Privacy Solution or Menace? Investigating Perceptions of Radio-Frequency Sensing

Maximiliane Windl[1,2], Omer Akgul[3,4], Nathan Malkin[5], Lorrie Faith Cranor[3]
[1]*LMU Munich* [2]*Munich Center for Machine Learning (MCML)*
[3]*Carnegie Mellon University* [4]*RSAC Labs* [5]*New Jersey Institute of Technology*

Abstract

Radio-frequency sensors are often introduced as privacy-preserving alternatives to cameras, as they enable similar use cases without relying on visual data. However, researchers argue that radio-frequency sensors cause privacy risks similar to cameras and even introduce additional risks. We conducted in-depth interviews ($N = 14$) and a large-scale vignette survey ($N = 510$) to understand people's perceptions and privacy concerns around radio-frequency sensing. Most interviewees were initially unaware of the full capabilities of radio-frequency sensing but expressed nuanced concerns upon learning more. Our survey revealed that, while people expressed concerns, they mostly preferred radio-frequency sensors over cameras in private locations. However, they preferred cameras when considering radio-frequency sensing from a neighbor's perspective and in security-relevant situations. Protective measures can reduce concerns, but the best protection depends on the context. Our findings can inform educational and legislative efforts to ensure a privacy-preserving future with radio-frequency technology.

1 Introduction

Radio-frequency (RF) sensing systems interpret RF waves, such as Wi-Fi or millimeter waves, to understand their environment. These systems are emerging as significant alternatives to many traditional single-purpose sensors, such as motion detectors, thermal sensors, and especially cameras, which are widely deployed in smart homes. Unlike traditional sensors (typically task-specific products), RF sensors can replicate many of these functions at a lower cost, often leveraging existing on-device communications hardware. While many commercially available smart home products still rely on cameras, RF sensors are being deployed rapidly, for example, in smart sleep monitors [66] or home security systems [51]. This is because many features that require cameras can be more efficiently realized with RF sensors, such as motion detection [33, 43], fall detection [54, 72], and even identifying people [63, 82] and recognizing emotions [85]. RF sensors offer other advantages over cameras: they are not sensitive to lighting and their functionality is unhindered by most physical objects (e.g., walls) [1, 3]. Moreover, as RF sensors do not rely on visual data, RF researchers frequently market them as privacy-preserving relative to alternatives [28, 32, 64]. However, declaring RF sensing privacy-preserving might be misleading, as much of the same information that cameras can infer can also be derived from RF sensors (and sometimes even more).

Indeed, with non-RF sensors, research has found that users have many privacy concerns, influenced by contextual factors [22, 37]. Hence, similar but unique frameworks might govern RF sensing perceptions. If so, regulation might be needed to limit excessive user harm. As the privacy-invasive nature of cameras has been well recognized, regulations in many jurisdictions mandate that people are informed of video monitoring. No such regulations currently exist for RF sensing, even though research documents the privacy risks it introduces [42, 47, 68]. In contrast to sensor-specific data, such as images captured by cameras or heart rate data from biometric sensors, the data generated by RF sensors typically contains multiple sensitive data types simultaneously, such as motion, identity, and even emotional states, making it even more concerning when leaked [68, 87]. In response, prior work developed technological defenses, for example, by using perturbations, filtering, and obfuscation techniques [42, 44, 62].

Although researchers have recognized the privacy risks introduced by RF sensing and developed technological defenses, no research has directly investigated people's perceptions of RF technology or defenses against it. Thus, it remains unclear whether users perceive RF sensing as more privacy-preserving when fully informed of its capabilities. We address this gap through the following research questions:

RQ1 How do people perceive the capabilities and privacy risks of RF sensing, and do they differ from cameras?

RQ2 How much do **contextual factors** affect comfort with RF sensors and preferences for RF sensors vs. cameras?

RQ3 How much do **protective measures** affect comfort with RF sensors and preferences for RF sensors vs. cameras?

We answer these questions through a two-part study. First, we conducted in-depth interviews ($N = 14$) to gauge people's knowledge of RF sensing and their reactions to the capabilities and privacy risks in various scenarios. Digging deeper, we ran a large-scale online vignette survey ($N = 510$) to find how much contextual factors influence comfort and preferences.

In our interviews, almost no participant initially knew about RF sensing. However, they expressed nuanced privacy concerns after we explained the technology, suggesting that RF sensing is not a privacy panacea. Moreover, introducing concrete RF sensing use cases to participants revealed contextual factors that influenced concerns. We varied these factors in our online vignette survey to measure their precise impact on comfort. We found that, even though participants expressed concerns, they still preferred RF sensors over cameras in private locations. Yet, outside their homes, especially for security-relevant use cases and when RF technology was deployed by neighbors, most people preferred cameras. We further found that most protective measures improve RF sensing comfort but are dependent on use case and perspective.

To the best of our knowledge, this paper is the first to conduct an in-depth investigation of people's perceptions of RF sensing, quantifying the extent to which contextual factors impact privacy concerns. In addition, this paper identifies the leading protective measures and their applicability in different contexts. We close by discussing how our findings can impact education and public policy. As such, our paper contributes to a privacy-preserving future with radio-frequency sensing.

2 Related Work

RF sensors create distinct privacy challenges, separating them from other sensors such as cameras and microphones. While cameras require line-of-sight and light, RF sensors are able to sense through physical barriers, regardless of light. This uniquely positions RF sensing in the privacy and surveillance discourse. Table 1 summarizes these distinctions, comparing the capabilities of IoT sensors commonly used in scenarios relevant to our study: security, health, and crowd analytics.

Below, we present research on RF sensing capabilities and risks, summarize attacks and countermeasures, and discuss users' privacy concerns related to sensing technologies.

2.1 RF Sensing Capabilities

RF sensing systems emit signals in all directions. When these signals encounter physical objects or people, they are scattered and reflected back to the sensor, depending on the properties of the object, such as its material and movement [41, 76]. By analyzing these reflected signals, the RF sensor can infer rich information, such as emotions [85], biometrics [19], and activities [60], which in turn enables numerous functions. Moreover, RF sensors can operate through nonmetallic solid objects and walls [1, 7, 15, 88], and, unlike typical visible-light cameras, they are not sensitive to lighting conditions. Like cameras, RF sensors can function in both spacious public areas and more private settings [83]. While RF sensing systems introduce privacy risks, many researchers still describe them as privacy-preserving alternatives, highlighting that they do not capture visual data [2, 27, 28, 53, 64]. In this paper, we investigate whether people actually do perceive RF sensing to be privacy-preserving.

RF sensing enables a variety of advanced surveillance capabilities. RF sensors are, for example, capable of tracking (multiple) people [2, 15, 64]. For instance, Adib and Katabi [1] identified the number of people in a room, their location, and gestures. Similarly, Pu et al. [56] were able to recognize nine different gestures anywhere in a house, and Tan and Yang [67] detected subtle finger movements. Such fine-grained detection also enables keystroke recognition [4]. Research has shown that, by extracting biometric data (body size and shape), it is possible to identify individuals [27]. Additionally, Ozturk et al. [52] developed a method to record sound with RF sensors, even through soundproof barriers. Collectively, these allow RF sensing systems to find applications in security-relevant use cases, for example, detecting intruders [13].

RF sensing also has many applications in healthcare. Wang et al. [72], for example, identified daily activities such as walking and sitting, as well as abnormal activities, such as falling. Shah and Fioranelli [61] used RF sensing to monitor heart rate, chest movement, body structure and orientation, sleep patterns, and breathing. Hsu et al. [34] developed a sleep monitoring system to monitor breathing, bed location, and bed entries/exits, and classify sleep and awake periods. These systems can also work for multiple users at a time and operate at long distances. Yue et al. [80], for example, developed a breathing monitor that accurately distinguished people sharing a bed. Similarly, researchers developed breathing [81] and heart rate monitors [3] that work for multiple people. RF sensors can also identify emotions by recognizing variations in heartbeats [85] or via gesture and pose recognition [58]. RF data might even detect Parkinson's disease [77]. Our study is informed by the range of demonstrated capabilities of this technology, with use cases reflecting both current realities and near-future possibilities.

2.2 RF Sensing Technological Defenses

In response to privacy risks, researchers developed technological countermeasures such as obfuscating or encrypting RF signals. For instance, Qiao et al. [57] developed PhyCloak, a system that distorts the part of the signal that could leak physical signatures of humans. Luo et al. [45] countered unauthorized eavesdropping while retaining the sensing capabilities by physically encrypting Wi-Fi channels, and Liu et al.

	RF Sensor	Camera	Motion Sensor	Microphone
Data Type	RF signals	Visual data	Motion	Audio signals
Lighting needs	Works in all lighting conditions, including complete darkness	Requires external lighting; limited use in low-light	Works in all lighting conditions, including complete darkness	Works in all lighting conditions, including complete darkness
Awareness	No visible indicators; can be hidden or placed behind walls and still function	Visually detectable with lens or indicator light features, though they can sometimes be hidden	Typically inconspicuous; often integrated into devices or fixtures	Detectable if standalone but often perceived as passive when integrated into devices
Range and Coverage	Penetrates obstacles (e.g., walls); monitors large areas (multiple rooms) within signal range	Limited to the camera's line-of-sight; covers a single area or room	Limited to a few meters; obstructed by barriers	Limited by audio propagation; significantly reduced by walls or barriers
Technical Limitations	Sensitive to overlapping signals and material properties of obstacles (e.g., metallic); interference from environmental noise	Requires sufficient lighting; limited in low-light conditions; line-of-sight required	Limited to line-of-sight; cannot detect through walls; prone to false triggers from environmental factors (e.g., pets, wind)	Limited by sound propagation; range reduced by walls and barriers; susceptible to overlapping sounds and background noise
Data Sensed/ Inferred	Motion, activities, biometrics (e.g., breathing, heart rate, identity), emotions	Motion, activities, biometrics (e.g., breathing, heart rate, identity), emotions, color, written text	Motion and presence	Conversations, activities (e.g., footsteps), emotions, identities
Privacy Implications	Collects various data (e.g., biometrics, activities) covertly, operates through physical barriers, and monitors multiple rooms without user awareness	Collects various visual and contextual data, including identifiable imagery; limited to line-of-sight and lighting conditions, making it more noticeable	Limited to basic data collection (motion and presence only) within the immediate vicinity of the sensor; potential for false positives	Captures audio data (e.g., conversations, ambient sounds) within the immediate vicinity; lacks visual imagery but susceptible to unnoticed passive recording

Table 1: Comparison of RF sensors, cameras, motion sensors, and microphones.

[42] developed a fine-grained filter that applies perturbation to disable some functions while leaving others unaffected. Liu et al. [44] used methods to erase behavior data from RF signals while enabling user authentication. Other approaches included an RF sensing shield that blocks sensing outside a perimeter [52, 78] or injecting decoy activities [62].

However, Nguyen et al. [49] argue that none of these methods can stop tracking fully, criticize the lack of commercial implementations, and note that detecting illegal tracking in sensor-rich environments remains a challenge. Thus, they recommend investigating effective RF signal encryption and access control at the physical network layer. In our work, we investigate the impact of these proposed defenses (e.g., shields [52] and filters [44]) on people's perceptions.

