"The city isn't uploading me to TikTok": Exploring Privacy Attitudes towards Data Collection in Urban Public Spaces

Julian Todt*
KASTEL Security Research Labs
Karlsruhe Institute of Technology
julian.todt@kit.edu

Emiram Kablo*
Paderborn University
ekablo@mail.upb.de

Felix Morsbach
KASTEL Security Research Labs
Karlsruhe Institute of Technology
felix.morsbach@kit.edu

Patricia Arias-Cabarcos
European Commission, Joint Research Centre (JRC)
KASTEL Security Research Labs
patricia.arias-cabarcos@ec.europa.eu

Thorsten Strufe
KASTEL Security Research Labs
Karlsruhe Institute of Technology
thorsten.strufe@kit.edu

Abstract

Smart cities promise safer streets, smoother traffic, and more efficient services, enabled by dense networks of urban sensors. Yet this infrastructure, often unnoticed by citizens, introduces pervasive privacy risks, from tracking, profiling, and sensitive inferences to subtle forms of self-censorship. Despite widespread deployment, little is known about how the public understands and perceives these sensing systems. To address this gap, we present an intervention-based user study (n = 172) in which participants are exposed to data collection by six urban sensors, including cameras and alternative technologies commonly framed as privacy-preserving. Participants encounter either the sensors alone or sensors accompanied by real-time data visualizations. Our results reveal widespread misunderstanding of some sensors (radar, LiDAR, Wi-Fi, depth, and thermal imaging sensors), particularly their capacity for identification and for attribute inferences such as gender or age. We also identify persistent misconceptions, including the belief that Wi-Fi poses privacy risks only when users connect to public networks. While making sensors visible and visualizing collected data improves privacy awareness, these measures alone are not enough for citizens to understand the actual risks of urban sensing. We derive recommendations for privacy-respecting smart city environments grounded in citizens' informational needs and expectations.

Keywords

privacy, transparency, sensors, smart city, user study

1 Introduction

Smart cities promise improved efficiency and safety through widespread data collection. While the utility of novel sensing technologies in smart cities is often highlighted, their inherent privacy risks towards individuals are only rarely discussed. This could mean that evidence-based policymaking enables far more extensive and gratuitous surveillance of individuals. Potential misconceptions by the public, who cannot evade this ubiquitous data collection, about how privacy-friendly these sensors are, exacerbate the problem.

Video cameras constitute one of the most widely deployed sensing technologies in urban environments, commonly justified in terms of public safety and crime prevention [82]. Their privacy risks have been widely explored and communicated in prior literature [8, 52, 72]. With various distinct biometric traits present in these recordings, particularly face and gait, a range of inferences are possible, such as identity [78], attributes (e.g., gender, age, and medical conditions) [16], and activity [75]. The public's awareness of these privacy risks has motivated calls for alternative sensing technologies to be used in smart cities, giving rise to the introduction of depth and thermal imaging cameras, LiDAR, and radar sensors, which often are framed as more privacy-friendly [39, 84, 89]. However, recent work shows that these sensors also allow for identification and attribute inferences, even when conventional images are not captured [7, 30, 65, 73].

In this context, it is unclear to which extent the general public is aware of what data is being collected in a smart city, and how attitudes change, when being exposed to data collection. While previous research investigated privacy concerns of individual sensors [62, 84] or cameras [11, 34, 92], no previous research has examined privacy attitudes toward multiple sensing technologies in a smart city setting collectively. Especially, because many of these sensors may be unfamiliar to people, it is uncertain whether increased visibility or exposure to the data they collect can meaningfully change understanding and correct potential misconceptions. This issue is particularly relevant for sensors that operate outside the spectrum of human perception, such as LiDAR, which are often less intuitively understood because they do not map directly to human biological senses [61]. To address this knowledge gap, we formulate the following research questions:

RQ1: [Awareness] Are people aware of existing data collecting smart city sensors and their inference capabilities?
RQ2: [Privacy Concern] How do people's privacy concerns vary regarding data collection by different sensor types in city public spaces?
RQ3: [Change of Attitude] Do privacy attitudes change after visualizing what data smart city sensors collect about people?

*Both authors contributed equally to this work.

Proceedings on Privacy Enhancing Technologies 2026(4), 1–29

https://doi.org/10.56553/popets-2024-0001

We investigate these questions via an extensive in-lab study with 172 participants. We conduct an intervention in which participants encounter a prototype smart city environment instrumented with six sensors and report their awareness and privacy concerns before and after being exposed to the sensors alone or to real-time visualizations of the data the sensors collect.

We find that participants hold a disparate and often inaccurate understanding of smart city sensing. While video cameras were widely recognized as capable of revealing identity and personal attributes, the capabilities of sensors such as radar, LiDAR, depth, thermal imaging, and Wi-Fi were substantially underestimated. Participants commonly believed that non-visual sensing supports only limited inference, and misconceptions were particularly evident for Wi-Fi, which many associated solely with voluntary network connection rather than passive signal analysis. Exposure to sensors and to visualizations of the data they produce increased awareness, but did not fully align participants' beliefs with the actual inference capabilities of these systems.

Understanding the extent of public awareness is essential for informing future deployments of urban sensing technologies and the design of transparency measures that support informed perceptions of privacy risks. Based on our findings, we derive implications for the design and governance of privacy-respecting smart city sensing that account for citizens' informational needs and expectations.

2 Background & Related Work

While there is no consensus on the definition of a *smart city*, proposed smart city technologies evolve around the idea of widespread collection of data with the goal to increase efficiency and efficacy of city services [13, 32, 51]. To achieve this data collection, a variety of sensing technologies have been proposed. This includes classic video cameras, but also depth cameras (which measure the distance of the scene to the camera), and thermal imaging cameras (measuring infrared light), either alone or in combination [15, 44, 70]. Furthermore, mmWave radar and LiDAR are often suggested as smart city sensors [74, 88, 93], which send out and then measure the reflection of radio waves and light, respectively. Finally, joint communication and sensing (JCAS) – using the existing communication infrastructure (e.g., 5G, Wi-Fi) to also sense the environment – is being standardized for the use in smart cities [42, 45, 91].

2.1 Inferences

Before we investigate to which extent the public is aware of privacy inferences from smart city sensors, we explore what is technically possible based on the state of the art. For this, we summarize relevant work in the literature to show which inferences have already been shown to be possible (see Table 1).

We limit ourselves to inferences via biometric data, i.e., data containing information about physiological or behavioral characteristics of humans [28]. While further inferences are possible, such as when individual's personal devices interact with the mobile wireless networks (e.g. Wi-Fi, 5G) [17, 50], we consider them out-of-scope for this study. The two biometric traits most prominent for sensing from far away and potentially without consent are face and gait – the way we walk – as opposed to traits like fingerprints that necessitate a direct interaction with the subject. Gait in particular has been shown to be highly distinctive [29].

Video cameras are the sensors most studied in extant work. Identity inference through face recognition [78] and gait analysis [10, 20–22, 63, 66, 67, 75, 94] has been shown extensively. Similarly, the gait-based activity inference has been demonstrated convincingly [63, 69, 75]. Finally, the inference ability of various soft biometric attributes, e.g. gender[1], age, and ethnicity both via face and gait recognition has been summarized by Dantcheva et al. [16].

Gait-based identification has also been shown for further sensors, including depth cameras [30, 37, 40], thermal imaging cameras [7, 71, 87], and LiDAR [64, 65, 79]. For thermal imaging sensors, face recognition based identification is also possible [4]. While we are not aware of literature that specifically investigates gait-based attribute inference with these sensors, we expect this to be reliably possible: Silhouette extraction is both the most common pre-processing step for video-based attribute inference and identity inference via depth and thermal imaging cameras. Even LiDAR-based identification projects point clouds to depth maps before flattening them to silhouettes. We therefore know from these identity inferences, that silhouettes can be extracted reliably from depth, thermal imaging and LiDAR sensors. As silhouettes are sensor-agnostic, we can use methods designed for video cameras to infer attributes in order to reliably infer age, gender and ethnicity [16]. As these sensors generally do not contain chromaticity information, inference of skin and hair color is not directly possible. At the same time, soft biometrics are often correlated. We therefore are positive that ethnicity can, for example, be used as a proxy to infer skin color with better than random accuracy.

For mmWave radars, extant literature has shown the general ability to infer identities [12, 48, 93], attributes [25] and activities [68]. At the same time, current work is limited to rather small datasets with a maximum of 95 individuals.

Finally, Wi-Fi sensing has also been shown to enable the inference of identities [9, 73, 76, 91], attributes [77] and activities [31, 85, 86]. We want to highlight that these systems do not rely on subjects to carry Wi-Fi devices. Rather, the interference to the Wi-Fi signals themselves from the individuals' body while walking close to communicating Wi-Fi devices can be measured and is sufficiently distinctive to allow for these inferences.

2.2 Privacy Perceptions

A substantial body of work has explored privacy concerns in smart environments, and with some individual sensors.

Sahoo et al. [62] examined privacy concerns around consumer thermal imaging using interviews with 70 participants, half shown explanatory videos. Participants expressed strong worries about bodily and emotional privacy and potential misuse of physiological data; those given explanations were more cautious, indicating that greater awareness increases privacy sensitivity and highlights the need for regulation and education. Windl et al. [84] combined in-depth interviews (n = 14) and a vignette survey (n = 510) to

[1]With "gender recognition", we adopt the common terminology in extant literature which does not properly differentiate between gender identity and biological sex – it therefore refers to automated systems as gender recognition even though the learned features likely refer to the biological sex of individuals which can inherently result in misclassifications.

Table 1: Inference capabilities by sensing technology based on prior work. ✓ indicates capability demonstrated in the literature; (✓) indicates indirect support; – indicates no evidence.

Sensor	Id.	Hair	Skin	Age	Gender	Origin
Video camera (RGB)	✓	✓	✓	✓	✓	✓
Thermal imaging camera	✓	–	(✓)	(✓)	(✓)	(✓)
Depth camera	✓	–	(✓)	(✓)	(✓)	(✓)
LiDAR	✓	–	(✓)	(✓)	(✓)	(✓)
Radar	✓	–	–	✓	✓	–
Wi-Fi	✓	–	–	✓	✓	–

Note. Id. = Identity. Hair and Skin refer to hair color and skin color, respectively.

study perceptions of radio-frequency (RF) sensing. Participants were largely unaware of its capabilities, but developed nuanced concerns once informed. RF sensors were preferred over cameras in private settings, though cameras were favored in security contexts. Emami-Naeini et al. [19] explored public attitudes toward smart-city data collection through interviews with 21 Seattle residents and a survey of 348 U.S. participants. They found the greatest concern for data involving identifiable individuals and the least for environmental data. While participants acknowledged safety as a benefit, they stressed transparency, and consent.

Research on public perceptions of camera-based surveillance consistently shows that attitudes toward being monitored are highly context-dependent [11, 34, 92]. People tend to accept or tolerate surveillance in public or, again, safety-related settings but express greater concern when monitoring serves commercial, workplace, or analytic purposes, such as emotion or health detection. Across studies, privacy perceptions are influenced by factors like the purpose of data use, access and control over footage, and the level of trust in system operators, emphasizing the need for context-aware and transparent approaches to surveillance design and regulation.

Several other studies investigated privacy perceptions on smart homes and Internet of Things (IoT) [6, 41, 53, 83, 90, 95]. Those works show that IoT adoption is driven by convenience and trust but constrained by persistent privacy concerns and limited user understanding. While users often rely on manufacturers or governments to protect their data, their comfort varies by context and perceived benefit. Collectively, the research calls for greater transparency, usable privacy controls, and socio-technical approaches that balance innovation with everyday privacy needs.

Mandal et al. [46] studied users' privacy perceptions of city-wide free Wi-Fi in the U.S. Through a survey of 199 participants, they found that although users were uneasy about data collection and sharing, most continued using the service due to their need for connectivity and trust in public or non-profit providers. The authors suggest that treating municipal Wi-Fi as a regulated utility could enhance long-term privacy protection.

No previous research has examined privacy attitudes toward multiple sensing technologies in a smart city setting collectively, while also investigating how those attitude changes differ between two groups, one exposed to visualizations of the collected data and one that is not.

3 Methodology

To investigate awareness, concern, and attitude change regarding sensing in public spaces, we designed a mixed-methods laboratory experiment that simulates a smart city environment instrumented with multiple sensors. The study was structured to measure three dimensions aligned with our research questions: baseline awareness of sensing capabilities (**RQ1**), sensor-specific privacy concern (**RQ2**), and attitude change under increased transparency about data collection (**RQ3**). In the following, we present an overview of the study process before going in depth with its design justification.

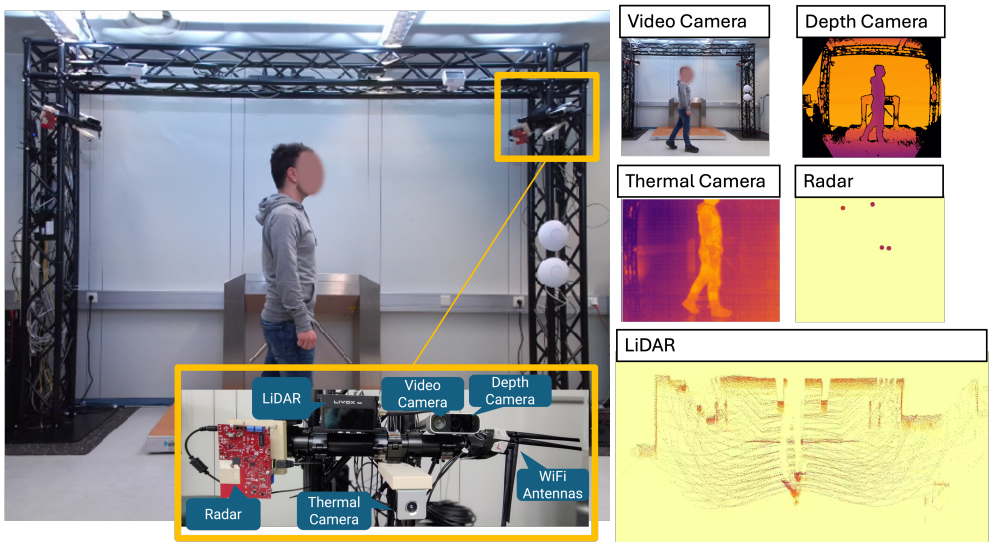
Participants walked through a prototype train-station turnstile equipped with six representative smart city sensors (see Figure 1a). All participants first completed a pre-exposure survey measuring their general awareness of smart city sensing, as well as inference beliefs and privacy concern for each of the six sensors under study. They were then exposed to the instrumented environment under one of two conditions. In the control condition (*walking*), sensors were seen and identified by name, reflecting the minimal transparency typically available in public infrastructures. In the treatment condition (*visualization*), participants were additionally shown visualizations of the data each sensor collects, operationalizing a transparency intervention that makes otherwise invisible data flows observable (see Figure 1b). At the end of the study, participants answered a post-exposure questionnaire designed to gather changes in inference beliefs and privacy attitudes.

3.1 Study Design

3.1.1 In-Lab Smart City Prototype. In the context of a smart city, we chose a train station scenario (see Figure 1a) as a common and relevant setting in which diverse sensing technologies naturally coexist. We built a basic physical infrastructure with a turnstile (to recreate the environment) and a selection of six smart city sensors. The selected sensors are: video camera, thermal imaging camera, depth camera, LiDAR, radar, and Wi-Fi. These six sensors were selected because they reflect the diversity of sensing technologies currently deployed or planned to be deployed in real train stations and mobility hubs, for applications ranging from measuring passenger flows to safety management or temperature screening [1–3, 18, 35, 57]. All of these sensors were mounted on the columns of the smart city prototype, so they were visible to participants.

3.1.2 Sensor Visualizations. Our aim was to approximate a realistic first step toward making sensor data visible in public infrastructures and to assess whether such basic, deployment-feasible transparency mechanisms can affect awareness and privacy attitudes. This design reflects a plausible real-world transparency approach, where municipalities or operators would likely expose simple, out-of-the-box visualizations rather than explanatory interfaces due to cost and integration constraints.

Accordingly, we implemented a basic visualization for each sensor that represents the actual or minimally processed data produced by the device (see Figure 1b). The video, depth, and thermal imaging camera outputs are taken directly from their native imaging interfaces, only applying a color map to the grayscale videos of depth and thermal imaging cameras to increase contrast. Visualizing LiDAR and radar data is challenging, as multi-dimensional data (three dimensions for LiDAR and four for radar) needs to be



(a) Scenario **(b) Sensor Visualizations**

Figure 1: (a) Smart city prototype scenario. Participants walk through a turnstile and see six sensors in the installation. (b) Visualization of sensor data collection shown to participants in the visualization (treatment) condition.

represented by two-dimensional images. For this, we render the point clouds from the point-of-view of the sensor and color the resulting image based on the measured distance of the sensor. For radar, the fourth dimension of velocity is not used for visualization. In summary, we selected visualization styles that closely resemble native sensor outputs with minimal processing. No visualization was presented for Wi-Fi, as this sensing technology's artifacts do not produce directly interpretable visual data. While approaches exist that infer visual information from Wi-Fi artifacts, such as [80, 81], they require substantial transformation (pre-processing, denoising and complex deep learning). As such, they do not align with our methodological goal to approximate realistic, low-cost transparency mechanisms that operators could plausibly deploy without additional inference pipelines.

