data collection. We then asked the participants to select the purposes for that they think the collected data about them could be used. In general, for all 3 scenarios, "enforcing policies" is the most selected purpose for data collection (over 75% of participants). This is a surprising result since most of the time, enforcing policies is not what the collected data is primarily used for.

Specifically, in the Bluetooth beacon scenario, "localization" is the least selected purpose, which is also an interesting result because it is actually the primary usage of Bluetooth beacons. Instead, most participants thought "enforcing policies" (76.5%) and "user profiling" (71.6%) were the purposes of the Bluetooth beacon's data collection. One participant was specifically concerned that Bluetooth beacons could get unauthorized access to his/her phone: "I would assume the Bluetooth beacon might also be able to access my phone without me realizing (P272)."

These results indicate people's misconceptions and lack of knowledge regarding the purposes of data collection in various contexts. Figure 3 shows the percentage of participants' responses for what purposes they think the collected data about them might be used.

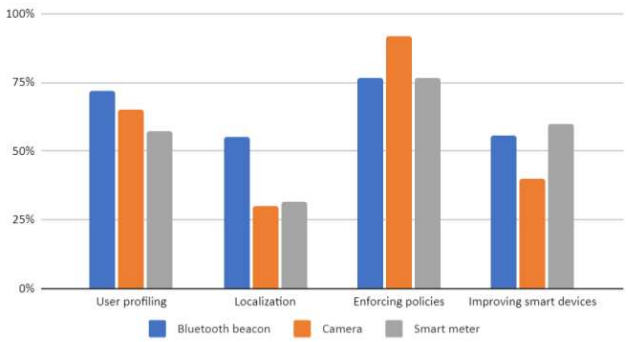

Figure 3. Participants' responses to "What purposes do you think data about you might be used for?" across 3 scenarios. Enforcing policies is the most popular selection for all 3 scenarios, which indicates the participants might have misconceptions about the purposes of the devices.

Takeaway 3: Interestingly, many participants may have misunderstandings about the purposes of the data collection. 76.5% of the participants in the Bluetooth beacon scenario thought that its data collection is used for enforcing policies. Even though some participants indicated that their understanding of IoT technologies, in general, is at or above average, many of them still believe that the data collection in the three scenarios is for enforcing policy purposes instead of for the functionalities of IoT devices. This may indicate one of the following: 1) participants are not fully aware of the purpose of different IoT devices and they have a misunderstanding of how IoT devices work, or 2) they do not believe that the IoT devices are utilized for the same purposes as they are intended and designed. Thus, it is important to inform people about data collection purposes and data access when designing notifications.

4.4. Notification Preferences for Data Collection in Smart Commercial Building (RQ2)

To understand participants' preferences for notifications in smart commercial buildings, we used the following questions regarding the presence of data collection:

- Do you want to be notified? Why and why not?
- What do you want to be notified about?
- How do you want to be notified?

We first asked these three questions at the beginning of the survey to get a general overview of the participants' notification preferences. We then presented the hypothetical scenarios and asked these questions again to investigate the participants' notification preferences specifically for the given scenario. As the participants were randomly presented with one of the three scenarios, we need to ensure that the participants in the three groups have a similar level of understanding of IoT technologies so that we can make a comparison among these three groups. We did not find statistically significant differences among the participants in the three groups, indicating that participants from all three groups have a similar level of IoT knowledge.

4.4.1. Participants' Notification Preferences. Next, we present participants' responses to our questions regarding

whether they want to be notified about the data collection and what information they want to know in general and in 3 scenarios. Table 2 lists all themes from the participants' responses to why they want or do not want to be notified about the data collection in each scenario.

General context. When asked whether they want to be notified about the presence of the devices collecting data about them at their workplace, the majority of participants (90.65%) wanted to be notified and only 9.35% did not want to be notified.

The majority of participants wanted to be aware of the data collection. Privacy rights and the safety of the data were also considered important to the participants. A participant mentioned "I want to know how my information may be handled and if it will affect me in my personal life or my work life (P1)." Other participants expressed privacy concerns such as "So I don't get spied on without knowing. And being aware of how my facial data is processed by my employer (P9)." A participant thought that he/she was already being spied on: "I already know they are spying on us but I would at least like to know from where (P153)."

The few participants that did not want notifications thought that the data collection would not affect them negatively or trusted whoever had access to the collected data: "I don't think it would affect my performance (P185).", "Doesn't bother me much (P151).", "Information collected by the company is strictly official and has little or nothing to do with my private life. This information also rests in credible hands (P195)." Some others were confident that they already knew how things work and that notifications are unnecessary: "I really understand how it works, I don't need any notification on them (P138).", "I personally don't feel it's necessary and also me not knowing would allow me to work and act normally (P281)."

Our data suggest 9 primary reasons why the participants wanted to be notified and 13 reasons why they did not want to be notified about the data collection. For example, increasing awareness of data collection by nearby smart devices remains the top reason why participants would like to be notified (n=246). Notably, 68 participants believed that they have privacy rights in the workplace; as a result, they should be notified of any nearby data collection: "No matter what that is my right to be notified" (P172), "It is one of the rights I have as an employee" (P178), or "I believe it is unethical for a company to record information about employees without first telling them about and what information is collected (P196)."

For what people want to be notified about, we asked the participants to select from a list of different options before they saw the scenarios as well as after reading the scenarios: the presence of data collection, purposes for which your data can be used, how your data can be used, for how long your data can be retained, and who can access your data. The majority of the participants (more than 89%) wanted to be notified about all of the listed options. Fewer participants (78%) wanted to know for how long their data can be retained. There were no significant differences in participants' preferences on what they would like to be notified about across a general context and 3 scenarios.