2.3 Perceptions of Sensing Technology

While there is no research on privacy perceptions of RF sensing, a large body of work has investigated privacy concerns in smart environments. People often feel uneasy or concerned in the vicinity of sensing technology [48, 73], reporting concern about the disclosure of personal data without consent [38, 39]. There are several contextual factors that impact privacy concerns [22, 37]. Emami-Naeini et al. [22], for example, found that people were more comfortable with data collection in public, more likely to consent to data collection they considered beneficial, and more likely to want notifications about data uses they were uncomfortable with. In addition, the sensor type impacts concern: while people accept temperature and motion sensors [10, 16, 86], they express strong concerns about cameras and microphones [12, 73]. Prior research identified bystanders as an especially protection-worthy user group, as they are typically unable to exert control and are often oblivious to being tracked [40, 79].

Studies explicitly focusing on surveillance cameras found that context had a strong impact on concerns. Impactful factors included the purpose of data collection, where collection and processing happens, and who has access to the recordings [14, 84]. Pierce et al. [55] explored the social and ethical issues raised by smart cameras, including the tensions between users and bystanders with diverging preferences and the potential violation of social boundaries. While some cameras go unnoticed, people who are aware of cameras practice self-regulating behaviors. Caine et al. [11], for example, found that older adults engaged in privacy-enhancing behaviors around cameras, such as blocking the camera's view or hiding things in the room. However, older adults have been found to be willing to sacrifice privacy if it means increasing their autonomy through health-related technology [69].

Little research has explicitly investigated RF sensing perceptions. Singh et al. [65] studied whether the human interpretability of sensor data is the primary factor driving privacy concerns. They used mmWave sensors as an example of devices that collect non-human-interpretable data, comparing these sensors with cameras and Wi-Fi routers in an online survey (n=160). Their findings indicate that with non-human-interpretable data, the inferences drawn from the data play a more significant role in concerns than interpretability. However, their study does not explore broader privacy perceptions of RF technology beyond data interpretability.

In contrast to prior work, our research provides a comprehensive exploration of privacy perceptions surrounding RF sensing. Unlike prior studies, we examine diverse contexts, explore the impact of protective measures, and highlight

context-dependent preferences for RF sensors over cameras. We employ qualitative and quantitative methods and use a representative sample for improved generalizability.

3 Interview Study Method

Since no prior work investigated users' perception of RF sensing, our first study took an exploratory approach. We conducted 14 semi-structured interviews to understand perceptions of the capabilities and privacy risks of RF sensing. We gave participants a brief, non-technical introduction, then asked about their privacy perceptions of RF sensing, how different situations influence these perceptions, differences in reactions to cameras and RF sensors, and preferences for notifications and regulations **(RQ1)**. We piloted the interview with two colleagues without RF sensing experience and one RF sensing expert, revising our protocol based on their feedback.

3.1 Interview Protocol

Interviews were conducted remotely in three parts: explanations, use cases, and preferences. Before starting, we ensured participants understood the study and consented. Interviews took approximately one hour, and we compensated participants with $16 via Prolific.

Explanations. The first part aimed to gauge our participants' existing RF sensing knowledge and educate them so that all participants would share a baseline understanding. We asked whether participants were familiar with RF sensing, Wi-Fi sensing, or millimeter wave sensing and, if so, to explain their understanding of it. Regardless of the participant's response, we continued with our detailed, slideshow-assisted explanation to ensure a common level of understanding.

We carefully refined our explanation to minimize bias. The explanation focused only on the capabilities of RF sensing and explained what the technology can and cannot do without referencing privacy implications. Our piloting confirmed that this approach supported balanced views. Pilot participants expressed a range of unique opinions, some intrigued by RF sensing and others voicing reservations. This diversity of opinions also suggests that we did not influence participants toward a particular stance.

The slideshow we used during the interview included images of cameras and RF sensors, an animated GIF that illustrated RF waves, a table outlining capabilities of RF sensors versus cameras, and images representing the different scenarios. The goal was to make it easier for participants to imagine themselves in the situations, while also helping them follow our explanations. The explanation related RF sensing to motion sensors and radar technology, as we assumed widespread familiarity with them. Next, we compared cameras and RF sensors and gave concrete examples of what each can infer.

We ensured that people understood our explanation by asking them to explain RF sensing and to describe how it differs from sensing with cameras. We corrected any misconceptions and repeated explanations whenever necessary. Finally, we asked participants to share their initial reaction to RF sensing. Please refer to OSF (see Section 11) for the full interview protocol, including our explanations and slideshow.

Use Cases. In the second part, we gathered insights on how contextual factors influence perceptions of RF sensing. We examined reactions to four scenarios: a health-monitoring system in a private home (*Private Health*), a security system for private home use (*Private Security*), a security system that monitors (e.g., for violence) a stadium (*Public Security*), and a system providing analytical insights into crowd behavior in a stadium (*Public Analytics*). We chose health and security scenarios because these are common applications of RF sensing. In addition, our scenarios contrast different levels of urgency and benefit (health vs. security vs. analytics). See Appendix Table 4 for the exact descriptions.

We used a Latin square design for the scenario order to prevent order effects. We examined different perspectives within each scenario. For *Private Health* and *Private Security*, we asked participants to adopt the system owner's perspective. For *Private Health*, we asked them to imagine recommending the system to an older adult. In addition, we asked participants to imagine being a visitor or living next to a neighbor with an RF sensor. For *Public Analytics* and *Public Security*, we only asked about the visitor's perspective. For each scenario and perspective, we asked participants whether they would prefer a camera or RF sensor and to explain why. When discussing the bystander perspectives, we additionally asked whether the system owner would have any obligation towards them (e.g., to inform them about tracking). To limit bias, we avoided explicitly asking about privacy during the discussions.

Preferences. In the final part of the interview, we asked participants to reflect on situations where they would prefer an RF sensor over a camera. We then asked about notification preferences in detail (e.g., when and how often). We also asked participants whether there should be laws or regulations about RF sensing and, if not already discussed, to consider how RF sensing could impact privacy. We asked participants for any closing remarks before we thanked them, stopped the audio recording, and ended the interviews.

3.2 Participants

We recruited 14 participants on Prolific who spoke English fluently, resided in the US, and were willing to be interviewed. We used Prolific's screeners to acquire a sex-balanced sample: seven female and seven male participants between 23 and 63 years old ($M = 39.8$, $SD = 13.6$). Ten participants had full-time jobs, two part-time, and two were job-seeking.

3.3 Data Analysis

We recorded a total of 10.18 hours ($M = 43.6$ minutes, $SD = 9.6$ minutes) of interview audio, which we transcribed using Zoom's cloud transcription and an offline instance of Whisper. After manually correcting transcripts, we performed thematic analysis [8]. To increase reliability, two researchers independently coded two random interviews, after which they discussed codes, resolved ambiguities, and formed a codebook. After that, they coded a third interview using this codebook and again discussed codes. Finally, one researcher coded the rest of the interviews before three more researchers joined to form code groups and overarching themes. We repeatedly revised these themes by comparing code snippets. This process resulted in four themes, 18 code groups, and 273 codes.

4 Interview Findings

We identified four main themes: RF Sensing Privacy Concerns, Camera vs. RF Sensing, Notifications, and Laws/Regulations.

4.1 RF Sensing Privacy Concerns

Participants had diverse opinions on RF sensing, highlighting the privacy-utility trade-off. Concerns were dependent on the scenario, type of data collected, location, exposure frequency, notification, protective options, trust in device owner, and user-specific factors.

Several participants were generally more comfortable with medically-required systems than with other use cases (P3, P4, P13): *"I would be perfectly fine with that. It's for their health, that is paramount"* (P13). Participants were also comfortable with RF sensing in the security scenario, expressing willingness to trade privacy for security (P1, P11). In contrast, participants were highly concerned when a neighbor had RF sensing, fearing it could capture data from their own apartment (P2, P4, P7, P11). Participants were specifically concerned about neighbors receiving health data (P2) or private activities: *"They can tell your movements and... you know, there's always romantic times"* (P6). Similarly, participants were concerned about RF sensor exposure as a visitor, where private information may be uncovered (P2, P7), such as early-stage pregnancy.

Participants frequently brought up the type of data collected, inferred, and stored (P2, P4, P8, P12). They were especially concerned about biometric data collection (P4, P8) and user identification (P8, P11).

Location also impacted concerns. Participants did not mind being monitored in public, as they expected it (P3, P5, P10, P11). Yet, even in public, people expressed concerns about data collection in private areas, such as restrooms (P2). Exposure frequency also played an important role: *"Unless it's a place I spend a lot of time. I probably really don't care"* (P12).

However, participants were generally accepting of RF sensing systems if they were notified in advance, if they knew what information could be collected and inferred, and knew where data is processed and stored (P3, P10, P11): *"Similar to disclosures on a website... I would want to know where that was going, how it was being interpreted, and by whom"* (P11). Participants also felt that protective options, such as setting a sensing perimeter or regulations, would mitigate privacy concerns (P4, P8, P12).

Many participants emphasized that their trust in the device owner impacts their concerns (P1, P2, P8, P10, P11, P13). While participants were generally comfortable with RF sensors of trusted entities, many expressed concerns about systems that belonged to an untrusted owner: *"If it's the neighbor's system, I'm okay with it. If it's Big Box security company storing the data and then selling it, I'm not okay with it"* (P8).

Finally, participants discussed personal factors, such as familiarity with RF sensing (P4, P8). Participants expected concerns to diminish with familiarity (P8). P4 highlighted additional concerns for at-risk populations: *"I could see it being a problem for people of color... LGBT, people who are at risk for being profiled or monitored more."*

4.2 Camera vs. RF Sensing

When deciding between cameras and RF sensors, participants weighed various factors against each other. The decision process generally involved utility and privacy considerations.

Almost everyone knew cameras provide visual evidence, which they desired for security-relevant scenarios (e.g., pursuing criminals) (P1–P5, P7, P8, P9, P11–P14). In contrast, some preferred the RF sensor because it did not collect visual data, giving them a feeling of privacy (P3, P4, P6, P8, P12): *"I'm somebody who likes to walk naked in my house... so I don't want cameras"* (P3).

At the same time, several participants preferred the RF system as it would not have blind spots, in contrast to cameras (P6, P9–P13). This is especially relevant for the health use case: *"If they fall and say they render themselves unconscious, but they're still breathing, you know, you'd be able to tell"* (P11). In addition, the RF sensor cannot be easily obscured, is not sensitive to bad visibility, and might still be able to recognize individuals if they mask themselves (P1, P6, P13): *"Essentially... anyone covering the camera and whatnot. Or if I were to get a package, and someone actually tries to hide themselves taking a package"* (P6).

Using similar reasoning, some preferred the camera to restrict the field of view (P4, P6, P13): *"That way I could limit it to... looking outside the house rather than being aware of everything"* (P4). Participants also preferred their neighbor to use a camera as it would not penetrate walls and infringe on privacy (P10–P14). Interestingly, P12 preferred the RF sensing system as a hacker could not make sense of the data: *"I just don't see how even the average... hacker, who might hack*

into a home system—what they would do with that data."

Finally, most participants preferred whichever system they believed would offer more accurate data and provide the most utility in the specific situation (P2, P4, P6–9, P11, P12, P14).