3.1.3 Survey. We use a two-step survey, fully detailed in the Appendix A, to capture participants' privacy attitudes regarding smart city sensors before and after being exposed to the smart city sensing scenario. The *pre-exposure* questionnaire is structured around the following question categories:

- **Awareness (RQ1).** The study starts with an open question about what type of sensors participants think collect their data in a city's public spaces. Then, we ask them what inferences they consider can be made on data collected by each of the six sensors under study. The questionnaire includes six attributes as potential inferences based on previous work investigating their inferability [16]: identity, gender, age, origin (ethnicity), hair color, and skin color. In total, they evaluate 36 sensor-attribute combinations.
- **Privacy Concerns (RQ2).** Participants rate their privacy concern on a 5-point Likert scale regarding six hypothetical smart city scenarios, each involving one of the six sensors under study. The presentation order of the scenarios is randomized, and the formulation is generic: "*Imagine you are in a public area and you see a* `{sensor_name}` *that collects information about you*". After the rating, we include open-ended qualitative questions, to get further insights on the reasons *why* people are concerned, unconcerned, or unsure.
- **Demographics.** We seek to understand users backgrounds, more specifically: age, gender, and technical background. This block of questions is included at the end of the questionnaire to avoid stereotype biases [60].

After the *pre-exposure* survey, participants are randomly assigned to the walking (control) or visualization (treatment) group. Participants in the walking condition walk through the turnstile area, where the six sensors under study are visibly located. We point out all the sensors to all participants by name. Participants in the visualization condition follow the same procedure and, additionally, they see a visualization of the sensors collecting their data (see Figure 1).

After participants are exposed to the smart city scenario, they fill out a *post-exposure* questionnaire that partially repeats the questions from the *pre-exposure* questionnaire. Specifically, it includes the questions on inference beliefs from the "Awareness" question block, and the full "Privacy Concerns" block plus an open-ended question for participants to explain why their level of concern changed if it did. This design allows us to measure and contextualize changes in privacy attitudes (**RQ3**).

3.2 Study Setup

3.2.1 Deployment and Ethical Assessment. The study was approved by the Institutional Review Board of our university and the data processing was done in coordination with the university's data protection office. Participants were recruited from a local student

panel that uses ORSEE [26] to manage participant registration and session scheduling. This standardized recruitment process helps depersonalize the experimenter–participant interaction and ensures consistent treatment across studies. Eligible participants were required to be over 18 years old, able to walk without assistance, and fluent in German. All participants were informed of the voluntary nature of the experiment, provided informed consent, and were compensated at a rate of €15 per hour; the estimated duration of the study was 60 minutes.

The questionnaires were administered via a local instance of the LimeSurvey web-based survey tool[2], with servers located in Germany and complying with the European data privacy regulations. To reduce inter-subject variance, participants were shown an introductory video rather than given an individual explanation.

3.2.2 Pilot Test. The study was piloted with 22 participants. It confirmed the estimated duration of the study to be 60 minutes, and that the data was collected properly. Based on participant's feedback, we simplified the presentation of the questions asking if each attribute inference is possible for each sensor. To reduce the reported answering fatigue, we designed two matrices with three sensors and six attributes, where participants can tick a checkbox when they believe an inference is possible. Furthermore, since not all participants were familiar with the sensors, we decided to add a short description for each one, so everybody had a common understanding of the terminology.

3.3 Data Analysis

3.3.1 Quantitative Analysis. We provide descriptive statistics for inference beliefs and privacy concern levels associated to the sensors under analysis. Furthermore, we use statistical tests to assess within-subject differences and analyze the impact of *walking* and of *visualization*. To examine how participants' beliefs about data inference changed, we analyze responses to whether each attribute (e.g., gender, or age) could be inferred from each sensor before and after intervention. Each response was binary ("yes"/"no"), and changes within each condition were tested using McNemar's test. Participants rated their level of concern for each sensor on a five-point ordinal scale ranging from "*not at all concerned (1)*" to "*extremely concerned (5)*", with an additional option "*I don't know*". Since "*I don't know*" does not represent a level of concern but rather the absence of a judgment, these responses were excluded from analyses of concern intensity. For within-subject comparisons, only participants who provided valid concern ratings at both time points (before and after intervention) were included, using Wilcoxon signed-rank tests. Additionally, we analyzed the "I don't know" responses separately as an indicator of uncertainty changes. We compared their proportion before and after intervention within each condition using McNemar's test to assess whether exposure to sensor visualizations reduced participants' uncertainty about their privacy concerns. All p-values were adjusted for multiple comparisons using the Benjamini–Hochberg false discovery rate (FDR) correction. We also conducted between-subjects analyses by comparing pre–post change scores between conditions using Mann–Whitney U tests (FDR-corrected).

[2]https://www.limesurvey.org/

3.3.2 Qualitative Analysis. The open-ended questions – involving general awareness of data collection in smart cities, reasons behind privacy concerns, and reasons explaining changes in participants' attitudes after the experiment – were analyzed qualitatively using an inductive thematic coding approach [49]. One researcher developed the codebook and initially coded all responses; a second researcher then independently coded the same data. Cohen's Kappa [14] was calculated to assess inter-coder agreement, and any coding discrepancies were discussed until an acceptable agreement level (Kappa > 0.7) was achieved. The calculated Kappa scores ranged from 0.7 to 0.79, indicating substantial agreement [47]. The complete codebooks are available in the Appendix C. When reporting our qualitative analysis, we report approximate rather than exact counts (see Figure 2). Precise frequencies for individual codes are provided in the codebook.

Questions regarding what made participants feel concerned, unconcerned, or uncertain about the described data collection scenario were asked conditionally, based on the participant's reported level of concern. These follow-up questions were posed separately for each sensor type: camera, depth camera, LiDAR, radar, thermal imaging camera, and Wi-Fi. Because the follow-up question was identical for each technology and the codes and categories were similar across scenarios, we created a single codebook for this question and applied it to all responses, regardless of the specific data collection technology.

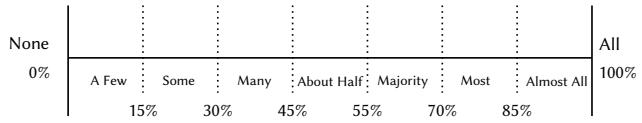


Figure 2: Overview of qualifiers and their corresponding percentages. Originates from Klivan et al. [38]

3.3.3 Sample Size. The study included 172 participants (86 per condition). Belief analyses used the full sample. For concern analyses, after excluding "I don't know" responses, per-sensor within-subject analyses involved between 59 and 86 participants in the walking condition and between 74 and 85 in the visualization condition. Power calculations for paired comparisons of this size indicate that the study is sufficient to detect medium-sized within-subject changes (approximately $d_z \approx 0.3$ on the 1–5 concern scale and ≈10 percentage-point shifts in binary belief and uncertainty measures). The sample was enough to achieve saturation in the qualitative analysis.

4 Results

The study was conducted in November 2024. In total, 1574 individuals were invited to participate, 215 signed up to participate, of which 19 did not show up, leaving 196 participants. After excluding incomplete and pilot data, 172 participants were retained for analysis, with 86 randomly assigned to the control (walking) condition and 86 to the treatment (visualization) condition. Participants were primarily young adults (M = 22.95, SD = 3.25; range 18–34), with a majority identifying as male (60.5%) and reporting an IT-related background (78.5%). As shown in Table 2, the two

groups were demographically similar in terms of gender and age. The treatment group included slightly more participants with an IT background (83.7% vs. 73.3%). On average, the experimental session lasted approximately 44 minutes (excluding introduction and administration, including experience; pre-questionnaire 11.1 ± 4.3 minutes; post-questionnaire 4.3 ± 2.6 minutes).

4.1 RQ1 - Awareness

We answer the first research question about participants' general awareness of smart city sensors and beliefs on inference capabilities.

4.1.1 General Awareness. When asked about what sensors/devices might collect information about people in smart city public spaces, our participants gave a median of 3 answers (ranging from 1-9) and collectively mentioned 49 unique sensors or devices with sensing capabilities (see Figure 6 in the Appendix). Almost all participants identified *sensors and detection technologies*, which included surveillance cameras, general cameras, and a few mentions of thermal imaging cameras, LiDAR, and radar. Many participants also mentioned Wi-Fi or network data as a potential source of data collection in public spaces. These answers highlight the relevance of the selected sensors for this study, although no participant referred to depth cameras. Other commonly identified sources of data collection were related to i) *payment systems and transaction devices*, including card readers, checkouts, and vending machines; ii) *mobile and portable devices*, specially smartphones; and iii) *identification and access technologies*, such as ticket devices and turnstiles.

4.1.2 Inference Beliefs. The heatmap in Figure 3 shows the original beliefs that our 172 participants held about what personal attributes could be derived from the six sensors under study. Perceptions of inference capability were strongly shaped by sensor type. Participants overwhelmingly believed that video cameras can reveal most personal attributes. The majority also believed that gender and age can be derived from other types of cameras (depth and thermal imaging). However, sensors like radar, LiDAR, and Wi-Fi were considered comparatively limited. It is to note that participants see gender and age as easier to infer with respect to other attributes. Interestingly, Wi-Fi was the only modality, beyond cameras, perceived as able to reveal identity, with 71% agreement. The qualitative analysis will reveal that this belief is linked to participants assuming a connection to a Wi-Fi network instead of actual passive sensing (see Section 4.2 for details).

Table 2: Detailed participant demographics by condition.

		Total *(N = 172)*	*Control* ***Walking*** *(n = 86)*	*Treatment* ***Visualization*** *(n = 86)*
Gender	Female	65 (37.79%)	34 (39.53%)	31 (36.05%)
	Male	104 (60.46%)	50 (58.14%)	54 (62.79%)
	Other	1 (0.58%)	1 (1.16%)	0 (0%)
	NA	2 (1.16%)	1 (1.16%)	1 (1.16%)
Age	Min	18	18	18
	Max	34	34	30
	Avg.	22.95± 3.25	23.19± 3.42	22.71 ± 3.07
IT	No	36 (20.93%)	23 (26.74%)	13 (15.12%)
	Yes	135 (78.49%)	63 (73.26%)	72 (83.72%)
	NA	1 (1.16%)	0 (0%)	1 (1.16%)

Note. NA = Not Answered

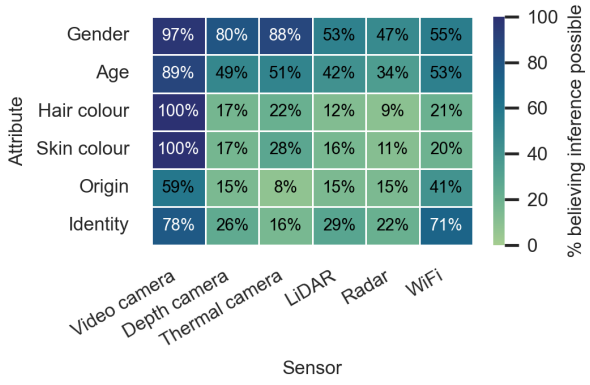


Figure 3: Percentage of participants (n = 172) that believed each attribute can be derived from each sensor.

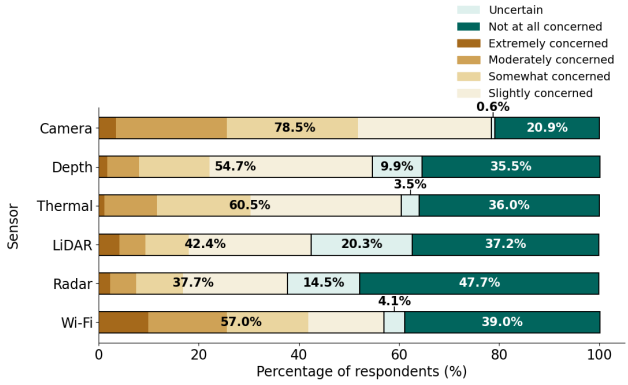


Figure 4: Percentages of participants who were concerned (including level of concern), unconcerned or uncertain for each sensor type before the intervention (n = 172).

> **Key Insight.** Participants showed general awareness that sensing occurs in public spaces, but their understanding was uneven and strongly shaped by visibility. Cameras were widely recognized as highly inferential, whereas other sensors such as radar, and LiDAR, were often seen as limited, for example considered unable to identify people, when they actually have this capability. Comparing these beliefs with established technical capabilities reveals systematic gaps and misconceptions, indicating that public understanding only partially reflects the real inference potential of smart city sensing.

4.2 RQ2 - Privacy Concerns

We now analyze people's privacy concerns per sensor to answer the second research question. As an overview, Figure 4 presents the absolute percentages of participants who expressed concern, no

concern, or uncertainty regarding the different sensors before being exposed to smart city sensing scenario. The graph also includes the levels of concern (Extremely concerned - Slightly concerned). Overall, 78.5% of participants reported feeling extremely, moderately, somewhat, or slightly concerned about the use of video cameras, followed by 60.5% for thermal imaging cameras, 57% for Wi-Fi and 54.7% for depth cameras. In contrast, lower levels of concern were observed for LiDAR sensors (42.5%) and radar (37.8%).

4.2.1 Reasons for Concerns. Here we discuss reasons for concerns and non-concerns mentioned by participants for each sensor.

When discussing sensing technologies in public spaces, participants repeatedly raised similar types of concerns, though the emphasis differed by sensor. The most common issues related to *data storage and processing*, particularly uncertainty about what data are collected, how they are used, and for what purpose, followed by recurring worries about *surveillance and privacy*. Beyond these general patterns, specific reasons emerged for each sensor type.

When asked about the **video camera**, many participants expressed concern about *surveillance and privacy*, fearing they were being observed, monitored, or tracked. They also worried about losing control over their personal data, and being identified, profiled or felt that their privacy is being invaded. Despite this, many still saw potential advantages in improved public safety: *"I feel very watched, even though it can, of course, be an advantage for my safety."* (transl.) - P48. An equal number emphasized concerns about *data storage and processing*, as they were unsure how their footage might be stored, used, or shared: *"I wouldn't really know what data is being collected about me at this moment. The uncertainty makes me concerned."* (transl.) - P51.

For **depth cameras**, *data storage and processing* stood out as the primary concern, mirroring that of video cameras. Many participants questioned how depth data were managed or disseminated, and a few were unsure about the exact type of data collected. Some also brought up *necessity and context*, noting that their level of concern depended on where and why these cameras operated. A similar number mentioned *surveillance and privacy*, associating depth cameras with the feeling of being observed or located.

Concerns about **LiDAR** followed a similar pattern, with *data storage and processing* again being the central issue. Some participants lacked clarity about what LiDAR captures and how the information is handled. Some questioned *necessity and purpose* of collecting such data in public spaces, while others admitted that their *limited knowledge about the technology* made them uneasy. A few considered LiDAR a rare and unusual situation, leading to increased concern: *"Not knowing what kind of data the device can learn about you. You're unfamiliar with it and feel distrustful and skeptical."* (transl.) - P107.

For **radar** systems, *data storage and processing* remained a predominant concern, particularly due to missing transparency around data handling. Many also expressed *surveillance and privacy* worries, fearing potential tracking or location disclosure. Some doubted the *necessity* of radar sensors in public. One person mentioned the *risk* of radiation that might affect their health. One felt concerned since they believe the data is being collected continuously.

In **thermal imaging** scenarios, many participants again focused on the *necessity and context* of data collection, questioning why such sensing was needed in public areas. The second most commonly cited reason was related to *data storage and processing* due to unclear dissemination procedures. While a few feared being personally *identified*, others believed it was unlikely, though they still felt uneasy. Some participants were particularly concerned about collection of *physiological or physical features* (e.g., body temperature or proportions), and a few noted that thermal images might reveal *health-related* information.

When asked about **Wi-Fi** data collection in public spaces, about half of the participants mentioned concerns related to *data storage and processing*, with some worrying about their personal data in general. A few participants stated that Wi-Fi data are *sensitive*, and others noted that their online behavior could be tracked and recorded, which left them concerned. A few participants also mentioned that the use of public Wi-Fi networks is *voluntary* and that Wi-Fi is useful and important for citizens, leaving them only slightly concerned. Another reason for limited concern, mentioned by a few participants, is their *acceptance* of the situation, as they stated that they are already used to using public Wi-Fi networks: *"I'm used to routers being in public areas. Besides, I see a purpose in their presence, since they are not (only) there to gather information."* (transl.) - P166.

Some participants feared that their devices could be hacked when connected to public Wi-Fi networks.

> **Key Insight.** Participants' concerns strongly depend on transparency and understanding, when they do not know what is collected, how it is used, or why, they feel concerned. Familiarity and perceived usefulness mitigate these worries somewhat, but lack of clarity about data handling remains the overarching issue across all sensor types.