Scenario 1: Bluetooth beacon. 91.36% of our participants wanted to be notified about the presence of the devices collecting data while 8.64% did not. Most people wanted to be notified of the purposes for which their data can be used. Participants wanted to be aware of any sensitive info that could be inferred from the data: "That's really creepy and I don't want to be constantly tracked (P81).", "I don't want potentially embarrassing info collected, like how often I use the bathroom (P261)." Some participants mentioned that the data collection could affect their job: "The Bluetooth beacon collects some personal data about my performance by interacting with other devices (P198).", "So I can decide whether or not it's a dealbreaker for me in keeping the job (P280)."

The majority of people thought that data collected from Bluetooth beacons would be used for enforcing policies and user profiling. A few participants thought that the data could be used for micromanagement, manipulation, profit from selling to third parties, or improving workspace efficiency. One participant mentioned "I want to know if my actions are being monitored in some way and have the potential to be used against me (P1)."

When asked about who would have access to the collected data, most people thought that their company would have access to the collected data (95.7%) and that their company would benefit from having the data access (87.7%). However, the majority of people (67.9%) were comfortable with themselves rather than their company having access to the collected data. A participant was worried that someone else might know their private activities: "If my whereabouts are being tracked, I want to know. It also prevents people from being blindsided when they're confronted with information that they thought no one knew about because they were alone when they were doing it (going from A to B, spending too much time somewhere, etc.) (P73)."

Scenario 2: Camera. 92.77% of our participants wanted to be notified about the presence of the devices collecting data while 7.23% did not. More people were interested in getting notified about who can access their data and the purposes for which their data can be used. In contrast to the other 2 scenarios, the participants were more concerned about their behaviors being monitored. A few participants did not want their activities to be watched by someone else: "So I don't do something embarrassing while I think I am alone and no one but me will ever see or know (P429)."

The majority of participants thought that camera data would be used for enforcing policies. One participant said: "Because if I do any mistake I will correct that (P45)." Many participants also selected user profiling as the purpose of using camera data. Some participants expressed concerns about past experience with camera data collection: "I have been through abusive periods of my life revolving heavily around cameras (P50)."

The majority of participants (95.2%) thought that their company would have access to the collected data. Many people also thought their supervisor and building manager would have access. Some mentioned the IT department and the software provider of the camera. Most participants were comfortable with themselves and their company having access to the collected camera data. Surprisingly, more participants were comfortable with their company than themselves having access (56.6% vs 55.4%). Some

Question	Categories	Number of responses			
		General	Bluetooth beacon	Camera	Smart meter
Why notified	Awareness of data collection	248	73	84	79
	Privacy rights/Ethics	71	23	31	20
	General concerns/curiosity	40	29	21	31
	Privacy violation	38	16	13	7
	Pay attention to their behavior	36	13	24	12
	Ensure safety of their data	24	10	11	4
	Trust/Communication/Interaction	18	20	18	8
	Ownership of their own data	12	18	14	23
	Understand the associated benefits	4	5	2	1
Why not notified	No violation/negative effects	7	1	0	1
	Nothing to hide	5	2	1	1
	Understand how it works	4	2	1	0
	Unnecessary/Not useful	4	2	4	10
	Burdensome/It will worry me more	4	1	0	3
	Feel comfortable with devices around	3	0	0	1
	Just don't want	3	0	2	7
	Not sensitive	2	1	0	2
	It makes no difference in my behavior	2	1	0	0
	No control anyways	2	1	0	0
	Employer's privilege	2	0	0	1
	Won't get enough info	1	0	0	0
	Not related to privacy	1	1	1	5
	Private property	0	1	0	0

TABLE 2. CATEGORIES OF QUALITATIVE RESPONSES REGARDING REASONS WHY THE PARTICIPANTS WANTED OR DID NOT WANT TO BE NOTIFIED ABOUT DATA COLLECTION

mentioned that they would like to get help with loss prevention or in case of theft occurs.

Although the participants would like to get help with loss prevention from their company, a few thought that they themselves would benefit from having access to the collected data (16.9%). Significantly more participants thought that their company would benefit from having access to the data (86.1%).

Scenario 3: Smart meter. 81.71% of our participants wanted to be notified about the presence of the devices collecting data while 18.29% did not. More people were interested in getting notified about who can access their data and the purposes for which their data can be used.

In contrast to the other 2 scenarios, more participants worried about the ownership of their data. Most said that it is their right to know about their own data being collected: "Because it's my data and it should belong to me (P241)." or "I feel it is my right to have access to the information that is gathered about me (P109)." Most people who did not want to be notified thought that it is not necessary or not useful: "I feel it's of no need to enable me to know the presence. I feel it's right to let it do its work without myself having to feel its presence (P11)." Some participants thought the data collection was not related to privacy: "Data based on resource consumption is not really privacy related (P7)."

Surprisingly, enforcing policies is the purpose of using the collected data that most participants thought. Noticeably fewer people selected "improving smart devices" which is actually the main purpose of smart meter data collection. A few people mentioned tracking resource usage and intimidation as the purposes of using smart meter data. Some participants expressed concerns about being monitored: "It feels like they are getting very close to crossing that bridge of going too far for me at least. I'd like to know what they are tracking/watching if I am an employee (P36)."