4.3 RF Sensing Notifications

All participants wanted to be notified about RF sensing but differed on preferences for modalities, frequency, and who should provide them. In general, the greater someone's privacy concern, the greater their desire to be notified.

Despite wanting notifications, participants noted that private individuals are not obligated to provide them (P1, P3, P5, P6, P10, P12). Participants especially wanted notifications in private spaces (P2, P4, P12, P14), but they accepted not being informed in public, where they expected monitoring (P3, P10, P11, P12). In addition, notification desire was mediated by privacy-relevant factors such as trust in the device owner (P5, P11); personal data collection, inferences, storage (P2, P4, P8, P11, P12); and RF exposure frequency (P7).

Several notification mechanisms were discussed. Most suggested public signage, inspired by video surveillance disclaimers (P2–P5, P7, P8, P11): *"No more than 'smile, you're on camera.' You know, we see those signs all the time"* (P11). In private settings, participants expected their neighbor or host to verbally inform them about such a system (P7, P12, P14): *"I would prefer if they just knocked on my door and said: Hey, just so you know, I've installed some sensors"* (P14). However, they only expected such verbal notifications if they had a friendly relationship with the owner; otherwise, participants again preferred signage (P4). Some suggested push notifications (P6, P11, P13). However, others noted that those get overwhelming quickly: *"[It's] insanely, incredibly prevalent, right? . . . it would go off constantly"* (P1). Other suggestions included on-demand lookup where the user would scan (e.g., through an app) for RF sensors (P1), email notifications (P10), social media (P10), or during Wi-Fi sign-in (P2).

Notification frequency preferences included: once if the system owner is trusted (P4, P10), every time when entering the RF tracking range (P11), and only when changes occurred in a previously consented tracking space (P4). Most participants believed the system owner should deliver notifications (P2, P3–P7, P10, P12–P14), whereas others believed the manufacturer (P10), the data processor (P11), or even the Wi-Fi carrier (P6) should.

4.4 RF Sensing Laws and Regulations

Participants proposed instituting laws around RF sensing, especially to protect sensitive data like demographic (P4), medical (P6, P14), activity (P14), and biometric data (P11). They wanted regulations in places with elevated expectations of privacy (P4, P12, P13): *"I think your home is your sanctuary. Any sensing device that can penetrate it needs to be regulated"* (P13). P1, alarmed about potential inferences, called for safeguards to prevent criminals from purchasing or obtaining RF systems, and other participants suggested implementing notifications similar to those used in video surveillance systems (P4, P7, P8). In contrast, P5 proposed a law that would arguably make the surveillance more invasive: *"You're required to tell someone: I'm concerned of Mr. Smith next door. He's been very depressed. But I'm also on my monitor, I notice this is his emotions."*

5 Online Vignette Survey Method

Through interviews, we uncovered factors that influence perceptions of RF sensing; however, the extent of this influence is unclear. Hence, we conducted a large-scale online between-subjects vignette (17 scenarios across three dimensions) survey on Prolific to answer our second and third research questions. We recruited 510 participants and asked each to answer questions about one scenario. First, we provided participants with a text version of the RF sensing explanation, refined from our interview study. After a successful comprehension check, participants were randomly assigned one of 17 vignette descriptions. They then answered questions about the technology in the vignette, responding to questions twice in random order: once for a camera and once for an RF sensor. Following this, we asked how protective measures affect their perceptions. Finally, we asked about participants' ownership of camera systems, demographics, and technology proficiency. Refer to OSF (see Section 11) for the full questionnaire.

5.1 RF Sensing Explanation

Based on our interview observations, in which no participant initially knew the full capabilities of RF sensing, we started by thoroughly explaining RF sensing technology in the survey, as it is essential for participants to have a consistent baseline understanding of the technology. Building on our interview experience, we used a refined explanation of RF sensing in the survey: we removed the motion sensor analogy and clarified RF sensing's ability to distinguish individuals, by noting that training with additional information is needed to link individuals with names. To ensure accurate understanding, we asked participants to correctly complete a comprehension check before proceeding. The check included four multiple-choice questions and one true/false question. These questions were straightforward for those who had read the provided explanation (which was available during the check). In addition, we initially added two free-text questions (however, those were not part of the comprehension check). We asked participants to explain RF sensing capabilities and to explain the difference between RF sensing and cameras. If participants answered any closed-ended comprehension check incorrectly,

they had a second chance. If their answer remained incorrect, we ended the survey.

Piloting. Given the importance of our explanations, we extensively tested our approach by gathering feedback from five HCI researchers and refining questions based on feedback. We then tested our survey on incremental batches of Prolific participants. Two of the first five participants likely used LLMs in their responses, as their responses were flawless, with GPT-like characteristics (e.g., punctuation, grammar, wordiness). Thus, we introduced LLM countermeasures: asking for self-attestation of no LLM use (similar to "oath taking" [35]), disabling paste, and introducing a keystroke counter. We then recruited 15 additional participants. None of them appeared to have used LLMs and only two would have been screened out, which we considered an acceptable outcome. We did not include their responses in our analysis. For the final survey, we added a question asking whether participants had heard about RF sensing and, if so, to briefly describe the capabilities. Regardless of the response, we showed the explanation to ensure a common understanding. Further, we only kept one free-response question, where we asked participants to explain the differences between cameras and RF sensors.

5.2 Vignettes

We investigated factors impacting interview participants' RF sensing perceptions: **use case, perspectives,** and **locations**. We used the same **use cases** as the interviews: *Private Health* monitoring, *Private Security*, *Public Security*, and *Public Analytics*. Since different **perspectives** led to varying preferences, we used our previous interview perspectives, where the participants: imagined they owned such a system (*Owner*), imagined they were visiting a place with such a system (*Visitor*), and imagined that their neighbor installed such a system (*Neighbor*). Finally, we used **locations** that were perceived with different sensitivities in prior work [73]: the *bathroom* as a sensitive location and the *hallway* as a non-sensitive location. In addition, we added the *front porch* for *Private Security* as it fits the narrative for both cameras and RF sensors. We combined these factors to construct our scenarios. However, not all combinations are realistic, such as a health monitor placed on a front porch. After eliminating such instances, we used 17 scenarios in our survey (see Appendix Table 5).

5.3 Questionnaire

After participants read our RF sensing explanations and passed the comprehension check, we randomly presented one of the 17 scenarios and asked participants to read and immerse themselves in it. As we used a between-subject design, every participant saw and rated one scenario. To ensure that participants had understood the scenario, we asked two reading check questions that they had to answer correctly to continue.

Next, we asked participants about scenario-specific preferences between cameras and RF sensors. Then, we asked the same set of questions twice, once for a *camera* and once for an *RF sensor-based* system (order was random). We asked (1) how useful participants found the system, (2) how comfortable they felt with the technology and how sensitive they considered the (3) collected data, and (4) the location of the system. We asked about perceived comfort and technology preference, as we had found in the interviews that these did not necessarily correlate; people could be concerned about a device but still prefer it over another. Based on interview findings, we also asked about utility, data sensitivity, and location sensitivity. We asked all questions on five-point, fully labeled Likert scales. We used bipolar scales wherever possible. Refer to OSF (see Section 11) for the full question text.

Our next section investigated how changes to the scenario affect perceptions. Specifically, we asked whether protections would affect comfort or technology preference. These protections were based on those identified by interview participants and discussed in prior work: an *RF shield* that blocks RF sensing outside a perimeter, *algorithmic filtering* that removes irrelevant personal data (e.g., only stores older adult data in private health scenario), a *law* that prohibits unauthorized data use, a *reduced exposure frequency* to "only once or twice," and a *notification* about RF sensing.

In the final section, we asked participants about their ownership of camera-based systems, collected demographic information, and assessed their tech-savviness [59].

5.4 Participants

We used Prolific to recruit a U.S. demographically-representative sample. Participants were recruited in batches until we obtained 30 ratings per scenario. After each batch, we checked whether participants failed the comprehension check twice. If so, we asked them to return their submission and excluded them from both the analysis and the reported sample size. In total, we excluded 161 participants. This resulted in a final sample of 510 participants, all of whom passed the comprehension check. To verify that the groups did not differ significantly in demographics, we conducted Chi-square tests for categorical variables (gender, tech-savviness, and education) and an ANOVA for age. All tests were non-significant ($p > .05$), indicating no statistically significant demographic differences between groups.

Our participants were between 18 and 95 years old ($M = 45.39$, $SD = 15.71$), mostly male ($N = 252$) or female ($N = 246$), some ($N = 10$) non-binary, one self-described as dual gender, and another as transgender. Most ($N = 191$) held a bachelor's degree, some college no degree ($N = 114$), or held a master's degree ($N = 67$). Participants were moderately tech-savvy: most ($N = 220$) sometimes provided tech advice. Many were familiar with camera-based smart devices, with an average of 0.75 devices owned per person ($SD = .17$). Exclud-

ing those who owned none ($N = 240$), the majority owned a camera-based security system ($N = 225$), followed by pet surveillance cameras ($N = 60$) and cameras to monitor people in their homes ($N = 43$). Nearly half (48%) of participants reported never hearing of RF sensing before, whereas 267 (52%) said they had. To assess familiarity, we asked those who claimed they knew the technology to explain, ultimately concluding that understanding was nearly nonexistent. The survey had a median completion time of 15 minutes, and we compensated participants with $4 ($16 per hour).

5.5 Analysis

We used labeled Likert scales, yielding ordinal data: ordered but with unequal intervals [31]. Thus, we used Aligned Rank Transform (ART) ANOVAs as they allow factorial analyses (including interactions) for nonparametric ordinal data like ours [75]. For post-hoc analyses, we used the ART-C procedure [21] with Bonferroni corrections applied. We report partial eta-squared for effect size estimation. Finally, to analyze the relationship between two variables, we used Kendall's Tau. Due to the large number of results, we only report those relevant to our research questions. Refer to the supplementary material (Section 11) for all results. We thematically analyzed qualitative text responses, reusing our interview codebook due to question similarity.

6 Online Vignette Survey Results

We present RF sensing attitudes using three high-level measurements: comfort with the scenarios, preference between RF sensing and cameras, and the impact of protective measures on comfort and preference (**RQ2**, **RQ3**). Given numerous interaction effects, we often filtered the data by variables to identify trends. We contextualize the quantitative results with qualitative findings and report scenario IDs alongside participant IDs for context (see Appendix Table 5).

6.1 Context Impact on Perceived Comfort

Summary. Overall, participants felt significantly more comfortable with cameras in security-relevant scenarios, when placed outside their homes, and from a neighbor's perspective. For all non-security-relevant scenarios and especially in private locations, participants felt more comfortable with RF sensors. While our results suggest that reducing the exposure frequency is an inadequate protection measure, all other measures we asked about led to significant comfort improvements. We further found that higher perceived utility comes with higher comfort and that perceived data and location sensitivity increase concerns.

We first investigated the impact of the context factors `Sensor`, `Use Case`, `Perspective`, and `Location` on the perceived comfort. Refer to Table 2 for the statistical results and effect sizes. We found significant main effects for `Sensor`, `Use Case`, and `Location`. However, reducing the meaningfulness of these effects [30], we also found significant interaction effects for `Sensor × Use Case`, `Sensor × Perspective`, `Sensor × Location`, `Use Case × Location`, `Sensor × Use Case × Location`, and `Sensor × Perspective × Location`. To better understand these effects, we ran post-hoc tests, finding that most of the significant interaction effects were caused by the bathroom `Location` and the neighbor `Perspective`. As a result, we analyzed the data both with and without these variables included.