4.2.2 Reasons for Non-Concerns. Out of 172 participants, 47.7% indicated that they had no privacy concerns regarding radar data. The percentage of participants expressing no concerns was 36% for thermal imaging data, 37.2% for LiDAR data, 39% for Wi-Fi data, 35.5% for depth camera data, and 20.9% for video camera recordings.

Across all sensing technologies, participants expressed non-concerns mainly when they perceived low personal risk, limited data sensitivity, or clear benefits. While the specific justifications differed by sensor, recurring themes emerged: *normality* of data collection in public, *perceived harmlessness* or *possible identification*, and *trust* in the purpose or entity responsible for collection. For **depth cameras**, **LiDAR**, **radar**, and **thermal imaging cameras**, the majority of participants emphasized the same main idea: that these technologies collect little personal data and that individual *identification* is not possible. This general belief that data are limited or abstract due to low-resolution images made these sensors seem harmless to many participants. For these same sensors, a few participants stated that their *limited knowledge about the underlying technology* also contributed to their lack of concern. Additional, sensor-specific reasons are described below.

When asked why participants were not at all concerned about **video camera** recordings, about half of the participants mentioned *security and safety* reasons, specifically, that video camera recordings in public spaces could make them feel safer and help reduce law violations and criminal activity: *"The city isn't uploading me to TikTok; they only look at the footage if something happens that is*

criminally or otherwise relevant, and I don't generally plan on doing anything like that." (transl.) - P193. About half of the participants also stated that being recorded is *normal* to them and something they were used to. Some participants mentioned that they *trust* the governmental agencies responsible for collecting the data.

For **depth cameras**, the majority of participants cited the *type of data* and its limited potential for harm as reasons for their lack of concern: *"I can't think of any use of the depth camera that would be harmful to me. In particular, I mainly associate depth cameras with harmless measurements."* (transl.) - P82.

Regarding **LiDAR**, some were unconcerned by the possibility of *location tracking*. A few also pointed out that other technologies, such as radar, Wi-Fi, or video cameras, already collect data, meaning LiDAR did not pose additional concern. One person mentioned that they are concerned about the increasing *image resolution* of today's technologies.

Coming to **radar** data, while many participants were concerned about their *location* being revealed, some were not worried at all about the collection of positional data in public spaces. A few participants mentioned that radar sensors can be useful in *traffic* contexts, such as navigation systems, taxis, and traffic surveillance.

About **thermal imaging camera**, a few participants also expressed trust in the data collectors here, and another few highlighted the *advantages* of adopting this technology in public spaces, for example, for practical applications like automatic light switches, for safety purposes, or for social reasons such as helping people when it is cold. In contrast to participants who were concerned about their *body information* being tracked, a few participants considered data such as body temperature or body contours to be of little value and were therefore unconcerned.

Reasons for not being concerned about **Wi-Fi** data, cited by many participants, were that recording Wi-Fi data is *normal* and something they have become accustomed to. Many also referred to their own behavior and knowledge, noting that the use of public Wi-Fi networks is *voluntary* and that they therefore have the option to connect or not, which left them unconcerned. Though one person mentioned that they have no control over what happens to their data but try to protect themselves by using a VPN. Others mentioned that they see *advantages* in having Wi-Fi available in public spaces, which likewise made them feel unconcerned.

> **Key Insight.** Participants who were not concerned generally perceived these sensing technologies as either safe, useful, or familiar, capturing data too abstract to threaten their privacy, operating under legitimate authority, or providing clear social benefits. However, evident misconceptions surface, especially the belief that identity cannot be obtained from certain sensors. Additionally, participants do not understand Wi-Fi as a sensing technology but conflate Wi-Fi sensing with the connection to public Wi-Fi networks.

4.2.3 Reasons for Uncertainty. We also asked participants who were uncertain about their level of concern to explain their reasons. This group included 20.3% of the participants for LiDAR data, 14.5% for radar, 9.9% for depth, 3.5% for thermal, 4.1% for Wi-Fi, and 0.6% (one participant) for camera data.

Except for video camera data, nearly all participants who were unsure about their level of concern across the other sensor types cited reasons related to *unawareness and a lack of knowledge*. Specifically, a lack of understanding of the technology was the main reason mentioned for depth data by the majority of participants, and for LiDAR data by about half. Some participants, when asked about radar data, explained that it was unclear what kind of data these sensors collect—similar to the uncertainty expressed about LiDAR and depth data. About half of the participants gave this reason when discussing Wi-Fi data. Regarding thermal imaging data, many participants stated that it was unclear whether *identification* of individuals was possible or whether personal information could be inferred.

Many participants who were unsure about their level of concern pointed to issues related to the *meaning and purpose* of the data collection scenario, especially LiDAR, radar, and depth camera.

One participant described themselves as uncertain because they recognize the benefits of video camera data collection but at the same time is concerned: *"On the one hand, I view the surveillance of public spaces for purposes such as police investigations positively. On the other hand, I also worry that the data could potentially fall into the wrong hands or be misused in general."* (transl.) - P134.

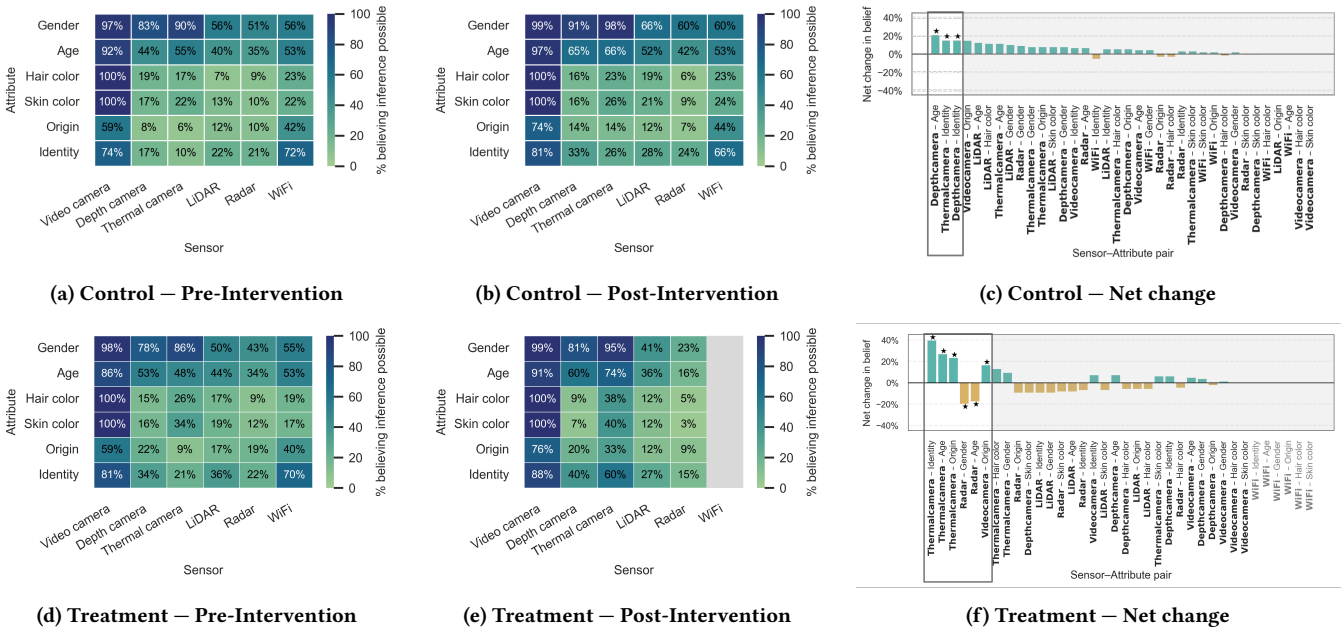
Security, safety, and privacy reasons also contributed to participants' uncertainty about their stance on data collection in public spaces. When asked about LiDAR and radar, one participant expressed concern that smartphone data could be tracked through these sensors. Another participant mentioned that the advantages of thermal imaging data collection might outweigh the disadvantages of personal data being gathered in public areas.

> **Key Insight.** Participants' uncertainty largely stems from limited understanding of the sensing technologies. Mirroring patterns seen in reasons for concern, the lack of transparency about what data are collected and why plays an important role in uncertainty. For some, uncertainty reflects a perceived trade-off between benefits such as safety or convenience and the potential privacy risks involved.

4.3 RQ3 - Changes in Attitude

To address the third research question – whether participants changed their beliefs and concerns about different types of data following the intervention – we compared beliefs and concern levels before and after the intervention. An open question to capture participants rationales was only posed when attitudes changed between before and after the intervention. We first present the quantitative findings, followed by the qualitative analysis of reasons behind the attitude change.

4.3.1 Changes in Inference Beliefs and Privacy Concerns. Changes in **inference beliefs** are summarized in Figure 5. In the walking group (control), three sensor-attribute pairs showed significant within-subject changes ($p < .05$). Participants became more likely to believe that depth cameras can infer age and identity, and that thermal imaging cameras can infer identity. These increases indicate that simply being made aware of the sensors in the environment, even without visualization feedback, can raise participants' awareness of the potential for personal information inference.



(a) Control — Pre-Intervention **(b) Control — Post-Intervention** **(c) Control — Net change**

(d) Treatment — Pre-Intervention **(e) Treatment — Post-Intervention** **(f) Treatment — Net change**

Figure 5: Beliefs about which attributes can be inferred from each sensor, and net changes in belief, for the control (top row) and treatment (bottom row) groups. Heatmaps show the percentage of participants who believe an attribute can be inferred pre- and post-intervention; bar charts show the net change in proportion of "yes" responses for each sensor–attribute pair (positive values indicate an increase in belief; negative values, a decrease). Values for Wi-Fi in the treatment group are not shown since there was no visualization for Wi-Fi data collection.

In the visualization (treatment) group, where participants viewed visualizations of the sensors' data, six significant changes were observed ($p < .05$). Beliefs about the thermal imaging camera inference capabilities increased for identity, age, and origin, and beliefs about the video camera increased for origin. In contrast, beliefs about radar decreased significantly for gender and age. Overall, the results suggest that visualization primarily increases perceived inference potential for imaging-based sensors (video, depth, thermal) while reducing inference beliefs for the other sensors (radar, LiDAR). In other words, after seeing what different sensors record, participants tended to believe that imaging-based sensors could reveal more personal information than they initially thought, whereas abstract sensing modalities appeared less revealing than expected. Between-subjects change-score tests confirmed significant condition differences for thermal-camera identity ($p = .008$), radar gender ($p = .008$), and radar age ($p = .022$).

Table 3: Pre- and post-intervention average privacy concern (M) per sensor and group. Concern was measured on a five-point scale from 1 ("not at all concerned") to 5 ("extremely concerned"). p-values are from Wilcoxon signed-rank tests. Arrows indicate the direction of change in concern.

Sensor	Group	n	Pre M (SD)	Post M (SD)	p
Camera	Control	86	2.66 (1.13)	2.97 (1.25) ↑	**.002**
	Treatment	85	2.54 (1.17)	2.86 (1.29) ↑	**.001**
Depth	Control	77	1.95 (1.02)	2.06 (0.99) ↑	.090
	Treatment	78	1.97 (0.99)	2.21 (1.10) ↑	.090
Thermal	Control	82	2.04 (1.08)	2.22 (1.11) ↑	**.003**
	Treatment	84	2.11 (1.03)	2.50 (1.14) ↑	**.002**
LiDAR	Control	59	1.93 (1.27)	2.02 (1.18) ↑	.236
	Treatment	74	1.95 (1.06)	1.92 (1.02) ↓	.965
Radar	Control	71	1.87 (1.22)	1.93 (1.10) ↑	.371
	Treatment	75	1.65 (0.86)	1.33 (0.62) ↓	**.002**
Wi-Fi	Control	82	2.45 (1.41)	2.61 (1.43) ↑	.090

Note. Higher scores indicate higher privacy concern. Bold p-values are significant at $p < .01$ (FDR-corrected). Wi-Fi was only included in the control group, as no visualization was presented for this sensor in the treatment condition.

Regarding **privacy concerns** (Table 3), average concern levels were generally low to moderate, ranging from around 2 ("slightly concerned") to 3 ("somewhat concerned") on a five-point scale. In the control group, concern significantly increased for the camera ($p = .0016$) and thermal imaging sensors ($p = .0033$). In the treatment group, which viewed the sensor visualizations, concern also increased for the camera ($p = .0014$) and thermal imaging sensor ($p = .0015$), but decreased for radar ($p = .0015$). No significant differences were found for depth or LiDAR, and Wi-Fi was not visualized. Overall, both groups became more concerned about imaging-based sensing technologies, while visual feedback appeared to reduce concern for less familiar sensors such as radar. These patterns are corroborated by between-subjects change-score tests. When pre–post change scores were compared between walking and visualization, for privacy concerns, only the radar sensor showed a significant between-condition difference ($p = .019$), with

Table 4: Percentage of "I don't know" responses pre- and post-intervention per sensor and group. p-values are from McNemar's test and corrected for multiple comparisons (FDR). Arrows indicate the direction of change in uncertainty.

Sensor	Group	Pre (%)	Post (%)	p
Camera	Control	0.00	0.00	1.000
	Treatment	1.16	0.00 ↓	1.000
Depth	Control	10.47	6.98 ↓	.500
	Treatment	9.30	0.00 ↓	**.020**
Thermal	Control	4.65	0.00 ↓	.375
	Treatment	2.33	0.00 ↓	.625
LiDAR	Control	26.74	22.09 ↓	.582
	Treatment	13.95	4.65 ↓	**.020**
Radar	Control	17.44	10.47 ↓	.187
	Treatment	11.63	2.33 ↓	**.036**
Wi-Fi	Control	3.49	3.49	1.000

Note. Bold p-values indicate significant changes at $p < .05$ (FDR-corrected). Wi-Fi was only included in the control group, as no visualization was presented for this sensor in the treatment condition.

concerns decreasing in the visualization condition and remaining approximately stable in the walking condition. All other sensors showed no significant between-condition differences in concern.

Instead of expressing a concern level, participants could also report when they did not know whether they were concerned. Table 4 summarizes which sensors people were privacy-uncertain about and how uncertainty changed after seeing the sensors and data visualizations. Uncertainty was very low for camera and thermal imaging sensors at both time points and did not change significantly. In the walking (control) group, no significant differences were observed. In the visualization (treatment) group, uncertainty significantly decreased for depth imaging sensors ($p = .020$), LiDAR ($p = .020$), and radar ($p = .036$), dropping from 9–14% undecided before exposure to less than 5% afterward. These results suggest that viewing sensor visualizations reduced participants' uncertainty about their privacy concerns, particularly for less familiar sensors.

> **Key Insight.** Sensor data visualizations shaped both beliefs about sensor inference capabilities and privacy concerns. Compared to the general rise in perceived inference and concern that appears with just seeing the sensors, visualising the data led to more calibrated responses: sustained concern for imaging-based sensors but reduced concern for less familiar, complex to visualize sensors. Overall, visual feedback reduced uncertainty and helped participants form privacy judgments.

4.3.2 Reasons for Changing Privacy Attitudes. For all sensors, the majority of participants (ranging between 61.7% and 75.5%) did not change their privacy concern level after the intervention in both the walking and visualization groups. The biggest changes occurred for camera and thermal imaging camera sensors, with 26.8% and 31.4% of participants feeling more concerned, respectively. The number of switches to less concerned where biggest for radar and LiDAR, with 18.6% and 14% of participants changing their mind in this direction, respectively. We now discuss reasons behind attitude changes.

Across all sensors, participants most commonly reported changing their privacy attitudes due to new or revised *expectations* about the amount, type, or visibility of data being recorded. This was particularly the case for some of the treatment participants when it came to **video camera**, **depth camera**, **LiDAR**, and about half of treatment group for **thermal imaging camera**. Those realized that more data could be collected than they had initially assumed, leaving them more concerned than before. The opposite effect, finding that less data were recorded than expected, was cited by the similar number of participants for depth camera and lidar, and many of radar treatment group as a reason for reduced concern. Furthermore, the *practical experience* of participating in the experiment increased concern levels for a few to some participants across all sensors, with no notable difference between the control and treatment groups. Another recurring aspect was perceived *identification*, especially for some participants in the treatment group of video camera, and a few treatments participants of depth camera, lidar and thermal imaging camera: the belief that one's identity could be recognized through the data raised the level of concern. On the other hand, recognizing that identification was unlikely applied to the treatment groups of the depth, radar, LiDAR, and thermal imaging camera data.

Feelings of being *observed or monitored* also surfaced repeatedly, especially in the control groups of camera, depth, lidar, radar and thermal imaging, who did not see a visualization. In the following, we report sensor-specific reasons for changes in privacy attitudes.

Some participants reported being more concerned about **video camera** recordings after the intervention, with concerns nearly evenly split between the treatment and control groups. Participants became more aware of the different *types of data* that could be recorded, such as personal information and motion, yet the intervention appeared to have minor effect on this awareness. One participant stated that dealing with the topic made them aware and more concerned after intervention.