In this scenario, most participants (92.7%) thought that their company would have access to the collected data. A few participants (13.4%) thought that they themselves would have access. When asked about who they are comfortable with having the access, more participants selected "Myself" than "My company" (64.0% vs 45.7%) which indicates that people preferred to have access to their data besides the company. However, the majority of participants (86.0%) still thought that their company would benefit from it. One participant added that whoever bought the collected data would benefit from it.

Takeaway 4: In general, most people (90.65% of participants) preferred to be notified about the presence of the devices collecting data about them at their workplace. Across 3 scenarios, participants' desire for notification is consistent in Bluetooth beacon and camera scenarios. However, about 10% fewer participants wanted to be notified in the smart meter scenario, suggesting that fewer people are concerned about smart meter data collection. For all 3 scenarios, participants expressed their preference for notification of all information about the data collection activity that we listed. Noticeably, participants in the Camera scenario were more interested in knowing whether their behaviors were being tracked, while those in the Smart meter scenario were more interested in the ownership of the collected data. The results indicate the importance of transparency in data collection.

4.4.2. Participants' Notification Methods Choices. Next, we present the participants' preferences of notification methods for data collection in general and in

3 scenarios. Figure 4 show the percentage of what the participants wanted to be notified about and how they wanted to be notified, respectively for 3 scenario groups.

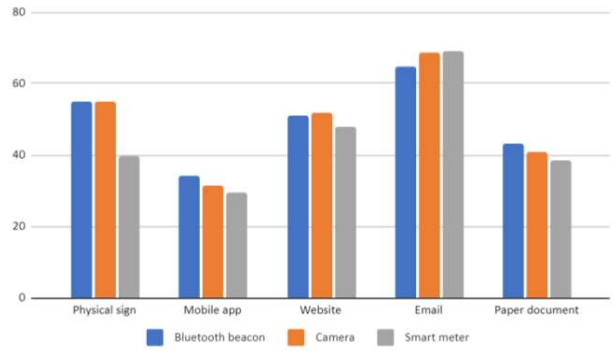

Figure 4. Participants' preferences for how they wanted to be notified across 3 scenarios.

Email is the most popular choice across all scenarios and in general. 69% of participants selected email as their preferred notification method. Notably, the amount of participants who preferred Email method is significantly larger than other methods. One participant says "I want to be notified of how my data is being gathered via email on a weekly basis (P113)."

Mobile App is surprisingly the least selected choice. Only 33% of participants preferred to be notified via mobile app. This choice has a significantly lower number of participants as compared to email (69%), physical sign (51%), and website (49%). Although mobile app has been a popular method of notification [41], our finding shows that participants do not prefer to receive mobile app notifications for smart commercial building context.

Physical Sign is more preferred in the Bluetooth beacon scenario and the Camera scenario. Our statistical test shows a significant difference for the "physical sign" option between the smart meter scenario and the other two scenarios ($p = 0.006$), as 6% fewer participants preferred physical sign in the smart meter scenario.

In-person notification is suggested in the Bluetooth beacon scenario and the Smart meter scenario. Other than indirect notifications, participants in these two scenarios also suggested having their supervisor or people from upper management notify them in person about the data collection (n = 5). We did not find anyone suggesting this method in the Camera scenario. However, in the Camera scenario, one participant suggested implementing a written policy document.

Across different means of notification, participants strongly preferred to be notified about the presence of a camera. Participants' negative experiences with cameras could cause such preference. For example, one participant specifically mentioned their bad past experience with camera data collection as the reason why they wanted notification: "I have been through abusive periods of my life revolving heavily around cameras (P50)."

Takeaway 5: Email and physical signs were generally the most preferred means of notification for data collection in smart commercial buildings. However, one-size-fits-all should not be the strategy for notification. Fewer participants preferred physical signs for the smart meter scenario, which is significantly different from the other two scenarios. Therefore, a flexible selection of notification strategies (e.g., device-specific strategies) may be needed to inform occupants about the type and purpose of data collection by different IoT devices in smart commercial buildings.

4.5. Potential Factors for Notification Preferences in Smart Commercial Building (RQ3)

In this section, we discuss factors that may influence people's notification preferences for different IoT devices in smart buildings. Specifically, we focus on the following three factors: participants' awareness, confidence, and understanding of IoT devices in smart buildings based on participants' responses to the pre-scenario questions (i.e., general context).

4.5.1. Awareness of data collection. We asked the participants whether they were aware of the data collection at their workplace. 52.44% reported being aware, and 47.56% reported being unaware. We further find that 91.5% within the aware group and 89.74% of participants within the unaware group reported wanting to be notified about the presence of data collection. This indicates that most occupants in smart commercial buildings may have concerns about their data being collected and thus want to be able to keep track of the data collection activities around them. It also confirms the importance of implementing notifications of data collection in commercial buildings to provide transparency.

Our result shows that the participants do not have significantly different notification preferences regardless of whether they are aware or unaware of data collection around them. However, regarding what people want to be notified about, we observed that about 4% more participants in the aware group selected "How your data can be used", while for the other choices, there are slightly more participants (less than 4%) in the unaware group. Regarding how people want to be notified, the response percentage for the physical sign is similar between the two groups. Mobile app (about 6% more participants) and website (about 2% more participants) are more preferred in the aware group, while email (about 7% more participants) and paper document (about 3% more participants) are more preferred in the unaware group.