Factor	dfn	dfd	F	p-value	η_p^2
Sensor	1	493	80.951	<.001***	.141***
UseCase	3	493	3.199	.023*	.019*
Perspective	2	493	0.112	.894	.000
Location	3	493	28.580	<.001***	.148***
Sensor×UseCase	3	493	25.048	<.001***	.132***
Sensor×Perspective	2	493	41.215	<.001***	.143***
UseCase×Perspective	1	493	0.084	.772	.000
Sensor×Location	3	493	43.837	<.001***	.211***
UseCase×Location	3	493	6.897	<.001***	.040***
Perspective ×Location	3	493	1.131	.336	.007
Sensor×UseCase×Persp.	1	493	0.012	.914	.000
Sensor×UseCase×Loc.	3	493	10.306	<.001***	.059***
Sensor×Persp.×Loc.	3	493	3.247	.022*	.019*
UseCase×Persp.×Loc.	1	493	0.607	.436	.001
Sensor×UseCase×Persp.×Loc.	1	493	0.036	.850	.000

Table 2: ART ANOVA results for the impact of all factors on comfort, including the effect sizes, numerator degrees of freedom (dfn), and denominator degrees of freedom (dfd).

6.1.1 Comfort Without Bathroom and Neighbor

While participants were generally more comfortable with RF sensors, they tended to be more accepting of cameras in security scenarios. They were especially uncomfortable with cameras in the public analytics use case. We further found that participants are more comfortable with an RF sensor indoors, whereas they are comfortable with cameras on their porches.

We first examined our data without the factors bathroom and neighbor included and found significant main effects for `Sensor` ($F(1,232) = 8.336$, $p = .004$, $\eta_p^2 = .035$), `Use Case` ($F(3,232) = 6.9$, $p < .001$, $\eta_p^2 = .082$), and `Location` ($F(1,232) = 4.375$, $p = .038$, $\eta_p^2 = .019$), as well as significant interaction effects for `Sensor × Use Case` ($F(3,232) = 15.144$, $p < .001$, $\eta_p^2 = .164$) and `Sensor × Location` ($F(1,232) = 16.456$, $p < .001$, $\eta_p^2 = .066$). See Figure 1 (a) for a visualization of `Sensor × Use Case`. Post-hoc tests revealed that participants were significantly more comfortable with a camera in the private security ($p < .001$) and public security use case ($p < .001$) than in the private health use case and significantly more comfortable with a camera in the public security compared to the public analytics use case ($p = .01$). We further found that participants were significantly more comfortable with an RF sensor in

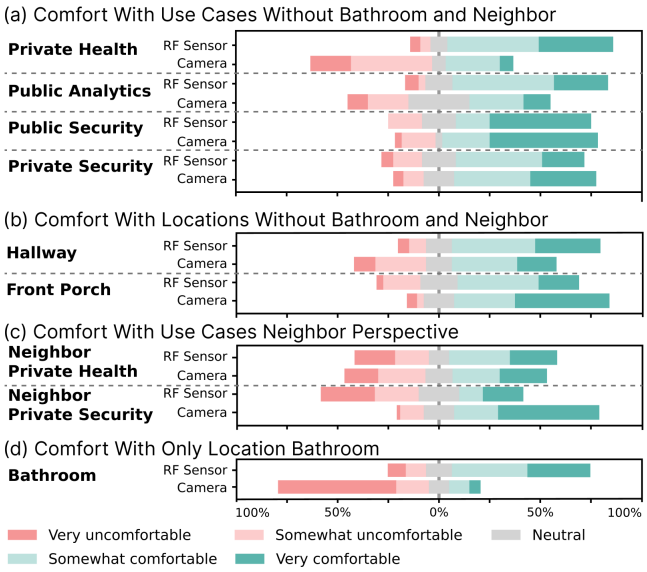

Figure 1: Comfort ratings: (a) across use cases and (b) locations (both excluding bathroom and neighbor), (c) from the neighbor perspective, (d) in a bathroom.

the private health, private security, public security, and public analytics use case than they were with a camera in the private health use case (all $p < .001$) and that they were significantly less comfortable with a camera in the public analytics than they were with an RF sensor in the private health ($p = .008$) or public security ($p = .045$) use case.

Participants explained their preference for cameras in security scenarios with the fact that they would have a much harder time making sense of RF's raw data than camera footage ($N = 13$): *"I can see that someone is there, but cannot tell who. That is extremely scary, in my opinion"* ($P505_{RNH}$). The greater comfort with RF sensors over cameras stemmed from a general discomfort with the collection of visual data ($N = 28$). Seven participants elaborated on their discomfort with visual data, noting that camera footage is easily interpretable, unlike RF sensing data, which requires processing. This led to greater concern about cameras being hacked and sensitive images being shared ($N = 31$). Additionally, many participants, finding the systems highly useful, expressed concern that the limited field of view of cameras could affect performance ($N = 43$): *"The camera cannot detect if the elderly person has fallen at other locations in the house unless the bathroom door is open"* ($P60_{HVB}$).

`Sensor` × `Location` is visualized in Figure 1 (b). A post-hoc test revealed that participants were significantly more comfortable with a camera than with an RF sensor on the front porch ($p = .022$) and a camera in the hallway ($p < .001$). In addition, participants were significantly more comfortable with an RF sensor in the hallway than with a camera ($p < .001$). Sixteen participants described being uncomfortable with cameras in private spaces and more comfortable with a camera in public spaces, such as a stadium's hallway. $P11_{ROF}$ explained: *"this is not a location where someone should have an expectation of privacy, so I am comfortable."* Only seven participants did not want any type of sensing technology in a private space.

6.1.2 Comfort in the Context of Bathroom and Neighbor

To complement the previous insights, we next looked at the `Location` bathroom and the `Perspective` neighbor in isolation. We found that participants in the neighbor perspective feel more comfortable with a camera than with an RF sensor. We again found higher comfort with cameras in security use cases. Unsurprisingly, we found that participants are generally uncomfortable with cameras in bathrooms.

We first filtered the data to only keep the neighbor `Perspective`, which revealed a significant main effect for `Sensor` ($F(1,87) = 13.648$, $p < .001$, $\eta_p^2 = .136$) and a significant interaction effect for `Sensor` × `Use Case` ($F(1,87) = 9.423$, $p = .003$, $\eta_p^2 = .1$), see Figure 1 (c). Post-hoc tests revealed that participants presented with a neighbor-perspective scenario were significantly more comfortable with a camera than an RF sensor in the private security use case ($p < .001$) or private health use case ($p = .027$). Moreover, they were also significantly more comfortable with a camera in the private security use case than in the private health use case ($p = .014$). Our qualitative analysis helps contextualize this. Here, 25 participants explicitly mentioned that they were more comfortable with a camera in the neighbor scenario, as the sensing area can be restricted much more easily: *"I don't want my neighbor knowing what I am doing in my own home, I'm fine with a camera because detection ends when I close my front door"* ($P296_{HNA}$). In addition, 20 participants explicitly mentioned that they were concerned about RF sensors' ability to sense through walls.

Finally, we filtered the `Location` to only keep the bathroom, which revealed a significant main effect for `Sensor` ($F(1,174) = 214.82$, $p < .001$, $\eta_p^2 = .552$). Figure 1 (d) shows that participants were significantly more comfortable with an RF sensor than with a camera in the bathroom, independent of the `Use Case` and `Perspective`. Participants explained that they were very uncomfortable with visual data getting collected in a bathroom ($N = 98$), and 10 participants even considered cameras in a bathroom illegal.

6.1.3 Impact of Protective Measures on Comfort

We next examined the impact of different *protective measures*. Overall, participants found reducing exposure frequency to be inadequate protection. All other protections had a significantly positive impact compared to the original ratings, though the effect varied by use case and perspective. From a neighbor's perspective, all measures significantly reduced concerns.

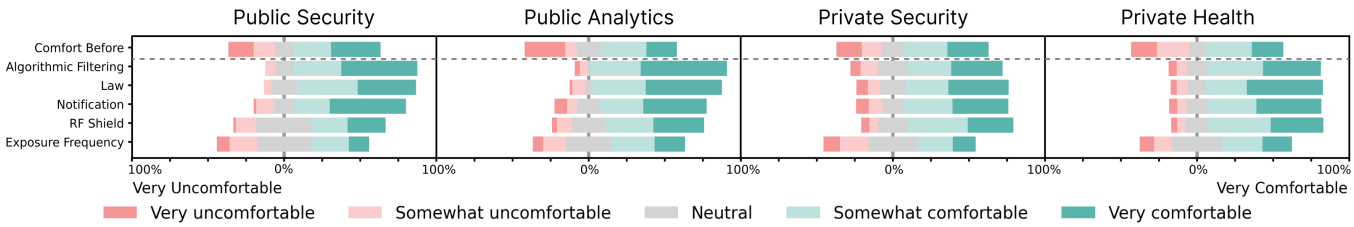

Figure 2: The comfort ratings for the different `Protective Measures` by the different `Use Cases` compared to the original comfort rating without protections. All were rated on a 5-point Likert scale.

We found significant main effects for `Protection Type` ($F(5,2465) = 66.561$, $p < .001$, $\eta_p^2 = .12$), `Use Case` ($F(3,493) = 4.107$, $p = .007$, $\eta_p^2 = .024$), and `Perspective` ($F(2,493) = 5.479$, $p = .004$, $\eta_p^2 = .022$); and significant interaction effects for `Protection Type` × `Use Case` ($F(15,2465) = 3.991$, $p < .001$, $\eta_p^2 = .024$) and `Protection Type` × `Perspective` ($F(10,2465) = 5.104$, $p < .001$, $\eta_p^2 = .02$). Similar to before, we conduct further analyses to untangle these interaction effects.

Impact of Protections in the Context of Use Case. First, we investigated `Protection Type` × `Use Case` by looking at each `Use Case` individually, see Figure 2. We found significant main effects for `Protection Type` for the public security ($F(5,290) = 17.211$, $p < .001$, $\eta_p^2 = .229$), public analytics ($F(5,290) = 12.574$, $p < .001$, $\eta_p^2 = .178$), private security ($F(5,1160) = 34.909$, $p < .001$, $\eta_p^2 = .131$), and private health ($F(5,725) = 17.624$, $p < .001$, $\eta_p^2 = .108$) use cases. Yet, for private security ($F(10,1160) = 3.641$, $p < .001$, $\eta_p^2 = .03$) and private health ($F(10,725) = 2.661$, $p = .003$, $\eta_p^2 = .035$), we also found significant interaction effects for `Protection Type` × `Perspective`. We report all significant comparisons compared to the original ratings.