A few participants, however, were less concerned after the intervention. A few from the control group reported feeling *safer*, and one person from the treatment group said they saw *no danger* in the data collection afterward.

Some participants became more concerned about **depth camera** data after the intervention because they developed concerns about particular *types of data* being collected, similar to concerns they had expressed earlier. They believed that personal information was being recorded, that motion recording itself was worrisome, and that gender, or age might be recognizable. One person was concerned because they did not know what a depth camera looks like and could easily confuse it with a video camera.

Reasons for being less concerned in the treatment group were that they believed that no appearance-related data was being collected, and that faces were not recognizable.

Some participants changed their attitudes regarding **LiDAR** data. For being more concerned, the split is even between both treatment and control group. One person mentioned that the survey design itself, continuously asking about their concern, made them feel concerned. A few participants realized that a lot of data is being recorded by the LiDAR sensor. A few mentioned that the fact that their origin, clothing, and hair color is recognizable through LiDAR made them more concerned. A few others from the treatment group

mentioned that they do not understand what data is being collected and therefore feel more concerned, similar for the control group. Surprisingly, some of the control group mentioned *specific data* that is being collected, which resulted in more concern, like motion recording, personal information, stature or posture recognizable, localization possible, and origin recognizable. Those were formulated more as possibilities than as known facts.

Reasons for being less concerned for the treatment group were that no real pictures or images were being recorded, and faces and gestures were not recognizable. For the control group, one person each mentioned they saw no danger in the intervention and that localization was not possible, leaving them less concerned than before. Reasons for uncertainty were that people from the control group did not know what data is being collected.

Some participants changed their attitudes regarding **radar** data after the intervention. More people from the control group felt more concerned after the intervention than from the treatment group. Reasons for the control group to feel more concerned were the belief that motion, stature or body posture, and location could be recorded through radar. Others feared that recording would happen without any reason. One person felt more concerned because of the continuous recording of the sensor, another because events can be recorded through radar data. Only a few participants from the treatment group felt more concerned after the intervention. One reason was that it gave them *more knowledge* about what data is being collected in general. Another reason for concern was that localization is possible. Reasons for less concern from control group participants were that they did not see *harm* in the data from the intervention: *"Doesn't affect my everyday life as long as I have nothing to hide."* (transl.) -P119.

The **thermal imaging camera** has the most "more concerned" participants in general. More people from the treatment group were more concerned after the intervention than people from the control group. Regarding the *type of data*, a few of the treatment group were concerned about personal information, motion recording, body temperature, and that gender and facial features could be recognized through that sensor. Similar reasons were mentioned by the control group. Additionally, one participant mentioned that age might be recognized, and another participant was concerned that recording might occur without a specific reason.

Some participants from the treatment group felt less concerned, citing the common reasons mentioned above. Only one person from the control group felt less concerned; their reason was that thermal imaging do not collect personal information.

Only some participants, the smallest number overall, changed their attitude after the intervention when it came to **Wi-Fi** data. None of them saw the visualization of Wi-Fi data, but about half of those who changed their attitude felt more concerned after the intervention. The main reason was that people did not understand how and what *type of data* was being collected. In contrast, a few participants mentioned that the intervention made them realize how the data is collected by the routers, approximately half of which asked us about the functionality of Wi-Fi sensing: *"In everyday life, one tends to underestimate the number of routers that collect data from you, in addition to those you are actually connected to. Within the framework of the experiment, this becomes even more apparent."* (transl.) -P186.

A few feared hacker attacks, misuse of the data, unauthorized sharing with third parties, or were concerned about how the data would be analyzed after collection. Many participants who changed their attitude were less concerned about Wi-Fi data after the intervention, as they realized that the data was being collected differently than they had thought before, or because they believed they knew how to use public Wi-Fi consciously. A few mentioned that no personal information can be gathered.

> **Key Insight.** Participants' changes in privacy attitudes were driven primarily by adjusted perceptions of what and how much data the sensors collect. Across all sensor types, increased concern often followed realizations, through the intervention or reflection, that more data, or more personal or identifiable information, could be captured than previously assumed, as well as awareness of being monitored. Conversely, reduced concern typically stemmed from the opposite perception: noticing or believing that less, non-identifiable, or less personal data were recorded, or that sensor outputs appeared abstract and non-threatening.

5 Discussion

We elaborate on the implications and recommendations that stem from our study, and provide a comparison to previous work as well as a discussion of limitations to contextualize and facilitate the interpretation of our findings.

5.1 Study Implications and Recommendations

Our study revealed that **people have an incomplete understanding of smart city sensor capabilities**. With technological advancements in processing, algorithms, and computing, sensor data can be instrumented and used to infer identities directly or personal attributes that, in combination with other data points, become identifying. Despite all six of the smart city sensors in our study being technically able to identify people, the vast majority of our participants originally thought identification was only possible with video cameras or through Wi-Fi – the latter erroneously understood as connecting to a public network instead of as a sensing technology. These knowledge gaps are critical, as they shape perceived privacy risks and can limit the ability to make informed choices.

Recommendations. Information about sensors, given by marketers, researchers, or in public communication, should provide nuanced descriptions of sensors' full privacy implications. In smart cities, regulatory interventions could focus on ensuring that claims about privacy-friendliness are correct, as well as on requiring the deployment of sensing technologies that minimize data collection when several options are possible. Further research on citizens' mental models and understanding of specific sensors would allow exploring how to elevate sensing literacy.

Privacy judgments are influenced by transparency. We used two levels of transparency: sensor visibility and real-time data collection visualization. Seeing the physical sensors alone influenced participants' privacy perceptions, leading them to correctly believe that cameras other than video cameras can infer identities. Visualization has a stronger impact, as people understood by seeing, and were able to re-calibrate their understanding of imaging-based

sensors to be more aligned with their actual technical capabilities. Visualizations also influenced privacy concerns, leading some participants to feel uneasy after knowing what a thermal camera "sees", or even imagining further potential privacy-invasive inferences that were not part of the study (e.g., health issues becoming apparent from thermal data). However, for sensors that are even less familiar and technically far from how human perception works, visualizations did not increase participants' understanding of privacy risks, revealing an interpretation gap that requires addressing. We used basic visualizations that represent the actual or minimally processed data produced by sensors, and our study confirms that these types of visuals are not generally sufficient. Our study highlights the value of transparency, and aligns with prior work exploring privacy concerns in smart cities, showing that citizens seek transparency [19].

Recommendations. Smart city sensor deployments should be at least clearly physically visible as a minimal form of transparency. Video cameras and signage for video camera presence are frequent in public areas and familiar to people, though this is not the case for other sensors, whose visibility or iconography are less salient. This lack of transparency has led in the past to several smart city projects facing public backlash and ultimately being shut down [23, 33]. Research is necessary to understand what type of transparency formats (visualizations, iconography, labels, acoustic warnings, etc.) are most efficient for citizens. Once this is understood, legal guidelines can be put in place with specific transparency requirements for smart cities.

Privacy concerns about smart city sensing are contextual. The qualitative analysis surfaced privacy perception nuances and trade-offs associated to the context of data collection. To better understand these contextual nuances and evaluate how participants' mental models align with real-world scenarios, we take the Contextual Integrity (CI) framework [55] into consideration. It conceptualizes privacy as the appropriateness of information flows defined by five parameters: the data sender, subject, recipient, attributes, and transmission principles. In our context, the participant represents the subject, the data senders are the sensor devices, and the attributes correspond to the sensor data being collected. We now focus on recipients and transmission principles[3]. This enables us to examine how participants' understanding of these factors.

Previous work [27, 59] outlines key sensor applications in real-world urban spaces. Those are energy, health, mobility, security/safety, water, and waste management. They also report real-world use cases of different cities worldwide [5, 54, 56, 58]. We situate participants' perceptions within these existing practices using CI and we found that participants most often referred to the purposes and conditions of data collection rather than to specific recipients, suggesting that participants mostly think about why and under what conditions data are used and collected, rather than by whom. One possible reason could be that actors within the actual data ecosystems, such as cloud providers or service operators, who function as intermediaries in data processing, remain invisible to them.

[3]An example flow could be: "A LiDAR sensor (sender) collects movement data (attributes) about individuals in a public space (subjects). The data are transmitted to the city's mobility department (recipient) to improve traffic management and public safety (transmission principle)"

Transmission Principles. Consistent with real-world smart city purposes [5, 27, 54, 59], participants perceived data use related to security/safety, mobility, research, and city services as generally not concerning, indicating that participants viewed data uses aligned with real-world smart city applications as acceptable, since those were viewed as contributing to public benefit. In contrast, purposes such as advertising, surveillance, or unknown uses were viewed as more concerning in participants' open responses, reflecting concerns about transparency and commercial exploitation. Conditions including consent were also central to positive judgments. References to the GDPR in participants' open responses (e.g., "GDPR is protecting") further indicated that regulatory compliance and trust in governance shape privacy perceptions. Conducting the study in Germany likely influenced participants' sensitivity to data use conditions, given the country's strong privacy culture and the enforcement of the GDPR. Under the GDPR, potential inferences of sensor data would be prohibited without explicit consent or a lawful basis, aligning with participants' perception of trust and desire for transparency in our findings.

Recipients. Participants' non concerning recipients mostly aligned with current practices [5, 24, 27, 54, 59], including cities, law enforcement agencies (e.g., police), and researchers. Conversely, private companies, third parties, hackers, and sometimes even governments were perceived as more concerning recipients, especially when their roles or intentions were unclear. Interestingly, several actual recipients prevalent in real-world smart city infrastructures, such as vehicle manufacturers and mobility service providers, cloud providers, road traffic authorities, or health authorities [5, 24, 27, 56, 58, 59], were rarely mentioned by participants. This may indicate not necessarily a gap in their mental models but rather that participants focused on more visible or immediately relatable actors within the data ecosystem, as mentioned above. Participants may also conceptually subsume entities like road traffic and health authorities under the broader category of "the city" or its administrative bodies.

Recommendations. Further research could focus on gaining a deeper understanding of contextual aspects of data sharing acceptability in smart cities. CI theory could be a helpful lens to analyze acceptability factors that can be used to evaluate how current smart city privacy policies align to citizens' expectations and shape future guidelines. Future studies could apply CI by systematically varying recipients and transmission principles, reflecting real-world practices, to evaluate their influence on perceived acceptability. This design process should consider diverse populations, e.g., through vignette-based surveys, and engage citizens as active participants, e.g., through focus groups.

5.2 Comparison to Previous Works

Similarities and differences between our findings and prior research on privacy perceptions across different sensors and cameras can be observed.

Regarding Wi-Fi, Mandal et al. [46] examined perceptions of city-wide free Wi-Fi and found that users generally accepted data collection because of their trust in public or non-profit providers and their need for connectivity. In our results, participants' comfort towards Wi-Fi data collection stemmed from perceiving it as a normal, beneficial service and from feeling personally responsible

for their own online behavior rather than from institutional trust. Nevertheless, participants were most concerned about the collection of personal and potentially identifiable data.

Comparable patterns emerge when contrasting our findings on thermal imaging with those of Sahoo et al. [62], as participants in both studies had concerns toward physiological data.

Similarly, parallels with Windl et al. [84] and Emami-Naeini et al. [19] can be seen: a lack of awareness and understanding of sensing technologies contributed strongly to privacy concerns. At the same time, participants acknowledged benefits such as enhanced security and safety, particularly in the context of public video surveillance.

Prior research on camera-based monitoring indicates that privacy perceptions are highly context-dependent [11, 34, 92]. While our study did not explicitly vary context or included scenario-based evaluations, a few participants referred to situational factors, such as location and purpose of data collection, when discussing their concerns. Many also emphasized that sharing health-related data felt particularly sensitive, and that their understanding of the technology strongly influenced how concerned they were. Cameras are among the most established sensing technologies in public spaces, and public attitudes toward them have shifted from initial privacy concerns to broader acceptance grounded in perceived safety and security benefits, despite mixed empirical evidence such as our findings or those by prior work [92, 96]. This pattern helps contextualize our results, as participants likewise considered safety-related data uses less concerning. Those insights from prior work on camera surveillance help anticipate how perceptions of other sensing technologies could evolve. Emerging sensors for urban spaces such as LiDAR, radar, depth, or thermal, remain less familiar to the public, and their potential benefits are not yet widely recognized. Our study therefore offers a baseline to examine whether acceptance of these newer sensing technologies will follow a trajectory similar to the normalization of cameras or evolve differently as awareness of their functions grows.

Interestingly, and in contrast to findings from previous studies [19, 36, 41, 53, 83, 84, 90, 95], trust was mentioned far less often in our participants' responses. Whereas earlier work highlights trust in manufacturers, governments, or data collectors as a key factor influencing privacy attitudes, our participants focused more on individual responsibility, awareness, and the perceived relevance of the collected data.

5.3 Limitations

We acknowledge some limitations of our study design. While we investigated concerns in urban public spaces, the actual setup was a prototype within a lab which could influence participant's experience, particularly since the sensing technologies were more obvious (and shown all at once) in comparison to a real-world scenario. One limitation of the study was a design issue: when asked about changes in their attitudes, two participants reported being confused by the response options and were unsure which option represented a greater or lesser degree of concern. This confusion may have been influenced by the fact that the study was conducted entirely in German. Our study is biased in terms of ethnicity and age and limited to able-bodied individuals. It is therefore potentially not representative of the public.

Additionally, the absence of visualization methods that require minimal processing for Wi-Fi prevents us from drawing conclusions about the effect of data visualization on privacy concerns and beliefs for this sensor. At the same time, the findings for the no-intervention condition (RQ2) remain valid and informative, highlighting important misconceptions about this sensing modality. Future studies could follow up by testing comparable more elaborated visualizations across sensors, including Wi-Fi.

Our sample was skewed to young, male, and tech-savvy people, whose perceptions may not represent those of the general population (see Appendix B.1 for demographic sensitivity analyses). In particular, our findings may underestimate broader public misconceptions. We encourage future work with more diverse participants to capture nuanced perceptions and build ground for designing smart city transparency that works for everyone.

Finally, the study design may have biased participants in some ways. Due to data protection requirements, the participant information sheet mentioned all sensors in our scenario (and the introductory video some of them), which could have biased the answers for the first question. We did not specify the type of radar used or that Wi-Fi would collect data via device-free human sensing. This could have misled participants to believe other sensing types to be used, in particular in the pre-questionnaire. Finally, when participants asked us questions about the sensors or potential inferences, we did withhold any answers which could have affected answers in the post-questionnaire. Our data includes notes of any questions that were answered.

6 Conclusion

In this paper, we investigated privacy attitudes towards data collection by a number of different sensing technologies that are planned to be used in smart cities. In an extensive intervention-based lab study with 172 participants, we found that while participants were generally aware of sensing in public spaces, their beliefs regarding inference capabilities showed significant misconceptions. The level of concern that participants have is strongly dependent on transparency and understanding of the data collection. Finally, live visualizations of the collected data enabled re-calibration of the perceived privacy risks, though their effect was limited.

These findings allowed us to highlight significant gaps in knowledge and understanding of contemporary sensing technologies and draw conclusions about recommended privacy-respecting smart city environments that address citizen's informational needs and expectations. Our recommendations, such as requiring transparent information about any public sensing, allows evidence-based policymaking to shape our cities' future.

Acknowledgments

The authors used generative AI-based tools to revise the text, improve flow and correct any typos, grammatical errors, and awkward phrasing.

Special thanks to Vanessa Susewind for translating the survey instrument and contributing it to the appendix.

This work was funded by the Topic Engineering Secure Systems of the Helmholtz Association (HGF) and supported by the KASTEL Security Research Labs, the Cluster of Excellence "Centre for Tactile

Internet with Human-in-the-Loop" (EXC 2050/2 CeTI – DFG Project ID 390696704), the Research Project SynthTrace (FKZ 16KIS2674K) and Anymos (FKZ 16KIS2507). The user studies were conducted via the Karlsruhe Decision&Design Lab (KD²Lab), an experimental lab funded by the DFG and the Karlsruhe Institute of Technology (INST_12138411-1_FUGG).

References

[1] 2022. Using SensMax TAC-B radar people-counting sensors at train stations. https://sensmax.eu/news-blog/using-sensmax-tac-b-people-counting-sensors-at-train-stations/.

[2] 2023. DASA-funded AI and LiDAR innovation helps enhance crowd safety. https://www.gov.uk/government/news/crowd-watch-dasa-funded-ai-and-lidar-innovation-helps-enhance-crowd-safety.

[3] 2023. OpenSpace and Avanti West Coast Rail: Using 3D LiDAR to improve crowd analytics in UK stations. https://ouster.com/insights/case-studies/open-space-and-avanti-west-coast-rail-uk.