4.5.2. Confidence with IoT. We used a 5-point Likert scale question to ask about participants' confidence levels with IoT technologies. For analysis purposes, we categorized "1-Extremely unconfident" and "2-Somewhat unconfident" into the unconfident group, "3-Neither confident nor unconfident" into the neutral group, and "4-Somewhat confident" and "5-Extremely confident" into the confident group. As a result, we had 16.3% (80 out of 492) unconfident, 16.3% (80 out of 492) neutral, and 67.5% (332 out of 492) confident responses. We further found that the majority of participants within each group

(96.3% in unconfident, 92.5% in neutral, and 88.9% in confident) wanted to be notified about the presence of devices collecting data. This result suggests that even though people are confident with IoT technologies in general, they still prefer to be notified about the data collection around them.

Regarding what people want to be notified of, we found statistical significance ($p = 0.001$) for "Presence of data collection", "How your data can be used" ($p = 0.043$), "For how long your data can be retained" ($p = 0.000$), and "Who can access your data" ($p = 0.038$). For all of this data collection information, our pair-wise comparison further shows a significant difference between the confident group and the unconfident group ($p = 0.002$, $p = 0.039$, $p = 0.000$, respectively). Across all information about data collection, fewer participants in the confident group wanted to be notified as compared to the other two groups.

Regarding how people want to be notified, we did not find any statistical significance for the three groups. However, we observed that slightly more participants in the unconfident group preferred the other means of notification (i.e., physical sign, website, email, and paper document) rather than mobile app. There are about 12% more participants in the confident group for mobile app selection than in the unconfident group.

4.5.3. Understanding of IoT. We used a 5-point Likert scale question to ask the participants how they would describe their understanding of the IoT. For analysis purposes, we categorized "1-No understanding" and "2-Below average" into the below-average group, "3-Average" as the average group, and "4-Above average" and "5-Strong understanding" into the above-average group. Thus, we had 6.9% (34 out of 492) below average, 35% (172 out of 492) average, and 58.1% (286 out of 492) above average. We further found that the majority of participants within each group (97% in the below-average group, 90.1% in the average, and 90.2% in the above-average group) wanted to be notified about the presence of devices collecting data. This result shows that even though people claimed to have an average or above-average understanding of IoT technologies, they still want notifications about the data collection around them.

Regarding what people want to be notified about, we did not find any statistical significance for the three groups. However, across all information about data collection, we observed that there were slightly more participants in the below-average group who wanted to be notified. It is understandable that people with a below-average understanding of IoT may want to be notified of more information about data collection.

Regarding how people want to be notified, we identified statistical significance for "mobile app" ($p = 0.009$) and "email" ($p = 0.021$). For both of these means of notification, our pair-wise comparison shows a significant difference between the average group and the above-average group ($p = 0.018$, $p = 0.049$, respectively). More participants in the above-average group preferred mobile app for notification, while more participants in the below-average group preferred email, physical sign, and paper document options.

Takeaway 6: In smart commercial buildings, transparency of data collection is crucial. Even if people are aware of the data collection, are confident with IoT technologies, or are knowledgeable about IoT, they are still more likely to prefer receiving notifications about the data collection activities. The less confident people are with IoT technologies, the more information about data collection they want to be notified of. Regarding means of notification, people who claim to be confident with IoT technology and people who claim to have an above-average understanding of IoT tend to prefer mobile app over other means. This indicates the need for a flexible notification strategy that considers the background of the users.

5. Discussion

In this section, we discuss the implications of privacy regulations and how our findings inform the design and operation of smart commercial buildings. We focus on how to inform and notify people about the type of data that is being collected, who may have access to their data, and how they can be better in charge of their own data. We further discuss the limitations of our study and potential future work.

5.1. Policy Implications

Recent privacy regulations around the world, including the European Union's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), lay the legal foundation for consumers to have control over the use and sharing of their personal information that businesses collect from them. Devices and systems that collect and use personal data about smart building occupants include: electronic access systems (such as smart entrances for exterior access points like gates and garages), thermostats, lighting, heating ventilation air conditioning (HVAC), sensors, voice recognition, and cameras. Businesses have to inform consumers about their data collection practices at or before the point of collection. Regardless of the method of collection, smart building owners must ensure visitors and guests are presented with clear and concise notice of the collection, use, and sharing of their personal information.

These laws lead to the fact that more respect and protection are being given to people's personal data, even at a heavy cost [26]. Therefore, to truly capitalize on the promise and benefits of smart buildings, it is not enough to minimize the data collected and limit the purpose of the data collection. Smart buildings need to take into account the occupants' *privacy preferences and background* to determine a respectful way to *notify* occupants of what data is being collected, how the collected data is utilized, and who has access to this data.

5.2. Key Designs to Improve Smart Building Data Collection Transparency

We detail our insights for designing data collection systems in smart commercial building settings as follows.

Occupants in smart commercial buildings may be affected by legal ramifications as compared to

occupants in private smart homes. In particular, for smart homes, the owners can agree on installing IoT devices that collect their data and have control over them. However, this may not apply to people working in smart commercial buildings where there are much more complex interactions. It could lead to the fact that these occupants may not be aware of the data collection in the building where they work, and even if they are aware, they may have misunderstandings of the data collection activities.

As shown in our study results, we found that nearly half of the participants (47.56%) were not aware of the collection of identifiable data about them. This result indicates that data collection in a smart commercial building is opaque to the occupants. The majority of participants (90.65%) reported that they wanted to be notified about the presence of devices collecting data about them in their work environment. Thus, to improve the smart building occupant experience, notifications about data collection activities should be carefully considered when planning to deploy IoT devices.