In the public analytics use case, people felt significantly more comfortable with algorithmic filtering ($p = .002$) and significantly less comfortable with reducing the exposure frequency ($p = .021$). In the public security scenario, people only felt less comfortable with reducing the exposure frequency ($p < .001$); all other protections did not significantly impact comfort ratings. Due to the interaction effects for the two private use cases, we again had to filter by perspective. Thereby, we found that in the private security use case, as an owner or visitor, people felt more comfortable with a protective law in place ($p = .018$) when being notified ($p = .009$) and significantly less comfortable with reducing the exposure frequency ($p < .001$). From the neighbor's perspective, they felt significantly more comfortable with all protections (RF shield, law, and notification $p < .001$, algorithmic filter $p = .005$). While we did not find any significant improvements for the private health use case from any perspective, we found that owners and visitors would be significantly less comfortable with reducing the exposure frequency ($p < .001$).

Impact of Protections in the Context of Perspective. Next, we investigated `Protection Type` × `Perspective` by filtering the data for each perspective, see Figure 3. For owners, we found significant main effects for `Protection Type` ($F(5,725) = 15.079$, $p < .001$, $\eta_p^2 = .094$), `Use Case` ($F(1,145) = 7.887$, $p = .006$, $\eta_p^2 = .052$), and `Location` ($F(2,145) = 4.355$, $p = .015$, $\eta_p^2 = .057$). Post-hoc tests revealed that owners felt significantly more comfortable with a protective law ($p < .001$). From the visitor perspective, we found a significant main effect for `Protection Type` ($F(5,1305) = 39.64$, $p < .001$, $\eta_p^2 = .132$) and a significant interaction effect for `Protection Type` × `Use Case` ($F(15,1305) = 1.856$, $p = 0.024$, $\eta_p^2 = 0.021$). After filtering by `Use Case`, post-hoc tests showed that visitors felt significantly less comfortable with a reduced exposure frequency in the private health ($p = .021$) and public security ($p = .002$) use cases. Finally, for the neighbor perspective, we again only found a significant main effect for `Protection Type` ($F(5,435) = 17.244$, $p < .001$, $\eta_p^2 = .165$). Post-hoc tests showed that neighbors felt significantly more comfortable with an RF shield in place, with algorithmic filtering, with a protective law, and when being notified (all $p < .001$).

6.1.4 Impact of Sensitivity and Utility

Lastly, we conducted correlation analyses to see if the perceived sensitivity of the collected data or location, and the perceived utility, impact comfort. We found that data and location sensitivity negatively impacted participants' comfort, whereas a higher perceived utility also led to higher comfort. We found a moderate negative correlation for location sensitivity ($r_\tau = -0.329$, $p < .001$), meaning that the more sensitive participants consider a location, the less comfortable they are with the situation. We also found a moderate negative correlation for data sensitivity ($r_\tau = -0.362$, $p < .001$), which shows that increased data sensitivity comes with greater discomfort. Finally, we found a strong positive correlation ($r_\tau = .502$, $p < .001$) for perceived utility, indicating that the more useful participants considered a system for themselves, the more comfortable they were with the sit-

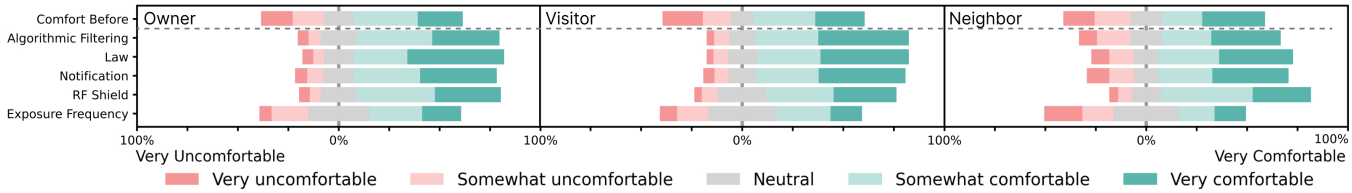

Figure 3: The comfort ratings for the different `Protective Measures` by the different `Perspectives` compared to the original comfort rating without protections. All were rated on a 5-point Likert scale.

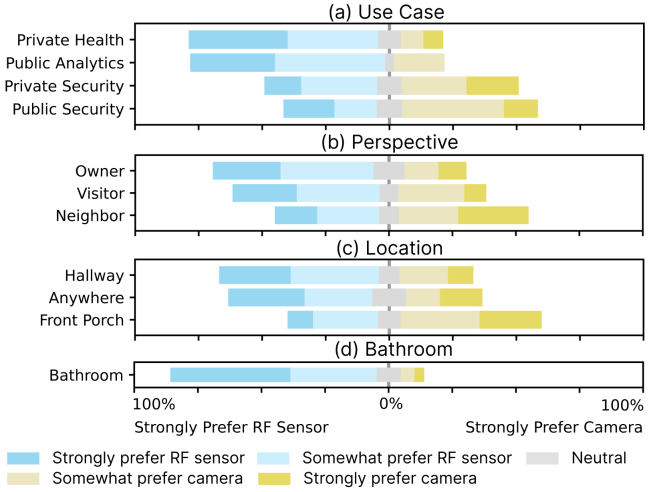

Figure 4: Plots (a) - (c) show preference without `Location` bathroom for (a) use cases, (b) perspectives, and (c) locations; (d) shows preferences only for the bathroom.

uation. Participants echoed this in their free-text responses, where 33 participants mentioned being comfortable with a sensing system simply because they considered the use case sensible and uncomfortable when they felt the use case would not benefit them.

6.2 Context Impact on Technology Preference

Summary. We investigated how different contextual factors impacted preferences between cameras and RF sensors. Participants preferred cameras for security use cases, since they can provide visual evidence to prosecute criminals. They also preferred that neighbors install cameras because those would not infringe on their privacy as they cannot penetrate walls. Furthermore, we found that participants preferred cameras in non-sensitive locations outside their houses. Protective measures did not shift their technology preferences significantly.

Comparing preferences for cameras and RF sensors, we found significant main effects for `Use Case`, `Perspective`, and `Location`. We also found significant interaction effects for `Use Case` × `Location` and `Perspective` × `Location`. See Table 3 for the results and effect sizes. Post-hoc tests showed that most significant effects were again triggered by the bathroom, so we again filtered our data by the `Location` bathroom. Figure 4 (d) shows preferences for devices in the bathroom, with a strong preference for RF sensors.

We first looked at our data without the bathroom included and found significant main effects for `Use Case` ($F(3,319) = 15.86$, $p < .001$, $\eta_p^2 = .13$), `Perspective` ($F(2,319) = 8.318$, $p < .001$, $\eta_p^2 = .05$), and `Location` ($F(2,319) = 10.183$, $p < .001$, $\eta_p^2 = .06$). Post-hoc tests for the `Use Case` revealed that participants significantly preferred a camera in the private security ($p < .001$) and public security ($p = .004$) use cases compared to the private health use case, see Figure 4 (a). They significantly preferred a camera in the public security ($p = 0.03$) and private security ($p = 0.001$) compared to the public analytics use case.

Our participants explained that they preferred the RF sensor for its comprehensive coverage ($N = 154$): *"It can sense in all directions and through walls, I would be able to secure a much larger area"* ($P28_{ROH}$). An additional 105 participants preferred the RF sensor because it did not capture visual data, even though some people realized that the sensor captures a lot of data at once, possibly making it more privacy-invasive after all: *"I realize the RF sensor captures info that is possibly more intrusive, for some reason, it feels less invasive"* ($P414_{RNF}$). In security scenarios, participants preferred cameras for providing visual evidence to track and prosecute criminals ($N = 69$): *"If someone was to break into my home, I would rather have the ability to see them so that they can be caught by the police"* ($P43_{RNH}$). Yet, 11 participants preferred the RF sensor for security scenarios, believing cameras would be easier for criminals to evade: *"You can stay in the blind spots of cameras or even cover them, I am unaware how that is possible for [RF] sensors"* ($P195_{RVB}$).

Factor	dfn	dfd	F	p-value	η_p^2
UseCase	3	493	23.859	<.001***	.127***
Perspective	2	493	16.105	<.001***	.061***
Location	3	493	26.492	<.001***	.139***
UseCase×Persp.	1	493	0.587	.444	.001
UseCase×Loc.	3	493	6.374	<.001***	.037***
Persp.×Loc.	3	493	2.763	.042*	.017*
UseCase×Persp.×Loc.	1	493	1.140	.286	.002

Table 3: All factors impact on tech. preference ART ANOVA.

Next, we ran post-hoc tests for `Perspective` and found that participants in the neighbor perspective significantly preferred the camera compared to the owner ($p = 0.002$) and visitor ($p = 0.004$), see Figure 4 (b). Finally, post-hoc tests for the `Location` revealed significant preference for the camera on the porch compared to anywhere ($p = 0.03$) and hallway ($p < .001$), see Figure 4 (c). We also ran analysis with only `Location` bathroom but did not find significant effects.

Investigating the impact of protective measures on preferences, we found significant main effects for `Protection Type` ($F(5,2465) = 5.253$, $p < .001$, $\eta_p^2 = .011$), `Use Case` ($F(3,493) = 17.658$, $p < .001$, $\eta_p^2 = .097$), `Perspective` ($F(2,493) = 18.214$, $p < .001$, $\eta_p^2 = .069$), and `Location` ($F(3,493) = 20.608$, $p < .001$, $\eta_p^2 = .111$), and significant interactions for `Protection Type` × `Use Case` ($F(15,2465) = 2.037$, $p = .01$, $\eta_p^2 = .012$), `Use Case` × `Location` ($F(3,493) = 2.692$, $p = .046$, $\eta_p^2 = .016$), `Perspective` × `Location` ($F(3,493) = 3.335$, $p = .019$,$\eta_p^2 = .02$), and `Protection Type` × `Use Case` × `Location` ($F(15,2465) = 1.731, p = .04, \eta_p^2 = .010$). However, post-hoc tests uncovered no differences.

7 Limitations

We used interviews and surveys to investigate perceptions of RF technology. While these methods are frequently used for analogous goals, especially when discussing emerging technologies [74], they inherently rely on self-reporting and the biases that come with it. For example, even though participants heavily weighed perceived utility against privacy concerns, their perceptions might differ if they actually used RF sensing systems. Participants' limited familiarity with RF sensing also impacted concerns, with some expressing that they were unsure about the exact boundaries and capabilities. Prior work has repeatedly shown that higher familiarity tends to decrease concerns [5, 73]. On the other hand, experience with (or media exposure to) actual privacy invasions associated with RF sensors could increase concern.

Since most participants were initially unfamiliar with RF sensing's full capabilities, we provided a detailed explanation before asking questions about it. Although we carefully crafted these explanations and confirmed through piloting that they did not lead to skewed perceptions, explaining unfamiliar technology may inherently introduce some bias. It would therefore be interesting to repeat our investigation after RF sensors have found more widespread adoption.

We recruited a U.S.-representative sample to reduce sampling bias and improve generalizability. While this approach helps minimize confounds and provides a solid foundation for future research, it also limits the applicability of our findings to other cultures. For instance, the U.S. population is generally more privacy-conscious than populations in countries like India and China [71], and less privacy-conscious than Europeans [70]. Beyond cultural factors, other demographic characteristics, such as gender, may also shape perceptions of RF technologies and warrant further exploration. Thus, future research could include more diverse cultural contexts and explicitly investigate demographic differences to understand how RF perceptions vary across populations.