[4] David Anghelone, Cunjian Chen, Arun Ross, and Antitza Dantcheva. 2022. Beyond the Visible: A Survey on Cross-spectral Face Recognition. arXiv:2201.04435 [cs]

[5] Leonidas Anthopoulos. 2017. Smart utopia VS smart reality: Learning by experience from 10 smart city cases. *Cities* 63 (2017), 128–148. https://doi.org/10.1016/j.cities.2016.10.005

[6] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 2, 2 (2018), 1–23.

[7] Rani Baghezza, Kévin Bouchard, Abdenour Bouzouane, and Charles Gouin-Vallerand. 2022. Profile Recognition for Accessibility and Inclusivity in Smart Cities Using a Thermal Imaging Sensor in an Embedded System. *IEEE Internet of Things Journal* 9, 10 (May 2022), 7491–7509. https://doi.org/10.1109/JIOT.2021.3127137

[8] David Jonathan Brooks. 2005. Is CCTV a social benefit? A psychometric study of perceived social risk. *Security Journal* 18, 2 (2005), 19–29.

[9] Yangjie Cao, Zhiyi Zhou, Chenxi Zhu, Pengsong Duan, Xianfu Chen, and Jie Li. 2021. A Lightweight Deep Learning Algorithm for WiFi-Based Identity Recognition. *IEEE Internet of Things Journal* 8, 24 (Dec. 2021), 17449–17459. https://doi.org/10.1109/JIOT.2021.3078782

[10] Hanqing Chao, Yiwei He, Junping Zhang, and Jianfeng Feng. 2019. GaitSet: Regarding Gait as a Set for Cross-View Gait Recognition. In *Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence and Thirty-First Innovative Applications of Artificial Intelligence Conference and Ninth AAAI Symposium on Educational Advances in Artificial Intelligence (AAAI'19/IAAI'19/EAAI'19, Vol. 33)*. AAAI Press, Honolulu, Hawaii, USA, 8126–8133.

[11] Andrew Tzer-Yeu Chen, Morteza Biglari-Abhari, I Kevin, and Kai Wang. 2018. Context is king: Privacy perceptions of camera-based surveillance. In *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 1–6.

[12] Yuwei Cheng and Yimin Liu. 2022. Person Reidentification Based on Automotive Radar Point Clouds. *IEEE Transactions on Geoscience and Remote Sensing* 60 (2022), 1–13. https://doi.org/10.1109/TGRS.2021.3073664

[13] Hafedh Chourabi, Taewoo Nam, Shawn Walker, J Ramon Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A Pardo, and Hans Jochen Scholl. 2012. Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences*. IEEE, 2289–2297.

[14] Jacob Cohen. 1960. A coefficient of agreement for nominal scales. *Educational and psychological measurement* 20, 1 (1960), 37–46.

[15] Enrico Collini, Luciano Alessandro Ipsaro Palesi, Paolo Nesi, Gianni Pantaleo, and William Zhao. 2024. Flexible Thermal Camera Solution for Smart City People Detection and Counting. *Multimedia Tools and Applications* 83, 7 (Feb. 2024), 20457–20485. https://doi.org/10.1007/s11042-023-16374-x

[16] Antitza Dantcheva, Petros Elia, and Arun Ross. 2016. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security* 11, 3 (March 2016), 441–467. https://doi.org/10.1109/TIFS.2015.2480381

[17] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. Unique in the Crowd: The Privacy Bounds of Human Mobility. *Scientific Reports* 3, 1 (March 2013), 1376. https://doi.org/10.1038/srep01376

[18] Deutsche Bahn. 2021. Security on trains and in stations. https://ibir.deutschebahn.com/2021/en/sustainability/governance/group-security/security-on-trains-and-in-stations/. States plan for ~11,000 station cameras by end of 2024.

[19] Pardis Emami-Naeini, Joseph Breda, Wei Dai, Tadayoshi Kohno, Kim Laine, Shwetak Patel, and Franziska Roesner. 2023. Understanding People's Concerns and Attitudes Toward Smart Cities. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 71, 24 pages. https://doi.org/10.1145/3544548.3581558

[20] Chao Fan, Saihui Hou, Junhao Liang, Chuanfu Shen, Jingzhe Ma, Dongyang Jin, Yongzhen Huang, and Shiqi Yu. 2025. OpenGait: A Comprehensive Benchmark Study for Gait Recognition Towards Better Practicality. *IEEE Transactions on Pattern Analysis and Machine Intelligence* (2025), 1–18. https://doi.org/10.1109/TPAMI.2025.3576283

[21] Chao Fan, Junhao Liang, Chuanfu Shen, Saihui Hou, Yongzhen Huang, and Shiqi Yu. 2023. OpenGait: Revisiting Gait Recognition Toward Better Practicality. In *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Vancouver, BC, Canada, 9707–9716. https://doi.org/10.1109/CVPR52729.2023.00936

[22] Chao Fan, Yunjie Peng, Chunshui Cao, Xu Liu, Saihui Hou, Jiannan Chi, Yongzhen Huang, Qing Li, and Zhiqiang He. 2020. GaitPart: Temporal Part-Based Model for Gait Recognition. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Seattle, WA, USA, 14213–14221. https://doi.org/10.1109/CVPR42600.2020.01423

[23] Teri Figueroa. 2020. *Mayor orders San Diego's Smart Streetlights turned off until surveillance ordinance in place.* The San Diego Union-Tribune. https://www.sandiegouniontribune.com/news/public-safety/story/2020-09-09/mayor-orders-san-diegos-smart-streetlights-turned-off-until-surveillance-ordinance-in-place Accessed: 2026-02-28.

[24] Matt Franchi, Hauke Sandhaus, Madiha Zahrah Choksi, Severin Engelmann, Wendy Ju, and Helen Nissenbaum. 2025. Privacy of Groups in Dense Street Imagery. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*. 2874–2891.

[25] Cinthya Celina Tamayo Gonzalez, Simone Soderi, Julian Todt, Thorsten Strufe, and Mauro Conti. 2025. Inferring Personal Attributes with a Mmwave Radar. In *2025 IEEE Wireless Communications and Networking Conference (WCNC)*. 1–6. https://doi.org/10.1109/WCNC61545.2025.10978264

[26] Ben Greiner. 2015. Subject pool recruitment procedures: organizing experiments with ORSEE. *Journal of the Economic Science Association* 1 (07 2015), 114–125. https://doi.org/10.1007/s40881-015-0004-4

[27] Gerhard P. Hancke, Bruno De Carvalho e Silva, and Gerhard P. Hancke, Jr. 2013. The Role of Advanced Sensing in Smart Cities. *Sensors* 13, 1 (2013), 393–425. https://doi.org/10.3390/s130100393

[28] Simon Hanisch, Patricia Arias-Cabarcos, Javier Parra-Arnau, and Thorsten Strufe. 2025. Anonymization techniques for behavioral biometric data: a survey. *Comput. Surveys* 57, 11 (2025), 1–54.

[29] Simon Hanisch, Evelyn Muschter, Admantini Hatzipanayioti, Shu-Chen Li, and Thorsten Strufe. 2023. Understanding Person Identification Through Gait. *Proceedings on Privacy Enhancing Technologies* (2023).

[30] Albert Haque, Alexandre Alahi, and Li Fei-Fei. 2016. Recurrent Attention Models for Depth-Based Person Identification. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Las Vegas, NV, USA, 1229–1238. https://doi.org/10.1109/CVPR.2016.138

[31] Khandaker Foysal Haque, Milin Zhang, Francesca Meneghello, and Francesco Restuccia. 2025. BeamSense: Rethinking Wireless Sensing with MU-MIMO Wi-Fi Beamforming Feedback. *Computer Networks* 258 (Feb. 2025), 111020. https://doi.org/10.1016/j.comnet.2024.111020

[32] Colin Harrison, Barbara Eckman, Rick Hamilton, Perry Hartswick, Jayant Kalagnanam, Jurij Paraszczak, and Peter Williams. 2010. Foundations for smarter cities. *IBM Journal of research and development* 54, 4 (2010), 1–16.

[33] Andrew J. Hawkins. 2020. *Alphabet's Sidewalk Labs shuts down Toronto smart city project.* The Verge. https://www.theverge.com/2020/5/7/21250594/alphabet-sidewalk-labs-toronto-quayside-shutting-down Accessed: 2026-02-28.

[34] Milton Heumann, Lance Cassak, Esther Kang, and Thomas Twitchell. 2016. Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace. *Rutgers JL & Pub. Pol'y* 14 (2016), 37.

[35] International Union of Railways (UIC). 2020. RAILsilience — How the rail sector fought Covid-19 during lockdowns. https://uic.org/IMG/pdf/railsilience__how_the_rail_sector_fought_covid-19_during_lockdowns.pdf.

[36] Emiram Kablo, Melina Kleber, and Patricia Arias Cabarcos. 2025. {PrivaCI} in {VR}: Exploring Perceptions and Acceptability of Data Sharing in Virtual Reality Through Contextual Integrity. In *34th USENIX Security Symposium (USENIX Security 25)*. 1531–1548.

[37] Wonjin Kim, Yanggon Kim, and Ki Yong Lee. 2020. Human Gait Recognition Based on Integrated Gait Features Using Kinect Depth Cameras. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. 328–333. https://doi.org/10.1109/COMPSAC48688.2020.0-225

[38] Sabrina Klivan, Sandra Höltervennhoff, Rebecca Panskus, Karola Marky, and Sascha Fahl. 2024. Everyone for themselves? a qualitative study about individual security setups of open source software contributors. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1065–1082.

[39] Xiangbo Kong, Zelin Meng, Lin Meng, and Hiroyuki Tomiyama. 2018. A privacy protected fall detection IoT system for elderly persons using depth camera. In *2018 International Conference on Advanced Mechatronic Systems (ICAMechS)*. IEEE,

31–35.

[40] M. S. Naresh Kumar and R. Venkatesh Babu. 2012. Human Gait Recognition Using Depth Camera: A Covariance Based Approach. In *Proceedings of the Eighth Indian Conference on Computer Vision, Graphics and Image Processing*. ACM, Mumbai India, 1–6. https://doi.org/10.1145/2425333.2425353

[41] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding People's Attitude and Concerns towards Adopting IoT Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 307, 10 pages. https://doi.org/10.1145/3411763.3451633

[42] Chenning Li, Zhichao Cao, and Yunhao Liu. 2022. Deep AI Enabled Ubiquitous Wireless Sensing: A Survey. *Comput. Surveys* 54, 2 (March 2022), 1–35. https://doi.org/10.1145/3436729

[43] Kung-Yee Liang and Scott L Zeger. 1986. Longitudinal data analysis using generalized linear models. *Biometrika* 73, 1 (1986), 13–22.

[44] Naomi Lintvedt. 2023. Thermal Imaging in Robotics as a Privacy-Enhancing or Privacy-Invasive Measure? Misconceptions of Privacy When Using Thermal Cameras in Robots. *Digital Society* 2, 3 (Sept. 2023), 33. https://doi.org/10.1007/s44206-023-00060-4

[45] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2020. WiFi Sensing with Channel State Information: A Survey. *Comput. Surveys* 52, 3 (May 2020), 1–36. https://doi.org/10.1145/3310194

[46] Prianka Mandal, Tu Le, Amit Seal Ami, Yuan Tian, and Adwait Nadkarni. 2025. " Free WiFi is not ultimately free": Privacy Perceptions of Users in the US regarding City-wide WiFi Services. *Proceedings on Privacy Enhancing Technologies* (2025).

[47] Mary L McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica* 22, 3 (2012), 276–282.

[48] Zhen Meng, Song Fu, Jie Yan, Hongyuan Liang, Anfu Zhou, Shilin Zhu, Huadong Ma, Jianhua Liu, and Ning Yang. 2020. Gait Recognition for Co-Existing Multiple People Using Millimeter Wave Sensing. *Proceedings of the AAAI Conference on Artificial Intelligence* 34, 01 (April 2020), 849–856.

[49] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. Sage.

[50] Abhishek Kumar Mishra, Aline Carneiro Viana, Nadjib Achir, and Catuscia Palamidessi. 2021. Public wireless packets anonymously hurt you. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 649–652.

[51] Saraju P Mohanty, Uma Choppali, and Elias Kougianos. 2016. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE consumer electronics magazine* 5, 3 (2016), 60–70.

[52] Norma Möllers and Jens Hälterlein. 2016. Privacy issues in public discourse: The case of "smart" CCTV in Germany. In *Privacy and Security in the Digital Age*. Routledge, 57–70.

[53] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an {IoT} world. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)*. 399–412.

[54] Andreea I. Niculescu and Bimlesh Wadhwa. 2015. Smart cities in South East Asia: Singapore concepts - an HCI4D perspective. In *Proceedings of the ASEAN CHI Symposium'15* (Seoul, Republic of Korea) *(ASEAN CHI Symposium'15)*. Association for Computing Machinery, New York, NY, USA, 20–23. https://doi.org/10.1145/2776888.2780362

[55] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[56] Ricardo Osorio-Oliveros, Aurora Tijerina-Berzosa, Juan Angel Gonzalez-Aguirre, Iqui Balam Heredia Marin, Mauricio Adolfo Ramírez-Moreno, and Jorge de Jesús Lozoya-Santos. 2022. PiBOT: Design and Development of a Mobile Robotic Platform for COVID-19 Response. In *Advances in Automation and Robotics Research*, Héctor A. Moreno, Isela G. Carrera, Ricardo A. Ramírez-Mendoza, José Baca, and Ilka A. Banfield (Eds.). Springer International Publishing, Cham, 252–260.

[57] Caspar A.S. Pouw, Alessandro Corbetta, Alessandro Gabbana, Chiel van der Laan, and Federico Toschi. 2024. High-statistics pedestrian dynamics on stairways and their probabilistic fundamental diagrams. *Transportation Research. Part C: Emerging Technologies* 159 (1 Feb. 2024). https://doi.org/10.1016/j.trc.2023.104468

[58] Michael Ramírez. 2021. *PiBot, the multifunctional robot developed on the Tec*. Transfer Tec. https://transferencia.tec.mx/2021/06/24/pibot-el-robot-multifuncional-desarrollado-en-el-tec/ Accessed: 2026-05-06.

[59] Mauricio A. Ramírez-Moreno, Sajjad Keshtkar, Diego A. Padilla-Reyes, Edrick Ramos-López, Moisés García-Martínez, Mónica C. Hernández-Luna, Antonio E. Mogro, Jurgen Mahlknecht, José Ignacio Huertas, Rodrigo E. Peimbert-García, Ricardo A. Ramírez-Mendoza, Agostino M. Mangini, Michele Roccotelli, Blas L. Pérez-Henríquez, Subhas C. Mukhopadhyay, and Jorge de Jesús Lozoya-Santos. 2021. Sensors for Sustainable Smart Cities: A Review. *Applied Sciences* 11, 17 (2021). https://doi.org/10.3390/app11178198

[60] Elissa M Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. 2017. A summary of survey methodology best practices for security and privacy researchers. (2017).

[61] Linn Robertsson, Boyko Iliev, Rainer Palm, and Peter Wide. 2007. Perception modeling for human-like artificial sensor systems. *International Journal of Human-Computer Studies* 65, 5 (2007), 446–459.

[62] Lipsarani Sahoo, Nazmus Sakib Miazi, Mohamed Shehab, Florian Alt, and Yomna Abdelrahman. 2022. You know too much: Investigating users' perceptions and privacy concerns towards thermal imaging. In *Privacy Symposium: Data Protection Law International Convergence and Compliance with Innovative Technologies*. Springer, 207–229.