Occupants in smart commercial buildings also have more concerns about their privacy as compared to those in smart homes: "For starters, in my own home I can control what's going on regarding my own electronics. At my job I'm at the mercy of what the board/tech committee/whoever would make this decision, I think I at least deserve to know how my privacy is going to be violated. Also, all the HIPAA implications that would come with having all or at least a large part of conversations in the building being listened to at all times." Some were uncomfortable with being monitored at their workplace and that could affect their productivity: "The data seems to be not related directly to my job, and I fear it could be used against me at some point. It feels like every aspect of my being is being monitored, and it does not create a comfortable environment. The camera sensor bothers me less than things like an energy sensor, because I know I am not doing anything that I would not like to be on camera, I am doing my job well. It's the random info that makes me uncomfortable, and I wonder just what is being done with it."

Notifications by email is consistently the most preferred method for the participant's preference on how to be notified across scenario and confidence groups. On the contrary, notification by mobile app is one of the lowest rated methods. This result shows a very different notification preference as compared to a smart home environment where people preferred mobile app notification the most [41]. Although notification by email is preferred in the smart commercial building context, it is important to note that email notification is only practical in scenarios where all data subjects can have their email addresses registered for notifications.

We suspect that the amount of user effort involved in receiving notifications is one of the deciding factors in the smart commercial building context. For example, emails require the least amount of user effort in the professional context, given that email is the most common way of communication at work. Similarly, physical signs, websites, or paper documents likely will not require the users to actively do anything to subscribe to the notifications. However, to receive notifications through a mobile app, users need to rely on an additional device, and installing an app also takes some effort.

In terms of what to notify the occupants, people seem to be less interested in: 1) data collected by smart meters, and 2) the duration with which data is retained. These results indicate that if a designer is looking to reduce fatigue by minimizing the amount of information in the notification, information about sensors similar to smart meters and duration information can be the first candidates to eliminate. When looking at the types of users, we found that factors such as confidence about IoT and IoT knowledge impact users' privacy notification preferences in different data collection scenarios. These results indicate that a notification system can likely take advantage of a user's self-reported understanding and confidence of IoTs to tailor the notification rate for privacy updates and changes.

People consider certain locations in the building (e.g., bathrooms) as private spaces where data should not be collected. Some participants mentioned that they do not want to be recognized while using the bathroom as there is no privacy. Even in the smart meter scenario, participants were okay with water use tracking but were hesitant about collecting data in private areas. Some participants in this scenario mentioned that water usage is not so much of a big deal, but they do not like the idea of someone keeping track of their bathroom usage. They further explained that it would be embarrassing if a supervisor or manager came by and questioned their usage. These results might indicate that smart building managers should consider setting different policies for data collection in public, semi-public, and private spaces in smart buildings.

It is important for smart buildings to create a fiduciary relationship with their occupants by aligning interests. Our findings (Section 4.3.2) indicate that many occupants feel the IoT data collection in smart buildings benefits others (e.g., building managers, employers) more than themselves, which may lead to common negative perceptions or misconceptions around unwanted surveillance. Although some of our participants recognized the potential personal benefits of such IoT data collection, it is not currently feasible for them to take full advantage of the data being collected. To improve the acceptance and resolve potential privacy concerns, it is critical for smart building managers to create a fiduciary relationship with occupants by aligning the interests of both parties.

We recommend that smart buildings should ensure occupants are aware of their personal benefits from various IoT data collection, which could be conveyed through effective privacy notifications in occupants' preferred formats. Also, necessary software infrastructure (e.g., APIs) that enables occupants to access and take advantage of certain collected IoT data for their personal benefits will contribute to building such a fiduciary relationship.

5.3. Limitations and Future Work

Our study has some limitations. First, our results rely on participants' self-reported data. To mitigate the bias, we cross-checked participants' answers throughout the survey to ensure their responses were consistent, indicating a satisfactory level of trustworthiness regarding their

preferences. Second, we used hypothetical scenarios in our study to prompt participants' preferences, and the preferences can vary based on context. Third, some of our participants may not have experience with smart buildings based on our definition. However, it is worth noting that in the survey, we asked whether participants had seen any smart devices in their building. The results indicated that the majority of our participants came across some IoT devices at their workplaces. Lastly, some participants may be biased due to the same questions regarding their preferences before and after we presented the scenarios.

Our study in this paper focuses on smart commercial building occupants in the US. However, as more countries and regions deploy smart building technology in real-world settings, future studies can consider cross-cultural perspectives. For example, our finding regarding occupants' perceptions of data access can be further extended to identify the differences based on different work cultures and regulations. Additionally, future work can potentially do a field study to further explore people's notification preferences in real smart building settings that consider different contexts. It is also interesting to explore workplace monitoring or tension between employees and employers. Some small-scale interviews or case studies at different types of smart building workplaces would be ideal to collect such data.

Our study is the necessary step toward designing a more effective data collection and disclosure scheme for smart buildings. Future research can look into building personalized notification systems for data collection in smart buildings. However, a complex multi-stakeholder environment could be a big challenge to deploying such personalized systems. Thus, exploring the complex relationships and potential conflicts between different stakeholders in the smart building context is also important.