8 Discussion

RF sensing introduces unique challenges: unlike visual sensors, RF sensors can operate through walls, are difficult to detect, and cannot be blocked easily. This perceived invisibility, coupled with limited user control and the technology's powerful inferential capabilities, raises novel concerns. While prior research has focused on data flows to third parties and the experiences of bystanders, our results suggest that RF sensing amplifies these dynamics. People may be unaware that data collection is occurring and, as bystanders, have even less leverage to negotiate with device owners. **Importantly, we show that preferences between RF sensors and cameras are context-dependent; RF sensing is not inherently more privacy-preserving, despite common assumptions.** We discuss our key findings related to balancing utility with privacy concerns, ethical considerations about marketing RF sensing as privacy-preserving, and legal discussions.

8.1 RF Sensing: Balancing Concerns & Utility

To the best of our knowledge, we are the first to explicitly investigate people's perceptions of RF sensing. In contrast to prior that work primarily examined data interpretability and inferences [65], we focus on how contextual factors affect comfort and preferences between RF sensors and cameras. We explored this through three questions: **RQ1** measured general perceptions of RF sensing; **RQ2** investigated how different contextual factors shape comfort with RF sensors, and **RQ3** examined the impact of protective measures on comfort.

Participants initially lacked awareness of RF sensing. However, upon learning about it, they expressed nuanced views, with contextual factors heavily shaping privacy concerns. This aligns with Nissenbaum's theory of Contextual Integrity: privacy is violated when data handling does not align with contextual norms [50]. Further, participants weighed RF sensors' perceived benefits, such as sensing large areas regardless of obstructions and lighting, against privacy concerns. This tension between utility and privacy resonates with the privacy calculus theory: users balance perceived benefits against risks [17]. Accordingly, when perceived benefits weighed heavier, participants tolerated RF sensing. For instance, the desire for a comprehensive health monitoring system outweighed concerns. In contrast, these very capabilities, especially to "see through walls," were seen as intrusive in other contexts. This dichotomy of comfort reflects findings from previous research on sensor-based systems, which shows that

people accept sensors in public or medical settings but reject them in private spaces [22, 89]. Additionally, our second study highlighted that concerns and protective measures are subject to contextual variations. While reducing exposure frequency was generally not seen as an effective solution, participants responded positively to notifications, regulations, algorithmic filtering, and limiting the RF tracking range. However, their preferences for these measures varied significantly depending on context. This suggests that regulations and technological safeguards should not follow a one-size-fits-all approach but should be tailored to individual needs.

Key Finding 1: Concerns about RF sensing are highly context-dependent. Features that make RF sensing valuable in certain scenarios raise serious privacy concerns in others.

Recommendation: RF sensor owners *and* those being sensed should have control over when and how sensing happens. Both sides benefit from transparency and clear limits on data use through policy and technical measures. We expect that balancing utility and privacy will be key to gaining user trust and widespread acceptance of RF sensing.

8.2 Are Privacy-Preserving Claims Accurate?

One key selling point of RF sensors is their claimed privacy protection due to not collecting visual data [32]. Initially, this seems valid, as research reports users' concern with visual data in private spaces [6, 73]. Some of our findings support this: participants were uncomfortable with cameras in their homes, particularly in sensitive areas such as bathrooms. However, our findings also reveal that RF sensors are not a silver bullet for privacy. Even though people generally found utility in health and safety scenarios, they were concerned about sensors picking up private activities irrelevant to the use case.

Additionally, some participants were uncomfortable with scenarios where RF sensors would sense through walls, especially when they did not own the sensor. This represents a fundamental contradiction in people's preferences: while, for themselves, they tend to select the option with greater utility (often, RF sensing), they prefer that their neighbors choose the more privacy-preserving option (cameras). Therefore, for most scenarios, it cannot be said that RF sensing is truly preferred or really privacy-preserving, since these opinions represent only one stakeholder's perspective. This suggests that while RF products may reduce concerns about visual data, they introduce other unaddressed privacy considerations.

Key Finding 2: Users are unaware of the full capabilities and risks of RF sensing. Thus, marketing radio-frequency sensors as privacy-preserving can be misleading.

Recommendation: Researchers should provide nuanced descriptions of the privacy implications of RF sensing. Companies should provide clear information about RF sensing capabilities and privacy implications in user manuals, product packaging, and marketing materials. Regulatory guidelines could ensure that claims are accurate.

8.3 Technical Privacy Protections are Needed

RF sensors can collect data through walls and infer a wide range of human attributes and activities, often far beyond what is needed in any particular use case. Accordingly, our participants often expressed privacy concerns, especially in relation to their neighbors. However, participants were significantly more comfortable with RF sensors when deployed with privacy protective measures. Unfortunately, while researchers have been working on RF sensing technical defenses, commercially available options appear non-existent. RF sensing devices could perform data processing on the device and store only relevant features and inferences (other types of sensor systems have taken this "edge featurization" approach [9]). More work is needed to design RF sensing systems that provide utility while minimizing data collection, ideally with verifiable assurances.

Privacy protections built into devices can ease privacy concerns; however, these do not address concerns about devices people are unaware of. Research is needed on RF sensing privacy shields that people could practically deploy. An effective approach could be to exploit the inherent technical limitations of RF sensing, such as using the signal interference vulnerability of RF sensing [57]. Similarly, the inability of RF waves to penetrate certain materials could be leveraged to create a simple blocker.

Key Finding 3: Technical measures can ease privacy concerns while preserving utility. However, more work is needed to develop comprehensive solutions and practical products.

Recommendation: Developers should integrate privacy-enhancing technologies. This can include adopting edge computing and featurization. Protections are especially crucial when people are unaware; here, solutions could leverage RF sensing's technical limitations.

8.4 Novel Capabilities Require Legal Action

RF sensing introduces privacy challenges beyond technical concerns, touching on sociological, legal, and ethical domains. From a sociological perspective, the hard-to-detect nature of RF sensing might enable widespread surveillance (e.g., by governments) and thus exaggerate harms [46]. Moreover, unlike cameras or microphones, RF sensing can penetrate walls with minimal loss of fidelity, which, as we show, raises privacy concerns in dense housing settings: participants were uneasy about RF systems capturing sensitive information from neighboring apartments without their knowledge. This concern leads to key questions: how to inform users about RF systems? How to give them the ability to take action? Solutions could potentially leverage IoT privacy labels [23, 24], informing consumers about data collected, processing, and privacy measures. Labels could also outline the capabilities of RF sensing, helping users understand the technology, a sore point in our interviews. Encouragingly, regulatory frameworks have

already been proposed for IoT labels [18, 29], and simple modifications could accommodate RF sensing products.

Legislation has a fundamental role in this ecosystem, too; informed consent and opt-out options could be mandated by law. This solution is not without its flaws: who bears responsibility for obtaining consent and providing controls? The device operator? The manufacturer? Supervising government agencies? Current privacy regulations, such as GDPR, do not explicitly address non-visual surveillance technologies [26]. While GDPR's general provisions for personal data processing indirectly cover such technologies, unlike traditional surveillance (e.g., CCTV requirements [25]), additional guidance has not been issued for RF sensing. Given the implications of widespread RF sensing adoption, such questions require urgent attention. Finally, participants feared RF sensing might inadvertently detect sensitive situations in neighboring apartments, such as domestic violence or mental health crises. With smart home data already being used in forensic investigations [20, 36], it is unclear if owners are responsible for reporting such information.

Key Finding 4: RF sensing introduces new privacy challenges due to its ability to sense through solid objects, potentially capturing data from neighbors and making it difficult for individuals to detect tracking.

Recommendation: A legal framework may be needed for reasonable use of RF sensing, specifying when notifications, informed consent, and controls are required. Similar to video surveillance, RF sensing should be explicitly addressed within existing legal frameworks.

9 Conclusion

We conducted interviews ($N = 14$) and a large-scale vignette survey ($N = 510$), to understand people's privacy perceptions of RF sensing technology compared to cameras. We found that, initially, most participants were unaware of the full capabilities of RF sensing. However, once they understood the technology, they expressed nuanced concerns impacted by contextual factors. People prefer RF sensors in intimate locations as they are more comfortable with RF sensors not collecting visual information. Yet, in security-relevant scenarios and from the neighbor's perspective, people preferred cameras for the visual evidence and their inability to penetrate walls. We further found that protective measures can improve comfort, but which protection people prefer is heavily impacted by context. We conclude that users need to be educated about RF sensing and call for new legal frameworks to safeguard privacy as the technology proliferates.

10 Ethics Considerations

The Carnegie Mellon University Institutional Review Board (IRB) reviewed and approved all study procedures and consent processes. In designing them, we focused on minimizing risks and ensuring participant autonomy and data protection. The primary stakeholders in our research were the interview and survey participants, as well as the broader public potentially affected by the deployment of RF sensing technologies. For participants, the main risks included discomfort or anxiety when discussing privacy concerns, particularly regarding sensitive use cases. However, all of our scenarios were hypothetical and we did not probe participants' personal experiences. We further ensured informed consent by clearly explaining the study's purpose, procedures, and potential risks and benefits. We gave participants opportunities to ask questions and allowed them to withdraw or pause their participation at any time without consequences. We collected minimal personal data, anonymized it, and securely stored it to prevent unauthorized access. A secondary stakeholder is the developers of RF sensing technology. While we did not directly interact with developers, we argue that the insights uncovered would benefit their products as well as their users.

Although we did not directly develop or deploy RF sensing artifacts, we acknowledge the broader societal implications. RF sensing, often presented as a privacy-preserving alternative to cameras, raises significant ethical questions due to its potential for misuse and unintended consequences. To address this, we presented our findings in a neutral, evidence-based manner to inform educational and legislative efforts.

11 Open Science

We provide the interview guideline, interview slideshow, interview codebook, survey questionnaire, survey analysis script, and anonymized survey data on OSF: https://doi.org/10.17605/OSF.IO/6WAMZ.

Acknowledgments

We thank Evan Zhao and Abdulazeez Alugo for their help with this research and our participants for contributing their time and perspectives. This project was supported, in part, by Craig Newmark Philanthropies and Innovators Network Foundation.

References

[1] Fadel Adib and Dina Katabi. See through walls with WiFi! *SIGCOMM Comput. Commun. Rev.*, 43(4), Aug 2013. URL https://doi.org/10.1145/2534169.2486039.

[2] Fadel Adib, Zach Kabelac, Dina Katabi, and Robert C. Miller. 3D tracking via body radio reflections. In *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, Seattle, WA, April 2014. USENIX Association. URL https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/adib.

[3] Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi, and Robert C. Miller. Smart homes that monitor breathing and heart rate. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, New York, NY, USA, 2015. Association for Computing Machinery. URL https://doi.org/10.1145/2702123.2702200.

[4] Kamran Ali, Alex X. Liu, Wei Wang, and Muhammad Shahzad. Keystroke recognition using WiFi signals. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, MobiCom '15, New York, NY, USA, 2015. Association for Computing Machinery. URL https://doi.org/10.1145/2789168.2790109.

[5] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home Internet of Things privacy norms using contextual integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(2), jul 2018. URL https://doi.org/10.1145/3214262.

[6] Katrin Arning and Martina Ziefle. "Get that camera out of my house!" conjoint measurement of preferences for video-based healthcare monitoring systems in private and public places. In Antoine Geissbühler, Jacques Demongeot, Mounir Mokhtari, Bessam Abdulrazak, and Hamdi Aloulou, editors, *Inclusive Smart Cities and e-Health*, Cham, 2015. Springer. URL https://doi.org/10.1007/978-3-319-19312-0_13.