[63] Alireza Sepas-Moghaddam and Ali Etemad. 2023. Deep Gait Recognition: A Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45, 1 (Jan. 2023), 264–284. https://doi.org/10.1109/TPAMI.2022.3151865

[64] Chuanfu Shen, Fan Chao, Wei Wu, Rui Wang, George Q. Huang, and Shiqi Yu. 2023. LidarGait: Benchmarking 3D Gait Recognition with Point Clouds. In *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, Vancouver, BC, Canada, 1054–1063. https://doi.org/10.1109/cvpr52729.2023.00108

[65] Chuanfu Shen, Rui Wang, Lixin Duan, and Shiqi Yu. 2025. LidarGait++: Learning Local Features and Size Awareness from LiDAR Point Clouds for 3D Gait Recognition. In *2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. 6627–6636. https://doi.org/10.1109/CVPR52734.2025.00621

[66] Chuanfu Shen, Shiqi Yu, Jilong Wang, George Q. Huang, and Liang Wang. 2025. A Comprehensive Survey on Deep Gait Recognition: Algorithms, Datasets, and Challenges. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 7, 2 (April 2025), 270–292. https://doi.org/10.1109/TBIOM.2024.3486345

[67] Kohei Shiraga, Yasushi Makihara, Daigo Muramatsu, Tomio Echigo, and Yasushi Yagi. 2016. GEINet: View-invariant Gait Recognition Using a Convolutional Neural Network. In *2016 International Conference on Biometrics (ICB)*. 1–8. https://doi.org/10.1109/ICB.2016.7550060

[68] Akash Deep Singh, Sandeep Singh Sandha, Luis Garcia, and Mani Srivastava. 2019. RadHAR: Human Activity Recognition from Point Clouds Generated through a Millimeter-wave Radar. In *Proceedings of the 3rd ACM Workshop on Millimeter-wave Networks and Sensing Systems (mmNets '19)*. Association for Computing Machinery, New York, NY, USA, 51–56. https://doi.org/10.1145/3349624.3356768

[69] Jan Slemenšek, Iztok Fister, Jelka Geršak, Božidar Bratina, Vesna Marija van Midden, Zvezdan Pirtošek, Riko Šafarič, Jan Slemenšek, Iztok Fister, Jelka Geršak, Božidar Bratina, Vesna Marija van Midden, Zvezdan Pirtošek, and Riko Šafarič. 2023. Human Gait Activity Recognition Machine Learning Methods. *Sensors* 23, 2 (Jan. 2023). https://doi.org/10.3390/s23020745

[70] Erik Stone and Marjorie Skubic. 2011. Evaluation of an Inexpensive Depth Camera for In-Home Gait Assessment. *Journal of Ambient Intelligence and Smart Environments* 3, 4 (2011), 349–361. https://doi.org/10.3233/AIS-2011-0124

[71] Daoliang Tan, Kaiqi Huang, Shiqi Yu, and Tieniu Tan. 2006. Efficient Night Gait Recognition Based on Template Matching. In *Proceedings of the 18th International Conference on Pattern Recognition - Volume 03 (ICPR '06)*. IEEE Computer Society, USA, 1000–1003. https://doi.org/10.1109/ICPR.2006.478

[72] Emmeline Taylor. 2010. I spy with my little eye: The use of CCTV in schools and the impact on privacy. *The Sociological Review* 58, 3 (2010), 381–405.

[73] Julian Todt, Felix Morsbach, and Thorsten Strufe. 2025. BFId: Identity Inference Attacks Utilizing Beamforming Feedback Information. In *Proceedings of 32nd ACM SIGSAC Conference on Computer and Communications Security (CCS '25), Taipei, October 13–17, 2025* (2025 ed.). Association for Computing Machinery (ACM). https://doi.org/10.1145/3719027.3765062

[74] Valentín Barral Vales, Tomás Domínguez-Bolaño, Carlos J. Escudero, and José A. García-Naya. 2024. An IoT System for Smart Building Combining Multiple mmWave FMCW Radars Applied to People Counting. *IEEE Internet of Things Journal* 11, 21 (Nov. 2024), 35306–35316. https://doi.org/10.1109/JIOT.2024.3434707

[75] Changsheng Wan, Li Wang, and Vir V. Phoha (Eds.). 2019. A Survey on Gait Recognition. *Comput. Surveys* 51, 5 (Sept. 2019), 1–35. https://doi.org/10.1145/3230633

[76] Dazhuo Wang, Jianfei Yang, Wei Cui, Lihua Xie, and Sumei Sun. 2022. CAUTION: A Robust WiFi-Based Human Authentication System via Few-Shot Open-Set Recognition. *IEEE Internet of Things Journal* 9, 18 (Sept. 2022), 17323–17333. https://doi.org/10.1109/JIOT.2022.3156099

[77] Fei Wang, Jinsong Han, Shiyuan Zhang, Xu He, and Dong Huang. 2018. Csi-net: Unified human body characterization and pose recognition.

[78] Mei Wang and Weihong Deng. 2021. Deep face recognition: A survey. *Neurocomputing* 429 (2021), 215–244.

[79] Yanxi Wang, Zhigang Chang, Chen Wu, Zihao Cheng, and Hongmin Gao. 2024. SpheriGait: Enriching Spatial Representation via Spherical Projection for LiDAR-based Gait Recognition. https://doi.org/10.48550/arXiv.2409.11869 arXiv:2409.11869 [cs]

[80] Yichao Wang, Yili Ren, Yingying Chen, and Jie Yang. 2023. Wi-Mesh: A WiFi Vision-Based Approach for 3D Human Mesh Construction. In *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems* (Boston, Massachusetts) *(SenSys '22)*. Association for Computing Machinery, New York, NY, USA, 362–376. https://doi.org/10.1145/3560905.3568536

[81] Yichao Wang and Jie Yang. 2022. 3D Human Mesh Construction Leveraging Wi-Fi. *ArXiv* abs/2210.10957 (2022). https://api.semanticscholar.org/CorpusID:

253018683
[82] Brandon C Welsh and David P Farrington. 2009. Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice quarterly* 26, 4 (2009), 716–745.
[83] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2 (2015), 463–476.
[84] Maximiliane Windl, Omer Akgul, Nathan Malkin, and Lorrie Faith Cranor. 2025. Privacy Solution or Menace? Investigating Perceptions of {Radio-Frequency} Sensing. In *34th USENIX Security Symposium (USENIX Security 25)*. 6045–6064.
[85] Chunjing Xiao, Daojun Han, Yongsen Ma, and Zhiguang Qin. 2019. CsiGAN: Robust Channel State Information-Based Activity Recognition With GANs. *IEEE Internet of Things Journal* 6, 6 (Dec. 2019), 10191–10204. https://doi.org/10.1109/JIOT.2019.2936580
[86] Chunjing Xiao, Yue Lei, Yongsen Ma, Fan Zhou, and Zhiguang Qin. 2021. DeepSeg: Deep-Learning-Based Activity Segmentation Framework for Activity Recognition Using WiFi. *IEEE Internet of Things Journal* 8, 7 (April 2021), 5669–5681. https://doi.org/10.1109/JIOT.2020.3033173
[87] Zhaojun Xue, Dong Ming, Wei Song, Baikun Wan, and Shijiu Jin. 2010. Infrared Gait Recognition Based on Wavelet Transform and Support Vector Machine. *Pattern Recognition* 43, 8 (Aug. 2010), 2904–2910. https://doi.org/10.1016/j.patcog.2010.03.011
[88] Hirozumi Yamaguchi, Akihito Hiromori, and Teruo Higashino. 2018. A Human Tracking and Sensing Platform for Enabling Smart City Applications. In *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*. ACM, Varanasi India, 1–6. https://doi.org/10.1145/3170521.3170534
[89] Jianfei Yang, He Huang, Yunjiao Zhou, Xinyan Chen, Yuecong Xu, Shenghai Yuan, Han Zou, Chris Xiaoxuan Lu, and Lihua Xie. 2023. MM-Fi: Multi-Modal Non-Intrusive 4D Human Dataset for Versatile Wireless Sensing. In *Advances in Neural Information Processing Systems*, A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine (Eds.), Vol. 36. Curran Associates, Inc., 18756–18768. https://proceedings.neurips.cc/paper_files/paper/2023/file/3baf7a39d07e9f4f1e258a412df94521-Paper-Datasets_and_Benchmarks.pdf
[90] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)*. 65–80.
[91] Yunze Zeng, Parth H. Pathak, and Prasant Mohapatra. 2016. WiWho: WiFi-Based Person Identification in Smart Spaces. In *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, Vienna, 1–12. https://doi.org/10.1109/IPSN.2016.7460727
[92] Shikun Zhang, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh. 2021. "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).
[93] Peijun Zhao, Chris Xiaoxuan Lu, Jianan Wang, Changhao Chen, Wei Wang, Niki Trigoni, and Andrew Markham. 2019. mID: Tracking and Identifying People with Millimeter Wave Radar. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, Santorini Island, Greece, 33–40. https://doi.org/10.1109/DCOSS.2019.00028
[94] Jinkai Zheng, Xinchen Liu, Wu Liu, Lingxiao He, Chenggang Yan, and Tao Mei. 2022. Gait Recognition in the Wild with Dense 3D Representations and A Benchmark. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, New Orleans, LA, USA, 20196–20205. https://doi.org/10.1109/cvpr52688.2022.01959
[95] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–20.
[96] Nils Zurawski. 2007. Video surveillance and everyday life: assessments of closed-circuit television and the cartography of socio-spatial imaginations. *International Criminal Justice Review* 17, 4 (2007), 269–288.

A Survey Instrument

This section contains the full survey that we used in our experiment. The original survey was in German. We first include the consent form, then the pre-questionnaire and finally the post-questionnaire.

A.1 Consent Form

Information: Thank you for participating in this study on privacy in smart cities. In this study, we are investigating what private information can be obtained about recorded individuals using sensors that will be found in a smart city, and how this sensor data can be anonymized. The sensors include video cameras, depth cameras, thermal imaging cameras, Wi-Fi routers, LiDAR and mmWave radar. You may participate in this study if you are above 18 years old and able to walk. The study consists of a series of exercises and an introductory questionnaire.
Participation in this study lasts approximately 60 minutes.

Procedure and Participation: If you decide to participate, we will first ask you to answer some general questions about yourself, such as your age and gender. We will then ask you to complete several short exercises within the sensors' recording range. This includes walking sequences with multiple repetitions. The potential risks for participants in this study are those associated with walking, such as mild fatigue or falls. The long-term benefit of this study for you is that better anonymization techniques for sensor data may help you to conceal your identity in the future.
Participation in this study is voluntary, and you are free to withdraw from the study at any time. You also have the option to withdraw your consent to the data already collected and request its deletion at any time.

Data Collection and Processing: The study is pseudonymous, which means that your data will only be associated with a random but fixed pseudonym and not with your real name. The purpose of collecting socio-demographic and physiological data is to be able to derive these characteristics from the sensor data. No attempt will be made to draw conclusions about personal characteristics other than those explicitly collected.
The evaluation results are generally only published in anonymized form (in tables and/or graphics), so that no conclusions can be drawn about individuals. For the sole purpose of investigating the privacy of human movements, your collected data may be made available to other scientists in pseudonymous form, provided you have explicitly consented to this.

□ I have read the participant information and privacy policy for participation in the privacy in smart cities study and consent to participate and the associated data processing. My consent also explicitly refers to the fact that biometric data about me and information about my ethnic background will be revealed in the study. I am aware that the consent is voluntary and can be refused without disadvantage or withdrawn at any time without giving reasons. I know that in the case of withdrawal, the lawfulness of the processing carried out on the basis of the consent until withdrawal remains unaffected. I understand that I can simply reach out to the contact person named in the participant information and privacy policy to withdraw my consent.

In addition to your consent to participate in the study, you can also declare your consent to the processing listed below by ticking the box. However, you can also participate in the study independently of this.
□ Optionally, I also explicitly consent that – for the sole purpose of investigating the privacy of human movements – my collected data may be made available to other scientists in pseudonymous form.

A.2 Study Questionnaire Part 1

Note: The following study questionnaire (see A.2 and A.3) is an English translation of the original German survey.

A.2.1 Start.

Q0 Your participant ID:
(Free text)

Q1 What sensors/devices do you think collect information about you in a city's public spaces? Before answering, it may be helpful to think about what you do in a day in the city. Name all the sensors/devices you can think of.
(Free text)

A.2.2 Privacy Perception (1).

Q2 Please indicate what information about you, you think, can be determined using the following sensors/devices:
Depth cameras are sensors that measure distances between points in the scene and the sensor and generate 2D images from this data.
Thermal imaging camera are sensors that measure light in the infrared range and use it to create images.

	Gender	Age	Hair color	Skin color	Origin	Identity
Video camera	□	□	□	□	□	□
Depth camera	□	□	□	□	□	□
Thermal imaging camera	□	□	□	□	□	□

A.2.3 Privacy concerns (1). Questions Q3-Q6 were repeated for each sensor/device in Q2

Scenario: Imagine you are in a public area and you see a [sensor/device] collecting information about you.

Q3 How concerned are you about the data collection scenario described?
(Answer choices: ○ Extremely concerned ○ Somewhat concerned ○ Moderately concerned ○ Slightly concerned ○ Not at all concerned ○ I don't know)

Q4 *If Q3 was answered with "Extremely/Somewhat/Moderately or Slightly concerned":* What exactly concerns you about the data collection scenario described?
(Free text)

Q5 *If Q3 was answered with "Not at all concerned":* What exactly about the data collection scenario described does not concern you at all?
(Free text)

Q6 *If Q3 was answered with "I don't know":* Why don't you know how concerned you are about the data collection scenario described?
(Free text)

A.2.4 Privacy Perception (2).

Q7 Please indicate what information about you, you think, can be determined using the following sensors/devices:
Radar (Radio Detection and Ranging) refers to detection and location methods based on the transmission and subsequent measurement of radio waves.
LiDAR (Light Detection and Ranging) is similar to radar, but uses laser beams instead of radio waves.
Wi-Fi refers to the standards for wireless data transmission in local networks.
(Free text)

	Gender	Age	Hair color	Skin color	Origin	Identity
LiDAR	□	□	□	□	□	□
Radar	□	□	□	□	□	□
Wi-Fi	□	□	□	□	□	□

A.2.5 Privacy concerns (2). Questions Q8-Q11 were repeated for each sensor/device in Q7

Scenario: Imagine you are in a public area and you see a [sensor/device] collecting information about you.

Q8 How concerned are you about the data collection scenario described?
(Answer choices: ○ Extremely concerned ○ Somewhat concerned ○ Moderately concerned ○ Slightly concerned ○ Not at all concerned ○ I don't know)

Q9 *If Q8 was answered with "Extremely/Somewhat/Moderately or Slightly concerned":* What about this described data collection scenario makes you concerned?
(Free text)

Q10 *If Q8 was answered with "Not at all concerned":* What about this described data collection scenario makes you not at all concerned?
(Free text)

Q11 *If Q8 was answered with "I don't know":* Why don't you know if you are concerned about this described data collection scenario?
(Free text)

A.2.6 Socio-demographic data.

Q12 Your age
(Number field)

Q13 Your gender
(Answer choices: ○ Female ○ Male ○ Other: (Free text))

Q18 Are you currently completing a degree or vocational training in the field of computer science or engineering, or have you already completed one, or do you work in one of these fields?
(Answer choices: ○ Yes ○ No ○ No answer)

A.3 Study Questionnaire Part 2

A.3.1 Privacy Perception.

Q19 After being recorded by these sensors/devices, please indicate again what information about you, you think, can be determined using the following sensors/devices.

	Gender	Age	Hair color	Skin color	Origin	Identity
Video camera	□	□	□	□	□	□
Depth camera	□	□	□	□	□	□
Thermal imaging camera	□	□	□	□	□	□
Radar	□	□	□	□	□	□
LiDAR	□	□	□	□	□	□
Wi-Fi	□	□	□	□	□	□

A.3.2 Privacy concerns. Questions Q20-Q21 were repeated for each sensor/device in Q19

Scenario: Imagine you are in a public area and you see a [sensor/device] collecting information about you.

Q20 How concerned are you about the data collection scenario described?

(Answer choices: ○ Extremely concerned ○ Somewhat concerned ○ Moderately concerned ○ Slightly concerned ○ Not at all concerned ○ I don't know)

Q21 *If Q20 was answered differently than Q3/Q8 regarding the same sensor/device:* Before the recording, you answered '[answer of Q3/Q8 in part 1 of the survey regarding sensor/device]'. What made you change your mind about your concern in this described data collection scenario?
(Free text)

B Additional Analyses

This section contains a demographic impact analysis, and further visualizations of our experiment's results.

B.1 Demographic Sensitivity Analyses

Table 5: Subgroup sample sizes by condition. Gender and IT categories with very small cell sizes (Other/Not Answered) were not included in the demographic analysis.

Subgroup	*Control* ***Walking***	*Treatment* ***Visualization***	Total
Female	34	31	65
Male	50	54	104
IT background: No	23	13	36
IT background: Yes	63	72	135

To assess whether demographic skew (see Table 5) influenced the quantitative results, we conducted exploratory demographic sensitivity analyses by gender and IT background[4]. These analyses were exploratory and not intended to support new demographic claims.

First, we repeated the within-condition and between-condition tests described in Section 3.3.1 within demographic strata. These tests, summarized in Tables 6, 7, and 8, showed several FDR-significant stratified *belief* results. Most reflected effects already observed in the full-sample analyses; the only additional belief signal not observed in the full sample was a control-group increase in video-origin beliefs within the IT-yes subgroup. In the gender-stratified within-subject *concerns* tests, the male subgroup reproduced the full-sample pattern. The female subgroup showed a significant increase in concern for cameras in the control condition and for thermal imaging cameras in treatment, but did not reproduce all full-sample effects; it also showed an additional treatment-group concern increase for depth cameras not observed in the general sample. The only additional subgroup-specific signal between conditions not present in the full sample was a LiDAR concern decrease in the non-IT subgroup.