6. Conclusion

Smart buildings and their applications are becoming more popular in urban areas around the world. They increasingly adopt IoT technologies to manage their resources and services. Large deployments of interconnected sensors, actuators, and smart devices in smart buildings improve productivity and user experience across application domains. However, this means pervasive, multimodal, continuous, and scalable data collection in such a semi-public space. This is also an underexplored domain. Therefore, our goal in this study is to understand the occupants' perceptions of data collection and their notification preferences for different data collection scenarios in smart commercial buildings. We conduct a user study with 492 participants who are occupants of smart commercial buildings. Our analysis results show that many participants (47.56%) are unaware of the data collection, and email is, in general, the most preferred means of notification. We also find that people have different preferences for notifications when they face different data collection scenarios. Our findings will help guide the design and implementation of privacy-related notifications in smart buildings and increase occupants' awareness of the nearby data collection. In the bigger picture, future smart cities can use the insights from this research to develop privacy-respecting infrastructure and effective notification schemes.

Acknowledgements

This research was supported in part by the National Science Foundation (NSF) Secure and Trustworthy Computing program (Grants CNS-1801316, CNS-2320903). Other grants supporting this research included NSF CNS 2114074, NSF OAC 2002985, NSF CNS 1943100, NSF OAC 1920462, NSF CNS 2323105, and Google Research Scholar Award. The US Government is authorized to reproduce and distribute reprints for Governmental purposes, notwithstanding any copyright notices thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied of the US Government or other funding agencies. This research was also partially funded by an internal grant at the University of Maryland, Baltimore County. We thank Clay Ford from UVA Stat Lab for providing statistical consulting and UVA Link Lab for providing feedback on the study design. We also thank our shepherd and anonymous reviewers for their constructive comments on this research.

References

[1] A survey on iot platforms: Communication, security, and privacy perspectives. Computer Networks, 192, June 2021.

[2] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. Peek-a-boo: I see your smart home activities, even encrypted! In Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '20, page 207–218, New York, NY, USA, 2020. Association for Computing Machinery.

[3] Joseph G Allen and John D Macomber. Healthy buildings: How indoor spaces drive performance and productivity. Harvard University Press, 2020.

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. 2(2), jul 2018.

[5] Leonardo Babun, Z. Berkay Celik, Patrick McDaniel, and A. Selcuk Uluagac. Real-time analysis of privacy-(un)aware iot applications. Proceedings on Privacy Enhancing Technologies, 2021(1):145–166, 2021.

[6] Natã Miccael Barbosa, Joon Sung Park, Yaxing Yao, and Yang Wang. "what if?" predicting individual users' smart home privacy preferences and their changes. Proceedings on Privacy Enhancing Technologies, 2019:211 – 231, 2019.

[7] Matthias Caesar and Jan Steffan. A location privacy analysis of bluetooth mesh. Journal of Information Security and Applications, 54:102563, 2020.

[8] Stephan Cejka, Felix Knorr, and Florian Kintzler. Privacy issues in smart buildings by examples in smart metering. 2019.

[9] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81:42–51, 2018.

[10] CookieYes. Gdpr cookie consent banner examples, November 2019.

[11] Council of European Union. General data protection regulation. https://gdpr-infor.eu, 2016.

[12] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. J. on Telecomm. & High Tech. L., 10:273, 2012.

[13] Stefany Cruz, Logan Danek, Shinan Liu, Christopher Kraemer, Zixin Wang, Nick Feamster, Danny Yuxing Huang, Yaxing Yao, and Josiah Hester. Augmented reality's potential for identifying and mitigating home privacy leaks. arXiv preprint arXiv:2301.11998, 2023.

[14] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. IEEE Pervasive Computing, 17(3):35–46, 2018.

[15] Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham J Mysore, Fredo Durand, and William T Freeman. The visual microphone: Passive recovery of sound from video. 2014.

[16] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. Bolder is better: Raising user awareness through salient and concise privacy notices. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pages 1–12, 2021.

[17] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In 2020 IEEE Symposium on Security and Privacy (SP), pages 447–464. IEEE, 2020.

[18] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. Proc. ACM Hum.-Comput. Interact., 2(CSCW), November 2018.

[19] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pages 1–16, 2021.

[20] MG Figueiro, B Steverson, J Heerwagen, R Yucel, C Roohan, L Sahin, K Kampschroer, and MS Rea. Light, entrainment and alertness: A case study in offices. Lighting Research & Technology, 52(6):736–750, 2020.

[21] Michelle Goddard. The eu general data protection regulation (gdpr): European regulation that has a global impact. International Journal of Market Research, 59(6):703–705, 2017.

[22] Eric Goldman. An introduction to the california consumer privacy act (ccpa). Santa Clara Univ. Legal Studies Research Paper, 2020.

[23] Scott Harper, Maryam Mehrnezhad, and John Mace. User privacy concerns in commercial smart buildings. Journal of Computer Security, (Preprint):1–33, 2022.

[24] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., 4(2), jun 2020.

[25] Farrokh Jazizadeh, Burcin Becerik-Gerber, Mario Berges, and Lucio Soibelman. An unsupervised hierarchical clustering based heuristic algorithm for facilitated training of electricity consumption disaggregation systems. Advanced Engineering Informatics, 28(4):311–326, 2014.

[26] Jennifer Huddleston. The price of privacy: The impact of strict data regulations on innovation and more. https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/, 2021.

[27] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I Hong. Exploring the needs of users for supporting privacy-protective behaviors in smart homes. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, pages 1–19, 2022.

[28] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P Knijnenburg. Privacy and the internet of things. Modern Socio-Technical Perspectives on Privacy, page 233, 2022.

[29] Jiakang Lu, Tamim Sookoor, Vijay Srinivasan, Ge Gao, Brian Holben, John Stankovic, Eric Field, and Kamin Whitehouse. The smart thermostat: using occupancy sensors to save energy in homes. In Proceedings of the 8th ACM conference on embedded networked sensor systems, pages 211–224, 2010.