[7] Arijit Banerjee, Dustin Maas, Maurizio Bocca, Neal Patwari, and Sneha Kasera. Violating privacy through walls by passive monitoring of radio windows. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, New York, NY, USA, 2014. Association for Computing Machinery. URL https://doi.org/10.1145/2627393.2627418.

[8] Ann Blandford, Dominic Furniss, and Stephann Makri. *Qualitative HCI Research: Going Behind the Scenes*. Synthesis Lectures on Human-Centered Informatics. Springer Cham, Cham, Switzerland, 2016. URL https://doi.org/10.2200/S00706ED1V01Y201602HCI034.

[9] Sudershan Boovaraghavan, Chen Chen, Anurag Maravi, Mike Czapik, Yang Zhang, Chris Harrison, and Yuvraj Agarwal. Mites: Design and deployment of a general-purpose sensing infrastructure for buildings. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 7 (1), March 2023. URL https://doi.org/10.1145/3580865.

[10] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference*, EISIC, 16, New York, NY, USA, 2016. IEEE. URL https://doi.org/10.1109/EISIC.2016.044.

[11] Kelly Caine, Selma Šabanovic, and Mary Carter. The effect of monitoring by cameras and robots on the privacy enhancing behaviors of older adults. In *Proceedings of the Seventh Annual ACM/IEEE International Conference on Human-Robot Interaction*, HRI '12, New York, NY, USA, 2012. Association for Computing Machinery. URL https://doi.org/10.1145/2157689.2157807.

[12] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. "It did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery. URL https://doi.org/10.1145/3411764.3445691.

[13] Shrenik Changede and Ashutosh Dhekne. Intrusense: an enhanced physical security system using UWB. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*, HotMobile '22, New York, NY, USA, 2022. Association for Computing Machinery. URL https://doi.org/10.1145/3508396.3512884.

[14] Andrew Tzer-Yeu Chen, Morteza Biglari-Abhari, and Kevin I-Kai Wang. Context is king: Privacy perceptions of camera-based surveillance. In *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, New York, NY, USA, 2018. IEEE. URL https://doi.org/10.1109/AVSS.2018.8639448.

[15] Kevin Chetty, Graeme E. Smith, and Karl Woodbridge. Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances. *IEEE Transactions on Geoscience and Remote Sensing*, 50(4), 2012. URL https://doi.org/10.1109/TGRS.2011.2164411.

[16] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, New York, NY, USA, 2012. Association for Computing Machinery. URL https://doi.org/10.1145/2370216.2370226.

[17] Mary J Culnan and Robert J Bies. Consumer privacy: Balancing economic and justice considerations. *Journal of social issues*, 59(2), 2003.

[18] Cyber Security Agency of Singapore. Cybersecurity certification for organisations, 2025. URL https://www.

csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-for-organisations. Accessed: 2025-05-06.

[19] Kailtyn Diederichs, Amy Qiu, and George Shaker. Wireless biometric individual identification utilizing millimeter waves. *IEEE Sensors Letters*, 1(1), 2017. URL https://doi.org/10.1109/LSENS.2017.2673551.

[20] Gokila Dorai, Shiva Houshmand, and Ibrahim Baggili. I know what you did last summer: Your smart home Internet of Things and your iPhone forensically ratting you out. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES '18, New York, NY, USA, 2018. Association for Computing Machinery. URL https://doi.org/10.1145/3230833.3232814.

[21] Lisa A. Elkin, Matthew Kay, James J. Higgins, and Jacob O. Wobbrock. An aligned rank transform procedure for multifactor contrast tests. In *The 34th Annual ACM Symposium on User Interface Software and Technology*, UIST '21, New York, NY, USA, 2021. Association for Computing Machinery. URL https://doi.org/10.1145/3472749.3474784.

[22] 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)*, Santa Clara, CA, July 2017. USENIX Association. URL https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

[23] 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)*, New York, NY, USA, 2020. IEEE. URL https://doi.org/10.1109/SP40000.2020.00043.

[24] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. An informative security and privacy "nutrition" label for Internet of Things devices. *IEEE Security & Privacy*, 20(2), 2022. URL https://doi.org/10.1109/MSEC.2021.3132398.

[25] European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices, 2019. URL https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. Accessed: 2025-05-06.

[26] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016. URL https://data.europa.eu/eli/reg/2016/679/oj.

[27] Lijie Fan, Tianhong Li, Rongyao Fang, Rumen Hristov, Yuan Yuan, and Dina Katabi. Learning longterm representations for person re-identification using radio signals. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, New York, NY, USA, 2020. IEEE. URL https://doi.org/10.1109/CVPR42600.2020.01071.

[28] Lijie Fan, Tianhong Li, Yuan Yuan, and Dina Katabi. In-home daily-life captioning using radio signals. In *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part II 16*. Springer, 2020. URL https://doi.org/10.1007/978-3-030-58536-5_7.

[29] Federal Communications Commission. U.S. Cyber Trust Mark, 2025. URL https://www.fcc.gov/CyberTrustMark. Accessed: 2025-05-06.

[30] Andy Field. *Discovering statistics using IBM SPSS statistics*. SAGE publications limited, 2024.

[31] Andy Field and Graham Hole. How to design and report experiments. 2003.

[32] Jiaqi Geng, Dong Huang, and Fernando De la Torre. Densepose from wifi. *arXiv preprint arXiv:2301.00250*, 2022. URL https://doi.org/10.48550/arXiv.2301.00250.

[33] Yu Gu, Jinhai Zhan, Yusheng Ji, Jie Li, Fuji Ren, and Shangbing Gao. Mosense: An RF-based motion detection system via off-the-shelf WiFi devices. *IEEE Internet of Things Journal*, 4(6), 2017. URL https://doi.org/10.1109/JIOT.2017.2754578.

[34] Chen-Yu Hsu, Aayush Ahuja, Shichao Yue, Rumen Hristov, Zachary Kabelac, and Dina Katabi. Zero-effort in-home sleep and insomnia monitoring using radio signals. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), sep 2017. URL https://doi.org/10.1145/3130924.

[35] Nicolas Jacquemet, Stéphane Luchini, Julie Rosaz, and Jason F Shogren. Truth telling under oath. *Management Science*, 65(1), 2019.

[36] Soram Kim, Myungseo Park, Sehoon Lee, and Jongsung Kim. Smart home forensics—data analysis of IoT devices. *Electronics*, 9(8), 2020. URL https://doi.org/10.3390/electronics9081215.

[37] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. Exploring privacy concerns about personal sensing. In Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe, editors, *Pervasive Computing*, Berlin, Heidelberg, 2009. Springer. URL https://doi.org/10.1007/978-3-642-01516-8_13.

[38] Evan Lafontaine, Aafaq Sabir, and Anupam Das. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI'21. ACM, 2021. URL https://doi.org/10.1145/3411763.3451633.

[39] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.*, 2 (CSCW), 2018. URL https://doi.org/10.1145/3274371.

[40] Roxanne Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, DIS '19, New York, NY, USA, 2019. Association for Computing Machinery. URL https://doi.org/10.1145/3322276.3322366.

[41] Jianshu Li, Zhicheng Chen, Feng Shi, and Zhaohui Yang. Radio frequency sensing with commodity devices: Principles, applications, and challenges. *Frontiers in Communications and Networks*, 3, 2022. URL https://doi.org/10.3389/frcmn.2022.1010228.

[42] Hankai Liu, Xiulong Liu, Xin Xie, Xinyu Tong, Tuo Shi, and Keqiu Li. Application-oriented privacy filter for mmWave radar. *IEEE Communications Magazine*, 61(12), 2023. URL https://doi.org/10.1109/MCOM.011.2200580.

[43] Jialin Liu, Lei Wang, Linlin Guo, Jian Fang, Bingxian Lu, and Wei Zhou. A research on CSI-based human motion detection in complex scenarios. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, New York, NY, USA, 2017. IEEE. URL https://doi.org/10.1109/HealthCom.2017.8210800.

[44] Jianwei Liu, Chaowei Xiao, Kaiyan Cui, Jinsong Han, Xian Xu, Kui Ren, and Xufei Mao. A behavior privacy preserving method towards RF sensing. In *2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*, New York, NY, USA, 2021. IEEE. URL https://doi.org/10.1109/IWQOS52092.2021.9521278.

[45] Jun Luo, Hangcheng Cao, Hongbo Jiang, Yanbing Yang, and Zhe Chen. MIMOCrypt: Multi-user privacy-preserving Wi-Fi sensing via MIMO encryption. *arXiv preprint arXiv:2309.00250*, 2023.

[46] David Lyon. *Surveillance Society: Monitoring Everyday Life*. McGraw-Hill Education (UK), Maidenhead, UK, 2001. URL https://books.google.com/books?id=FJBEBgAAQBAJ.

[47] Yongsen Ma, Gang Zhou, and Shuangquan Wang. WiFi sensing with channel state information: A survey. *ACM Comput. Surv.*, 52(3), Jun 2019. URL https://doi.org/10.1145/3310194.

[48] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4), 2019. URL https://doi.org/10.2478/popets-2019-0068.

[49] Van-Linh Nguyen, Ren-Hung Hwang, Bo-Chao Cheng, Ying-Dar Lin, and Trung Q. Duong. Understanding privacy risks of high-accuracy radio positioning and sensing in wireless networks. *IEEE Communications Magazine*, 62(5), 2024. URL https://doi.org/10.1109/MCOM.004.2300090.

[50] Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79, 2004.

[51] Origin Wireless. Trupresence™. https://www.originwirelessai.com/trupresence/. Accessed: 2025-01-22.

[52] Muhammed Zahid Ozturk, Chenshu Wu, Beibei Wang, and KJ Ray Liu. Radiomic: Sound sensing via radio signals. *IEEE Internet of Things Journal*, 10(5), 2022.

[53] Muhammed Zahid Ozturk, Chenshu Wu, Beibei Wang, Min Wu, and KJ Ray Liu. Radio SES: mmWave-based audioradio speech enhancement and separation system. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 31, 2023. URL https://doi.org/10.1109/TASLP.2023.3250846.

[54] Sameera Palipana, David Rojas, Piyush Agrawal, and Dirk Pesch. Falldefi: Ubiquitous fall detection using commodity Wi-Fi devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(4), jan 2018. URL https://doi.org/10.1145/3161183.

[55] James Pierce, Richmond Y. Wong, and Nick Merrill. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, New York, NY, USA, 2020. Association for Computing Machinery. URL https://doi.org/10.1145/3313831.3376347.

[56] Qifan Pu, Sidhant Gupta, Shyamnath Gollakota, and Shwetak Patel. Whole-home gesture recognition using wireless signals. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, MobiCom '13, New York, NY, USA, 2013. Association for Computing Machinery. URL https://doi.org/10.1145/2500423.2500436.

[57] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. PhyCloak: Obfuscating sensing from communication signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, Santa Clara, CA, March 2016. USENIX Association. URL https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/qiao.

[58] Muneeba Raja and Stephan Sigg. Applicability of RF-based methods for emotion recognition: A survey. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, New York, NY, USA, 2016. IEEE. URL https://doi.org/10.1109/PERCOMW.2016.7457119.