Second, we fitted moderation models to test whether the effect of condition on pre–post change differed by gender or IT background. For inference beliefs, we used logistic generalized estimating equations (GEE) [43] including condition, time, subgroup, and their interaction, with repeated responses clustered by participant. No significant condition × time × subgroup interaction was observed for either gender ($p = .088$) or IT background ($p = .324$). For privacy concerns, Gaussian GEE models also showed no significant demographic moderation. The condition × time × gender interaction was not significant ($b = 0.17$, $SE = 0.13$, 95% CI $[-0.08, 0.42]$, $p = .182$), nor was the condition × time × IT-background interaction ($b = -0.05$, $SE = 0.14$, 95% CI $[-0.33, 0.23]$, $p = .739$)

Overall, the demographic sensitivity analyses did not change the interpretation of the main results. Stratified tests showed several significant belief effects, most of which reflected patterns already observed in the full-sample analyses, and privacy-concern patterns were largely consistent with the full-sample results, with only isolated subgroup-specific deviations. Formal moderation models found no significant demographic moderation by gender or IT background, indicating that intervention effects did not differ reliably across these subgroups.

B.2 Visualizations

Figure 6 shows the number of sensors mentioned in the first question by each participant as a bar plot. Figure 7 compares the percentages for each concern level for each sensing technology before and after the intervention. Figure 8 compares the reasons that participants reported for feeling (non-)concern for each sensor. Finally, Figure 9 visualizes the changes of attitude for each sensor.

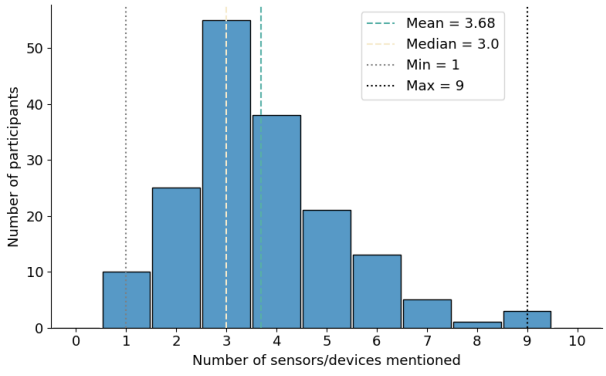


Figure 6: Distribution of the number of sensors/devices mentioned per participant. $n = 172$.

[4]Age-based analyses were not performed because age variability in our sample was limited.

Table 6: Summary of stratified sensitivity analyses. Within-subject tests repeat the main pre–post tests within each subgroup; between-condition tests compare pre–post change scores between walking and visualization conditions within each subgroup.

Analysis	Gender strata	IT-background strata
Beliefs, within-subject	Female treatment subgroup showed significant increases for thermal-camera identity and origin; no FDR-significant belief changes were observed in the male subgroup.	IT-yes subgroup broadly mirrored the full-sample pattern and showed one additional control-group increase for video-origin beliefs; IT-no subgroup showed no FDR-significant within-subject changes.
Beliefs, between-condition	Female subgroup showed a significant treatment-related increase for thermal-camera identity; male subgroup showed a significant treatment-related decrease for radar-gender beliefs.	IT-no subgroup showed a significant treatment-related increase for thermal-camera identity; IT-yes subgroup showed a significant treatment-related decrease for radar-gender beliefs.
Concerns, within-subject	Male subgroup mirrored the full-sample pattern; female subgroup partly overlapped with the full sample and showed an additional significant increase in concern for depth cameras in treatment.	IT-yes subgroup mirrored the full-sample pattern; IT-no subgroup showed no FDR-significant within-subject changes.
Concerns, between-condition	Decreased concern for radar was significant in the male subgroup, consistent with the full-sample pattern.	Radar concern decrease was significant in the IT-no subgroup; LiDAR concern decrease in this subgroup was the only additional signal not present in the full sample.

Table 7: FDR-significant ($p < .05$) stratified inference-belief results. Within-subject rows report subgroup-specific pre–post changes tested with McNemar tests. Between-condition rows report subgroup-specific comparisons of pre–post change scores between walking (control) and visualization (treatment) conditions, tested with Mann–Whitney U tests.

Stratification	Stratum	Sensor–attribute	Group / Comparison	p
Within-subject pre–post changes				
Gender	Female	Thermal–Identity	Treatment	.002
	Female	Thermal–Origin	Treatment	.044
IT background	IT-yes	Depth–Age	Control	.028
	IT-yes	Depth–Identity	Control	.028
	IT-yes	**Video–Origin**	**Control**	**.028**
	IT-yes	Thermal–Identity	Control	.028
	IT-yes	Thermal–Identity	Treatment	.001
	IT-yes	Video–Origin	Treatment	.013
	IT-yes	Thermal–Age	Treatment	.013
	IT-yes	Thermal–Origin	Treatment	.026
Between-condition change-score comparisons				
Gender	Female	Thermal–Identity	Control vs. Treatment	.001
	Male	Radar–Gender	Control vs. Treatment	.019
IT background	IT-no	Thermal–Identity	Control vs. Treatment	.026
	IT-yes	Radar–Gender	Control vs. Treatment	.039

Note. Bold entries indicate subgroup-specific signals not observed in the full-sample analyses.

Table 8: FDR-significant ($p < .05$) stratified privacy-concern results. Within-subject rows report pre- and post-intervention average concern (M) within each subgroup and condition, tested with Wilcoxon signed-rank tests. Between-condition rows report pre–post change scores (Δ) compared between walking (control) and visualization (treatment) conditions, tested with Mann–Whitney U tests. Higher values indicate higher privacy concern, measured on a 5-point scale from not at all to extremely concerned.

Stratification	Stratum	Sensor	Group / Comparison	n	Pre M / Δ_C	Post M / Δ_T	p
Within-subject pre–post changes							
Gender	Male	Camera	Control	50	2.82	3.14 ↑	.027
	Male	Camera	Treatment	53	2.55	2.92 ↑	.011
	Male	Thermal	Control	49	2.16	2.43 ↑	.018
	Male	Thermal	Treatment	53	2.13	2.47 ↑	.015
	Male	Radar	Treatment	50	1.60	1.28 ↓	.015
	Female	Camera	Control	34	2.44	2.74 ↑	.045
	Female	**Depth**	**Treatment**	**29**	**1.83**	**2.21 ↑**	**.048**
	Female	Thermal	Treatment	30	2.03	2.57 ↑	.048
IT background	IT-yes	Camera	Control	63	2.78	3.13 ↑	.003
	IT-yes	Camera	Treatment	71	2.48	2.80 ↑	.004
	IT-yes	Thermal	Control	62	1.92	2.16 ↑	.003
	IT-yes	Thermal	Treatment	70	2.04	2.46 ↑	.004
	IT-yes	Radar	Treatment	66	1.58	1.30 ↓	.009
Between-condition change-score comparisons							
Gender	Male	Radar	Control vs. Treatment	–	$\Delta_C = +0.17$	$\Delta_T = -0.32$ ↓	.013
IT background	**IT-no**	**LiDAR**	**Control vs. Treatment**	**–**	$\Delta_C = +0.07$	$\Delta_T = -0.71$ ↓	**.014**
	IT-no	Radar	Control vs. Treatment	–	$\Delta_C = -0.05$	$\Delta_T = -0.67$ ↓	.025

Note. Bold entries indicate subgroup-specific signals not observed in the full-sample analyses.

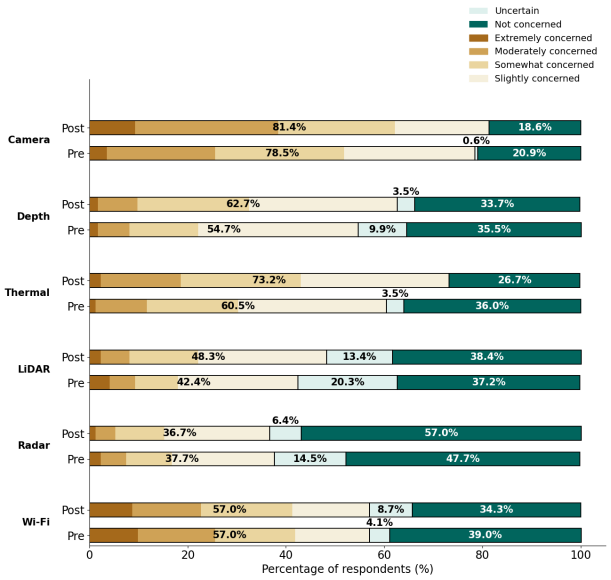


Figure 7: Percentages of participants showing concern levels before and after the intervention for each sensor type. $n = 172$**.**

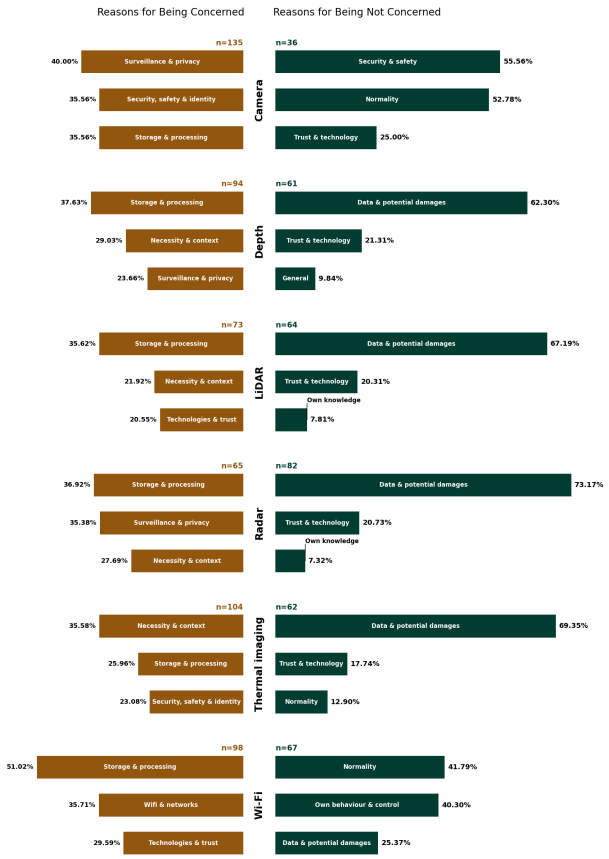
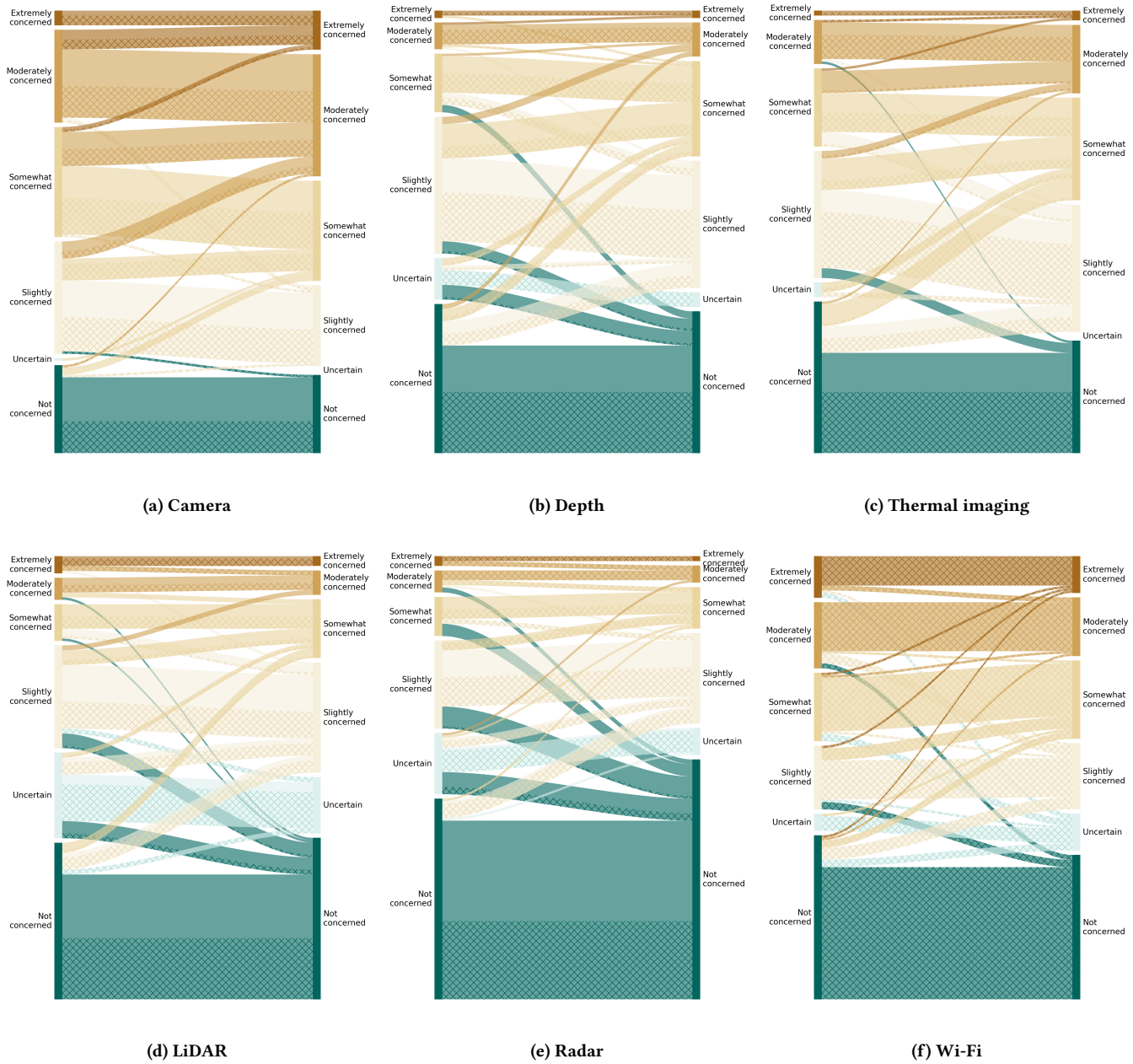


Figure 8: Reasons for concerns and non-concerns for each sensor.



(a) Camera (b) Depth (c) Thermal imaging

(d) LiDAR (e) Radar (f) Wi-Fi

Figure 9: Pre- and Post-Intervention Concern Levels for each sensor, control group hatched, treatment group unhatched.

C Complete Codebook

This section contains the entire codebook used for the qualitative analysis of our experiment.

Table 9: Codebook to question Q1 which contains categories and codes used to code free text answers. Kappa: 0.79. n = 172. Percentages in parentheses indicate the proportion of participants (out of the total) who referred to that category. The number in parentheses next to each code represents its absolute frequency.

What sensors/devices do you think collect information about you in a city's public spaces?	
Categories	**Codes**
Sensors and detection technologies (98.84%)	surveillance camera (121), camera (44), motion sensors (27), thermal imaging camera (18), anti theft sensors (12), light barriers (8), speed sensors (8), LiDAR (8), radar (6), detectors (5), infrared (4), ultrasonic sensors (3), magnetic sensors (3), sensors for (self-driving) cars (3), RGB sensor camera (2), general sensors/scanners (2), door opener sensors (2), optical sensors (1), radiation sensors (1), meta detectors (1)
Communication and networking technologies (45.93%)	Wi-Fi (71), mobile network (31), Bluetooth (9), social media (1)
Payment systems and transaction devices (39.53%)	card readers (53), checkouts (13), atm (7), vending machine (1), mensa card (1)
Mobile and portable devices (25.00%)	smartphone (42), smartwatch (5), laptop (3), tablet (1)
Traffic and security infrastructure (18.6%)	traffic cameras/sensors (21), traffic light sensors (6), parking (garages) (4), dashcams (1), gatekeeper data (1)
Identification and access technologies (19.9%)	ticket device (16), turnstiles (8), chip ID (8), RFID (3), NFC (3), face recognition (1), biometric data (1)
Location and movement data (15.7%)	location (22), satellite (3), rental transport devices (3)
Audio (6.12%)	microphone (12)
Software and services (5.81%)	apps (5), coffee machine (1)

Table 10: Codebook for question Q4/Q9 which contains categories and codes used to code free text answers. Kappa: 0.71. The question was asked to 172 participants for each type of sensor: Video camera (n = 135), Depth camera (n = 94), LiDAR (n = 73), Radar (n = 65), Thermal imaging camera (n = 104), Wi-Fi (n = 98). Percentages in first row indicate the proportion of participants for each sensor type (out of the total) who referred to that category. The numbers in the following rows refer to each code represents its absolute frequency for the type of sensor. A "+" attached to the code means that this was a reason for a non-concern.