[30] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), pages 399–412, Santa Clara, CA, July 2017. USENIX Association.

[31] Anne Oeldorf-Hirsch and Jonathan A Obar. Overwhelming, important, irrelevant: Terms of service and privacy policy reading among older adults. In Proceedings of the 10th International Conference on Social Media and Society, pages 166–173, 2019.

[32] Office of the California Attorney General. California consumer privacy act (ccpa): First modified regulations. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf, 2020.

[33] Primal Pappachan, Martin Degeling, Roberto Yus, Anupam Das, Sruti Bhagavatula, William Melicher, Pardis Emami Naeini, Shikun Zhang, Lujo Bauer, Alfred Kobsa, Sharad Mehrotra, Norman Sadeh, and Nalini Venkatasubramanian. Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences. In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 193–198, 2017.

[34] Stanley Presser, Mick P. Couper, Judith T. Lessler, Elizabeth Martin, Jean Martin, Jennifer M. Rothgeb, and Eleanor Singer. Methods for Testing and Evaluating Survey Questions, chapter 1, pages 1–22. John Wiley & Sons, Ltd, 2004.

[35] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In Proceedings of the Internet Measurement Conference, IMC '19, page 267–279, New York, NY, USA, 2019. Association for Computing Machinery.

[36] Luis Puche Rondon, Leonardo Babun, Ahmet Aris, Kemal Akkaya, and A. Selcuk Uluagac. Survey on enterprise internet-of-things systems (e-iot): A security perspective, 2021.

[37] Luis Puche Rondon, Leonardo Babun, Ahmet Aris, Kemal Akkaya, and Arif Selcuk Uluagac. Poisonivy: (in)secure practices of enterprise iot systems in smart buildings. Proceedings of the 7th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, 2020.

[38] Michael Rubinstein et al. Analysis and visualization of temporal variations in video. PhD thesis, Massachusetts Institute of Technology, 2014.

[39] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015), pages 1–17, 2015.

[40] Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick Mcdaniel, Engin Kirda, and Arif Selcuk Uluagac. Kratos: multi-user multi-device-aware access control system for the smart home. Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020.

[41] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "it would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In CHI Conference on Human Factors in Computing Systems, pages 1–13, 2022.

[42] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. Are those steps worth your privacy? fitness-tracker users' perceptions of privacy and utility. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., 5(4), dec 2022.

[43] Alexandra Voit, Dominik Weber, Yomna Abdelrahman, Marie Salm, Paweł W. Woźniak, Katrin Wolf, Stefan Schneegass, and Niels Henze. Exploring non-urgent smart home notifications using a smart plant system. In 19th International Conference on Mobile and Ubiquitous Multimedia, MUM '20, page 47–58, New York, NY, USA, 2020. Association for Computing Machinery.

[44] Andreas Wagner, William O'Brien, and Bing Dong. Exploring occupant behavior in buildings. Wagner, A., O'Brien, W., Dong, B., Eds, 2018.

[45] Tong Wu, Murtadha Aldeer, Tahiya Chowdhury, Amber Haynes, Fateme Nikseresht, Mahsa Pahlavikhah Varnosfaderani, Jiechao Gao, Arsalan Heydarian, Brad Campbell, and Jorge Ortiz. The smart building privacy challenge. In Proceedings of the 8th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, pages 238–239, 2021.

[46] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In Proceedings of the 2019 chi conference on human factors in computing systems, pages 1–12, 2019.

[47] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW):1–24, 2019.

[48] Shikun Zhang, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh. "did you know this camera tracks your mood?": Understanding privacy expectations and preferences in the age of video analytics. Proceedings on Privacy Enhancing Technologies, 2021(2):282–304, 2021.

[49] Shikun Zhang, Yuanyuan Feng, and Norman Sadeh. Facial recognition: Understanding privacy concerns and attitudes across increasingly diverse deployment scenarios. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021), pages 243–262, 2021.

A. Background Details of Participants

In Figure 5 and Figure 6, we show participants' level of confidence with the IoT technologies and participants' understanding of the IoT technologies, respectively.

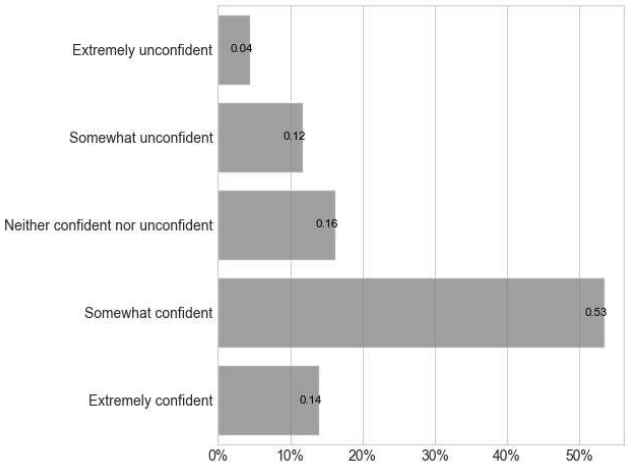

Figure 5. Participants' level of confidence with the IoT technologies on a 5-likert scale (1-Extremely unconfident to 5-Extremely confident).