[59] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016. URL https://doi.org/10.1109/SP.2016.24.

[60] Nuerzati Resuli, Marjorie Skubic, and Scott Kovaleski. Learning room structure and activity patterns using RF sensing for in-home monitoring of older adults. In *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, New York, NY, USA, 2020. IEEE. URL https://doi.org/10.1109/BIBM49941.2020.9313335.

[61] Syed Aziz Shah and Francesco Fioranelli. RF sensing technologies for assisted daily living in healthcare: A comprehensive review. *IEEE Aerospace and Electronic Systems Magazine*, 34(11), 2019. URL https://doi.org/10.1109/MAES.2019.2933971.

[62] Jayanth Shenoy, Zikun Liu, Bill Tao, Zachary Kabelac, and Deepak Vasisht. RF-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM 2022 Conference*, SIGCOMM '22, New York, NY, USA, 2022. Association for Computing Machinery. URL https://doi.org/10.1145/3544216.3544256.

[63] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Mobihoc '17, New York, NY, USA, 2017. Association for Computing Machinery. URL https://doi.org/10.1145/3084041.3084061.

[64] Stephan Sigg, Markus Scholz, Shuyu Shi, Yusheng Ji, and Michael Beigl. RF-sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals. *IEEE Transactions on Mobile Computing*, 13(4), 2014. URL https://doi.org/10.1109/TMC.2013.28.

[65] Akash Deep Singh, Brian Wang, Luis Garcia, Xiang Chen, and Mani Srivastava. Understanding factors behind IoT privacy–a user's perspective on RF sensors. *arXiv preprint arXiv:2401.08037*, 2024.

[66] SleepScore Labs. Sleepscore max sleep improvement system. https://shop.sleepscore.com/products/sleepscore-product. Accessed: 2025-01-22.

[67] Sheng Tan and Jie Yang. Wifinger: leveraging commodity wifi for fine-grained finger gesture recognition. In *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '16, New York, NY, USA, 2016. Association for Computing Machinery. URL https://doi.org/10.1145/2942358.2942393.

[68] Sheng Tan, Yili Ren, Jie Yang, and Yingying Chen. Commodity WiFi sensing in ten years: Status, challenges, and opportunities. *IEEE Internet of Things Journal*, 9(18), 2022. URL https://doi.org/10.1109/JIOT.2022.3164569.

[69] Daphne Townsend, Frank Knoefel, and Rafik Goubran. Privacy versus autonomy: A tradeoff model for smart home monitoring technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, NY, USA, 2011. IEEE. URL https://doi.org/10.1109/IEMBS.2011.6091176.

[70] Sabine Trepte and Philipp K Masur. Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study. 2016.

[71] Yang Wang, Gregory Norice, and Lorrie Faith Cranor. Who is concerned about what? a study of American, Chinese and Indian users' privacy concerns on social network sites. In Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres, editors, *Trust and Trustworthy Computing*, Berlin, Heidelberg, 2011. Springer. URL https://doi.org/10.1007/978-3-642-21599-5_11.

[72] Yuxi Wang, Kaishun Wu, and Lionel M. Ni. Wifall: Device-free fall detection by wireless networks. *IEEE Transactions on Mobile Computing*, 16(2), 2017. URL https://doi.org/10.1109/TMC.2016.2557792.

[73] Maximiliane Windl and Sven Mayer. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.*, 6(MHCI), 2022. URL https://doi.org/10.1145/3546719.

[74] Maximiliane Windl, Jan Leusmann, Albrecht Schmidt, Sebastian S. Feger, and Sven Mayer. Privacy communication patterns for domestic robots. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*,

Philadelphia, PA, August 2024. USENIX Association. URL https://www.usenix.org/conference/soups2024/presentation/windl.

[75] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. The aligned rank transform for nonparametric factorial analyses using only anova procedures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, New York, NY, USA, 2011. Association for Computing Machinery. URL https://doi.org/10.1145/1978942.1978963.

[76] Wenqing Yan and Ambuj Varshney. Enabling l3: low cost, low complexity and low power radio frequency sensing using tunnel diodes. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, New York, NY, USA, 2022. Association for Computing Machinery. URL https://doi.org/10.1145/3495243.3558281.

[77] Yuzhe Yang, Yuan Yuan, Guo Zhang, Hao Wang, Ying-Cong Chen, Yingcheng Liu, Christopher G Tarolli, Daniel Crepeau, Jan Bukartyk, Mithri R Junna, et al. Artificial intelligence-enabled detection and assessment of parkinson's disease using nocturnal breathing signals. *Nature medicine*, 28(10), 2022.

[78] Yao Yao, Yan Li, Xin Liu, Zicheng Chi, Wei Wang, Tiantian Xie, and Ting Zhu. Aegis: An interference-negligible RF sensing shield. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, New York, NY, USA, 2018. IEEE. URL https://doi.org/10.1109/INFOCOM.2018.8485883.

[79] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019. URL https://doi.org/10.1145/3359161.

[80] Shichao Yue, Hao He, Hao Wang, Hariharan Rahul, and Dina Katabi. Extracting multi-person respiration from entangled RF signals. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(2), jul 2018. URL https://doi.org/10.1145/3214289.

[81] Youwei Zeng, Dan Wu, Jie Xiong, Enze Yi, Ruiyang Gao, and Daqing Zhang. FarSense: Pushing the range limit of WiFi-based respiration sensing with CSI ratio of two antennas. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 3(3), sep 2019. URL https://doi.org/10.1145/3351279.

[82] Yunze Zeng, Parth H. Pathak, and Prasant Mohapatra. WiWho: WiFi-based person identification in smart spaces. In *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, New York, NY, USA, 2016. IEEE. URL https://doi.org/10.1109/IPSN.2016.7460727.

[83] Jie Zhang, Zhanyong Tang, Meng Li, Dingyi Fang, Petteri Nurmi, and Zheng Wang. CrossSense: Towards cross-site and large-scale WiFi sensing. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, New York, NY, USA, 2018. Association for Computing Machinery. URL https://doi.org/10.1145/3241539.3241570.

[84] 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.

[85] Mingmin Zhao, Fadel Adib, and Dina Katabi. Emotion recognition using wireless signals. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, New York, NY, USA, 2016. Association for Computing Machinery. URL https://doi.org/10.1145/2973750.2973762.

[86] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018. URL https://doi.org/10.1145/3274469.

[87] Siwang Zhou, Wei Zhang, Dan Peng, Yonghe Liu, Xingwei Liao, and Hongbo Jiang. Adversarial WiFi sensing for privacy preservation of human behaviors. *IEEE Communications Letters*, 24(2), 2020. URL https://doi.org/10.1109/LCOMM.2019.2952844.

[88] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y Zhao, and Haitao Zheng. Et tu Alexa? when commodity WiFi devices turn into adversarial motion sensors. In *Network and Distributed Systems Security (NDSS) Symposium 2020*, 2020.

[89] Martina Ziefle, Simon Himmel, and Wiktoria Wilkowska. When your living space knows what you do: acceptance of medical home monitoring by different technologies. In *Proceedings of the 7th Conference on Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society: Information Quality in e-Health*, USAB'11, Berlin, Heidelberg, 2011. Springer-Verlag. URL https://doi.org/10.1007/978-3-642-25364-5_43.

A Appendix

Name	Description
Private Security	Imagine you have an indoor security system installed in your home. It constantly surveils your entrance area to alert you in case of suspicious activity so that it can trigger the alarm. You can also receive notifications on specific activities, such as kids arriving home from school, without triggering the alarm.
Private Health	Imagine you have an older adult in your life who still lives independently in their home. You want to ensure their safety, so you install a health monitoring system. Its main purpose is to send out an alert when it detects a person has fallen. Besides that, it can also recognize and alert in case of unusual breathing and heart rate patterns.
Public Security	Imagine you visit a stadium for a major event. The whole stadium is equipped with a security system to monitor the area to prevent crimes, such as theft or violence. In addition, the system also monitors general crowd movements and densities to avoid overcrowding and to ensure compliance with capacity limits.
Public Analytics	Imagine you visit a stadium for a major event. The stadium has a crowd monitoring system to inform event organizers about crowded food stands and bathrooms, ensuring timely refilling and frequent cleaning. Moreover, the system provides analytical insights, such as which routes most people take to allow the strategic placement of advertisements or merchandise booths, and insights into the general demographics of the crowd to allow conclusions about the types of people attracted by certain events.

Table 4: The use-case scenarios we used in our interviews.

ID	System	Perspective	Location	Scenario
HOH	Private Health	Owner	Hallway	You have installed a health monitoring system for older adults in your household. This system collects health data, provides alerts for unusual health patterns and emergencies such as falls. The system is placed in the hallway.
HOB	Private Health	Owner	Bathroom	You have installed a health monitoring system for older adults in your household. This system collects health data, provides alerts for unusual health patterns and emergencies such as falls. The system is placed in the bathroom.
HNA	Private Health	Neighbor	Anywhere	Your neighbor has installed a health monitoring system for older adults in their household. This system collects health data, provides alerts for unusual health patterns and emergencies such as falls.
HVH	Private Health	Visitor	Hallway	You are visiting a friend who has installed a health monitoring system for older adults in their household. This system collects health data, provides alerts for unusual health patterns and emergencies such as falls. The system is placed in the hallway.
PHVB	Private Health	Visitor	Bathroom	You are visiting a friend who has installed a health monitoring system for older adults in their household. This system collects health data, provides alerts for unusual health patterns and emergencies such as falls. The system is placed in the bathroom.
ROH	Private Security	Owner	Hallway	You have installed a security system in your household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed in the hallway.
ROF	Private Security	Owner	Front Porch	You have installed a security system in your household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed on the front porch.
ROB	Private Security	Owner	Bathroom	You have installed a security system in your household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed in the bathroom.
RNF	Private Security	Neighbor	Front Porch	Your neighbor has installed a security system in their household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed on the front porch.
RNH	Private Security	Neighbor	Hallway	Your neighbor has installed a security system in their household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed in the hallway inside their apartment.
RVH	Private Security	Visitor	Hallway	You are visiting a friend who has installed a security system in their household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed in the hallway.
RVF	Private Security	Visitor	Front Porch	You are visiting a friend who has installed a security system in their household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed on the front porch.
RVB	Private Security	Visitor	Bathroom	You are visiting a friend who has installed a security system in their household to prevent suspicious activity. This system provides notifications of unusual events such as intrusions. The system is placed in the bathroom.
UVH	Public Security	Visitor	Hallway	You are visiting a stadium with a security system that prevents crimes, monitors crowds, and ensures safety. The system is placed in hallway areas.
UVB	Public Security	Visitor	Bathroom	You are visiting a stadium with a security system that prevents crimes, monitors crowds, and ensures safety. The system is placed in the bathrooms.
AVH	Public Analytics	Visitor	Hallway	You are visiting a stadium with an analytics system that monitors crowd flow, provides demographic insights, and optimizes placement of resources. The system is placed in hallway areas.
AVB	Public Analytics	Visitor	Bathroom	You are visiting a stadium with an analytics system that monitors crowd flow, provides demographic insights, and optimizes placement of resources. The system is placed in the bathrooms.

Table 5: The scenarios used in our online survey.