What about this described data collection scenario makes you concerned?						
	Camera	**Depth**	**LiDAR**	**Radar**	**Thermal**	**Wi-Fi**
Storage and processing	**35.56%**	**37.63%**	**35.62%**	**36.92%**	**25.96%**	**51.02%**
data processing unclear	18	14	7	10	8	7
data dissemination unclear	24	11	4	6	6	9
type of data unclear	0	6	12	6	5	7
personal data	2	2	2	2	4	24
data collection in general	6	5	5	5	6	3
data storage	7	4	0	1	2	3
lots of information	5	1	0	0	0	8
duration of data storage	2	3	0	0	1	1
continuous data collection	0	0	0	1	0	0
Surveillance and privacy	**40.00%**	**23.66%**	**17.81%**	**35.38%**	**16.35%**	**9.18%**
stay/location	8	6	9	20	1	8
observation/monitoring	23	7	1	0	7	0
tracking	11	2	3	4	3	1
protection of privacy	7	4	0	1	3	0
loss of control	5	2	0	0	2	1
lack of anonymity	2	2	1	1	2	0
changing behavior	4	1	0	0	0	0
military observation/espionage	2	0	1	1	1	0
Necessity and context	**21.48%**	**29.03%**	**21.92%**	**27.69%**	**35.58%**	**6.12%**
necessity/purpose unclear	18	24	15	17	35	5
Concern depending on the location	4	2	0	0	2	0
helpful+	3	1	1	0	1	0
scenario-dependent	1	0	0	1	1	1
concern depending on the recipient	2	1	0	0	0	0
without any purpose of security/safety	2	0	0	0	0	0
concern depending on the data	1	0	0	0	0	0
concern independent of camera	1	0	0	0	0	0
Security, safety and identity	**35.56%**	**13.98%**	**19.18%**	**13.85%**	**23.08%**	**21.43%**
identification	28	10	5	3	6	9
safety+	23	3	0	2	3	0
no identification+	0	0	7	4	7	1
profile	2	1	1	1	1	3
presence of people	1	1	1	2	2	1
record bank details	0	0	0	0	0	6
record passwords	0	0	0	0	0	4
classification	0	0	0	0	5	0
origin	2	0	0	0	2	0
non-obvious data	2	0	0	0	0	0
less safety through cameras	0	0	1	0	0	0
Data collection attitudes	**11.85%**	**10.75%**	**12.33%**	**12.31%**	**9.62%**	**17.35%**
acceptance	5	2	0	0	2	9
unusual	0	2	2	4	5	0
without consent	3	2	1	2	2	2
general problem	3	1	3	0	0	2
fear	2	0	2	1	0	1
unaware of data collection	1	2	0	1	1	1
generally concerned	2	1	1	0	0	0
avoidance	0	0	0	0	0	3

	Camera	Depth	LiDAR	Radar	Thermal	Wi-Fi
Physiological and physical features	**19.26%**	**8.60%**	**8.22%**	**10.77%**	**17.31%**	**1.02%**
movements	12	2	2	6	4	0
action/habits	13	1	0	2	1	1
body characteristics/proportion/temperature	0	1	2	0	8	0
appearance	4	0	0	1	2	0
health status/data	0	0	1	0	6	0
facial expression/reaction	3	2	1	0	0	0
objects	0	0	0	1	3	0
biometric data	0	3	0	0	0	0
distances	0	1	1	0	0	0
shapes and structures	0	0	1	0	0	0
Technologies and trust	**2.96%**	**7.53%**	**20.55%**	**7.69%**	**1.92%**	**29.59%**
not enough knowledge about technology	0	6	11	5	2	2
device can be hacked	0	0	0	0	0	17
fear of data loss on smartphone	2	0	1	0	0	9
3d models	0	1	2	0	0	0
algorithms for data collection	2	0	0	0	0	0
ai	0	1	0	0	0	1
gdpr is protecting+	0	0	1	0	0	0
data from smartphone	0	0	0	0	0	0
Comparison of technologies	**5.93%**	**13.98%**	**10.96%**	**7.69%**	**7.69%**	**1.02%**
depth less data recording	0	9	0	0	0	0
camera collects more than other tech	7	0	0	0	0	0
thermal less data recording	0	0	0	0	5	0
radar similar to LiDAR	0	0	4	1	0	0
depth same as other cameras	1	3	0	0	0	0
LiDAR more data than radar	0	0	3	1	0	0
radar less concerned	0	0	0	3	0	0
mix monitoring	0	0	0	0	1	0
thermal as depth	0	0	0	0	2	0
depth more than video	0	1	0	0	0	0
LiDAR less observed	0	0	1	0	0	0
thermal more data than depth	0	0	0	0	1	0
Wi-Fi less observed	0	0	0	0	0	1
Abuse and risks	**13.33%**	**4.30%**	**2.74%**	**4.62%**	**5.77%**	**5.10%**
data misuse	13	1	1	0	2	3
data collection used against one	3	2	1	2	5	0
fraud/deep fakes	2	1	1	0	0	2
manipulation/extortion	1	0	0	0	1	0
radiation endangers health	0	0	0	1	0	0
Wi-Fi and networks	**0.00%**	**0.00%**	**0.00%**	**0.00%**	**0.00%**	**35.71%**
Wi-Fi data sensitive	0	0	0	0	0	12
online behavior	0	0	0	0	0	11
Wi-Fi use voluntary+	0	0	0	0	0	11
Wi-Fi important for citizens+	0	0	0	0	0	6
Disclosure and Use by Third Parties	**5.19%**	**4.30%**	**0.00%**	**0.00%**	**1.92%**	**2.04%**
state	4	2	0	0	1	0
company	2	2	0	0	1	0
marketing of data	2	1	0	0	0	1
data for advertising purposes	1	1	0	0	0	1

Table 11: Codebook to question Q5/Q10 which contains categories and codes used to code free text answers. Kappa: 0.7. The question was asked to 172 participants for each type of sensor: Video camera (n = 36), Depth camera (n = 61), LiDAR (n = 64), Radar (n = 82), Thermal imaging camera (n = 62), Wi-Fi (n = 67). Percentages in first row indicate the proportion of participants for each sensor type (out of the total) who referred to that category. The numbers in the following rows refer to each code represents its absolute frequency for the type of sensor.

What about this described data collection scenario makes you not at all concerned?						
	Camera	**Depth**	**LiDAR**	**Radar**	**Thermal**	**Wi-Fi**
Security and safety	**55.56%**	**8.20%**	**3.13%**	**6.10%**	**6.45%**	**0.00%**
safety	15	3	0	1	4	0
violation of the law	6	1	2	1	0	0
lower criminality	3	0	0	0	0	0
traffic	0	1	1	3	0	0
Not for tracking	1	0	0	1	0	0
Normality	**52.78%**	**6.56%**	**6.25%**	**3.66%**	**12.90%**	**41.79%**
normal/habituation	13	0	0	0	0	27
public places	8	2	0	0	0	0
indifferent	2	1	0	0	4	0
unavoidable	1	0	0	0	0	1
(more) data also collected elsewhere	2	1	4	3	4	1
Trust and technology	**25.00%**	**21.31%**	**20.31%**	**20.73%**	**17.74%**	**4.48%**
trust	5	3	0	0	4	0
research purposes	0	0	1	0	1	0
total population	0	0	1	0	0	0
advantages/spec. purpose	1	1	2	2	4	2
no difference to other technologies	0	1	0	0	1	0
positioning/measuring/location	3	7	9	15	0	1
concern only in combination with other technologies	0	1	0	0	1	0
dependent on government	1	1	0	0	0	0
today's technologies concerning-	0	0	1	0	0	0
Own behaviour and control	**11.11%**	**3.28%**	**3.13%**	**3.66%**	**1.61%**	**40.30%**
own/careful behaviour	0	0	0	0	0	5
public Wi-Fi not used	0	0	0	0	0	1
public Wi-Fi voluntary	0	0	0	0	0	14
advantages of public Wi-Fi	0	0	0	0	0	9
nothing to hide	0	0	1	1	0	0
outside of own control	1	1	0	0	0	1
not connected	3	1	1	2	1	1
Data and potential damages	**16.67%**	**62.30%**	**67.19%**	**73.17%**	**69.35%**	**25.37%**
data does no harm	1	4	6	5	6	2
no clear data	0	5	3	8	3	1
anonymous data	0	5	0	2	4	0
not valuable data	0	2	3	2	1	4
not much personal data	0	20	24	26	12	7
head/face not recognizable	0	0	1	1	1	0
no identification possible	0	12	9	19	16	2
data about body	0	1	1	1	4	0
movement	0	1	2	1	1	1
objects	0	0	1	2	0	0
not target object	0	0	0	2	0	0

	Camera	Depth	LiDAR	Radar	Thermal	Wi-Fi
General	**0.00%**	**9.84%**	**6.25%**	**6.10%**	**11.29%**	**14.93%**
awareness	0	0	0	0	0	8
generally unconcerned	0	4	2	2	6	0
unclear	0	1	2	2	0	1
naivety	0	1	0	1	0	0
privacy not violated	0	0	0	0	1	1
Own knowledge	**0.00%**	**8.20%**	**7.81%**	**7.32%**	**8.06%**	**2.99%**
missing knowledge about technology	0	3	5	6	3	1
unaware	0	0	0	0	1	1
purpose unknown-	0	2	0	0	1	0

Table 12: Codebook to the question Q6/Q11 which contains categories and codes used to code free text answers. Kappa: 0.7. The question was asked to 172 participants for each type of sensor: Video camera ($n = 1$), Depth ($n = 17$), LiDAR ($n = 35$), Radar ($n = 25$), Thermal imaging camera ($n = 6$), Wi-Fi ($n = 7$). Percentages in first row indicate the proportion of participants for each sensor type (out of the total) who referred to that category. The numbers in the following rows refer to each code represents its absolute frequency for the type of sensor.

Why don't you know if you are concerned about this described data collection scenario?						
	Camera	**Depth**	**LiDAR**	**Radar**	**Thermal**	**Wi-Fi**
Unawareness and lack of knowledge	**0.00%**	**94.12%**	**94.29%**	**84.00%**	**83.33%**	**85.71%**
lack of knowledge about technology	0	11	19	5	1	0
type of data unclear	0	4	9	6	1	4
identification unclear	0	5	3	3	2	0
technology not recognizable	0	2	4	3	1	0
uncertainty in personal data	0	1	2	5	1	1
inferences unclear	0	0	3	3	1	0
data collector unclear	0	0	1	0	0	0
precision of data unclear	0	0	0	1	0	0
data collection generally unclear	0	0	0	0	0	1
data storage unclear	0	0	0	0	0	0
Meaning and purpose	**100.00%**	**23.53%**	**14.29%**	**8.00%**	**16.67%**	**0.00%**
purpose unclear	0	3	5	2	0	0
necessity unclear	0	1	0	0	0	0
place of action unclear	0	0	0	0	1	0
indecisive	1	0	0	0	0	0
Security, safety and privacy	**100.00%**	**5.88%**	**2.86%**	**16.00%**	**16.67%**	**42.86%**
smartphone access concerning	0	0	1	1	0	2
safety	1	0	0	1	0	0
advantages outweigh disadvantages	0	0	0	0	1	0
data in wrong hands	1	0	0	0	0	0
trust	0	0	0	0	0	1
no surveillance	0	0	0	1	0	0
no personal data involved	0	1	0	0	0	0
not the target	0	0	0	1	0	0

Table 13: Codebook for the question Q21 which contains categories and codes used to code free text answers. Kappa = 0.7. The question was asked for each type of sensor: Camera (n = 50), Depth (n = 63), LiDAR (n = 56), Radar (n = 51), Thermal (n = 66), Wi-Fi (n = 42). Percentages in first row indicate the proportion of participants for each sensor type (out of the total) who referred to that category. The numbers in the following rows refer to each code represents its absolute frequency for the type of sensor.

What made you change your mind about your concern in this described data collection scenario?											
	Camera		**Depth**		**LiDAR**		**Radar**		**Thermal**		**Wi-Fi**
	T	**C**	**T**	**C**	**T**	**C**	**T**	**C**	**T**	**C**	**C**
	23	27	43	20	32	24	28	23	47	19	42
Expectations	**56.5%**	**25.9%**	**67.4%**	**50.0%**	**56.3%**	**37.5%**	**60.7%**	**34.8%**	**63.8%**	**42.1%**	**35.71%**
Concerned											
more data than expected	6	4	12	5	8	3	1	2	24	6	6
practical experience	5	3	7	3	5	5	3	1	2	0	4
study questions	1	0	0	0	1	0	1	0	1	1	1
Unconcerned											
less data than expected	0	0	12	2	6	0	12	2	3	0	5
no danger in experiment	1	0	0	0	0	1	1	4	0	1	1
no localization possible	0	0	0	0	0	1	0	0	0	0	0
Data specifications	**34.8%**	**22.2%**	**30.2%**	**20.0%**	**40.6%**	**41.7%**	**32.1%**	**30.4%**	**25.5%**	**31.6%**	**14.3%**
Concerned											
personal information	4	3	4	0	2	1	0	0	5	1	2
motion recording	2	2	3	3	3	3	0	2	3	3	0
stature/posture recognizable	0	0	1	1	0	2	0	2	0	3	0
lots of data	0	2	2	0	1	1	0	0	0	0	0
localization possible	0	0	0	0	0	2	3	2	0	0	1
gender recognizable	1	0	3	0	0	0	0	0	1	1	0
origin recognizable	1	0	0	0	1	1	0	0	0	0	1
face features	1	1	0	0	0	0	0	0	1	0	0
age recognizable	1	0	1	0	0	0	0	0	0	1	0
body temperature readable	0	0	0	0	0	0	0	0	2	0	0
clothing recognizable	0	0	0	0	1	0	0	0	0	0	0
hair color recognizable	0	0	0	0	1	0	0	0	0	0	0
Unconcerned											
no personal data	0	0	1	0	5	1	6	2	2	1	2
no pictures as recordings	0	0	0	0	2	0	2	0	0	0	0
no data about appearance	0	0	1	0	0	0	1	0	0	0	0
face not recognizable	0	0	1	0	1	0	0	0	0	0	0
gestures not recognizable	0	0	0	0	1	0	0	0	0	0	0
Knowledge and understanding	**17.4%**	**18.5%**	**4.7%**	**15.0%**	**12.5%**	**20.8%**	**7.1%**	**8.7%**	**19.1%**	**0.0%**	**45.2%**
Concerned											
unawareness	1	1	1	1	2	4	1	0	0	0	12
recording like video camera	0	0	0	1	1	1	0	0	8	0	0
video cameras hold most data	2	4	0	0	0	0	1	0	0	0	0
dealing with topic	1	0	0	0	1	0	0	0	1	0	1
camera confusion	0	0	0	1	0	0	0	0	0	0	0
recording like thermal imaging camera	0	0	1	0	0	0	0	0	0	0	0
Unconcerned											
conscious use	0	0	0	0	0	0	0	1	0	0	6
consent	0	0	0	0	0	0	0	1	0	0	0

What made you change your mind about your concern in this described data collection scenario? (cont.)											
	Camera		**Depth**		**LiDAR**		**Radar**		**Thermal**		**Wi-Fi**
	T	**C**	**T**	**C**	**T**	**C**	**T**	**C**	**T**	**C**	**C**
	23	27	43	20	32	24	28	23	47	19	42
Identification	**26.1%**	**14.8%**	**14.0%**	**5.0%**	**12.5%**	**8.3%**	**7.1%**	**13.0%**	**21.3%**	**21.1%**	**2.4%**
Concerned											
personal identification	6	4	4	0	3	2	0	3	7	4	1
Unconcerned											
no identification	0	0	2	1	1	0	2	0	3	0	0
Feelings and emotions	**17.4%**	**40.7%**	**2.3%**	**20.0%**	**0.0%**	**25.0%**	**10.7%**	**21.7%**	**0.0%**	**21.1%**	**2.4%**
Neutral											
getting used to/acceptance	1	1	0	1	0	2	1	0	0	0	0
fear of breaking rules	0	1	0	0	0	0	0	0	0	1	0
Concerned											
feeling of observation/recording	3	6	0	3	0	4	2	5	0	3	1
Unconcerned											
safety feeling	0	3	1	0	0	0	0	0	0	0	0
Use, Purpose, Abuse	**4.3%**	**14.8%**	**2.3%**	**5.0%**	**3.1%**	**0.0%**	**3.6%**	**8.7%**	**2.1%**	**5.3%**	**16.7%**
Concerned											
data analysis concern	1	0	1	0	1	0	1	0	1	0	3
abuse of purpose	0	3	0	1	0	0	0	0	0	0	2
recording without cause	0	0	0	0	0	0	0	2	0	1	0
sharing with third parties	0	2	0	0	0	0	0	0	0	0	1
misuse by organizations	0	1	0	0	0	0	0	0	0	0	0
hacker attack	0	0	0	0	0	0	0	0	0	0	1
Surveillance	**0.0%**	**22.2%**	**2.3%**	**5.0%**	**0.0%**	**8.3%**	**0.0%**	**13.0%**	**2.1%**	**5.3%**	**2.4%**
Concerned											
continuous recording	0	3	0	1	0	1	0	1	0	1	0
record events	0	0	1	0	0	1	0	1	1	0	0
mobile phone actions	0	1	0	0	0	0	0	0	0	0	1
manipulation/control	0	1	0	0	0	0	0	0	0	0	0
no control	0	1	0	0	0	0	0	1	0	0	0
Unclear	**4.3%**	**3.7%**	**0.0%**	**5.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**2.1%**	**0.0%**	**2.4%**
Neutral											
unclear	0	1	0	1	0	0	0	0	1	0	0
study design issues	1	0	0	0	0	0	0	0	0	0	1
Privacy	**4.3%**	**3.7%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**
Concerned											
invasion of privacy	1	1	0	0	0	0	0	0	0	0	0