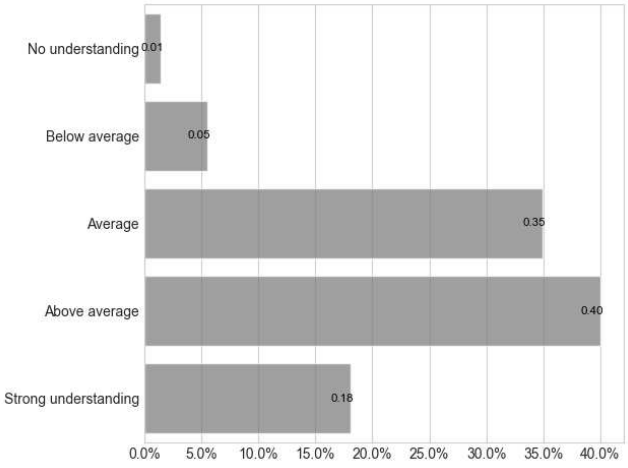

Figure 6. Participants' understanding of the IoT technologies on a 5-likert scale (1-No understanding to 5-Strong understanding).

B. Survey Instrument

B.1. Screening

1. **Which of the following working environments best describe where you have worked in or are currently working in? (Choose all that apply)**
   - ☐ I work from home
   - ☐ I have a private office to myself
   - ☐ I share a private office with some colleagues
   - ☐ I work in an open workspace with a designated desk
   - ☐ I work in an open workspace without a designated desk
   - ☐ I work outdoors
   - ☐ I work in a retail/service sector (e.g., restaurants, retail stores, grocery stores)
   - ☐ Other: _____

B.2. Main Survey

— Background and Awareness Questions —

2. **What devices do you notice at your workplace? (Choose all that apply)**
   - ☐ Camera
   - ☐ Motion sensor
   - ☐ Energy sensor
   - ☐ Water sensor
   - ☐ Light sensor
   - ☐ Temperature sensor
   - ☐ Smart TV
   - ☐ Smart speaker
   - ☐ Other: _____
   - ☐ None
3. **Are you aware of the devices' data collections at your workplace?**
   - ☐ Yes
   - ☐ No

— Perception of Data Collection Questions —

- Scenario 1 (Bluetooth beacons): Suppose your employer installs Bluetooth beacons (devices that wirelessly broadcast a unique identifier to nearby electronic devices) at your workplace. These beacons are used to collect location and movement information to understand how the space is being used.)
- Scenario 2 (Cameras): Suppose your employer installs video surveillance cameras at your workplace that collect photo/video footage to ensure workplace security.
- Scenario 3 (Smart meters): Suppose your employer installs smart meters at your workplace that collect data about human activities and resource usage (e.g., energy consumption, bathroom usage) to monitor and optimize the building's resource consumption.

4. **In the scenario, who do you think will have access to the collected data about you? (Choose all that apply)**
   - ☐ My building manager
   - ☐ My supervisor
   - ☐ The government
   - ☐ The manufacturer of the devices

□ My company
□ Myself
□ Other: _____

5. In the scenario, who are you comfortable with having access to the collected data about you? (Choose all that apply)
□ My building manager
□ My supervisor
□ The government
□ The manufacturer of the devices
□ My company
□ Myself
□ Other: _____

6. In the scenario, who do you think will benefit from having access to the collected data about you? (Choose all that apply)
□ My building manager
□ My supervisor
□ The government
□ The manufacturer of the devices
□ My company
□ Myself
□ Other: _____

7. In the scenario, which of the following purposes do you think the collected data about you might be used for? (Choose all that apply)
□ User profiling
□ Localization
□ Enforcing policies
□ Improving smart devices
□ Other: _____
□ None

— Notification Preferences Questions —

Note that for post-scenario, we replace "at your workplace" with "in the scenario" to apply the context.

8. Do you want to be notified about the presence of the devices collecting data about you at your workplace?
□ Yes
□ No

9. Please briefly explain why you want (or why you don't want) to be notified:

_____

10. At your workplace, which of the following do you want to be notified about? (Choose all that apply)
□ Presence of data collection (including types of data being collected)
□ Purposes for which your data can be used
□ How your data can be used
□ For how long your data can be retained
□ Who can access your data
□ None of the above

11. How do you want to be notified? (Choose all that apply)
□ Physical sign
□ Mobile app
□ Website
□ Email
□ Paper document
□ Other: _____

— Demographic Information —

12. With which gender identity do you most identify?
□ Male
□ Female
□ Other: _____
□ Prefer not to answer

13. What is your age group?
□ 18 - 24 years old
□ 25 - 34 years old
□ 35 - 44 years old
□ 45 - 54 years old
□ 55 - 64 years old
□ 65 - 74 years old
□ 75 years or older
□ Prefer not to answer

14. What is the highest level of education you have completed?
□ Some high school
□ High school graduate
□ Some college
□ Associate's degree (2-year college)
□ Bachelor's degree (4-year college)
□ Graduate degree (Masters, PhD, MD, JD, etc.)
□ Other: _____
□ Prefer not to answer

15. What is your annual personal income before taxes (USD)?
□ Less than $10,000
□ $10,000 - $24,999
□ $25,000 - $49,999
□ $50,000 - $74,999
□ $75,000 - $99,999
□ $100,000 - $149,999
□ $150,000 and greater
□ Prefer not to answer

— Confidence and Understanding —

16. How confident are you with the Internet of Things technologies in general (e.g., voice assistants, smart security camera, drones, smart watches, virtual reality glass, etc.)?
□ Extremely unconfident
□ Somewhat unconfident
□ Neither confident nor unconfident
□ Somewhat confident
□ Extremely confident

17. How would you describe your understanding of the Internet of Things?
□ No understanding
□ Below average
□ Average
□ Above average
□ Strong understanding