Between a Rock and a Hard Place: Examining Public Understanding and Perceptions of Data Practices in Smart Cities

Wejdan Alsarih
University of Bristol
Bristol, UK
wejdan.alsarih@bristol.ac.uk

Inah Omoronyia
University of Bristol
Bristol, UK
inah.omoronyia@bristol.ac.uk

Kopo M. Ramokapane
University of Bristol
Bristol, UK
marvin.ramokapane@bristol.ac.uk

Abstract

Smart cities are often presented as modern, sustainable, and efficient environments that enhance safety and convenience through advanced technologies. However, their heavy reliance on data collection raises significant privacy concerns. As technology evolves faster than public awareness, questions emerge about whether these cities adequately protect individuals' data. This study explores residents' understanding of smart cities and their perceptions of data collection and sharing. In this study, we conduct semi-structured interviews with 19 residents across two countries to examine how people conceptualise smart cities and interpret the collection, processing, and sharing of their data. Our analysis shows that residents hold fragmented and often inaccurate mental models of smart-city infrastructures; view data practices as simultaneously beneficial and risky; and lack meaningful clarity about data flows, retention, and institutional responsibility. Participants considered consent important yet mostly infeasible given the pervasive and unavoidable nature of smart-city data collection. We also identify culturally grounded differences in trust, privacy sensitivities, and expectations of governance across the two contexts. Our findings challenge assumptions embedded in current smart-city governance and consent models and point to the need for transparent, accountable, and contextually attuned data practices.

Keywords

Privacy, Smart cities, Data collection, Data sharing, Consent

1 Introduction

The growing population and urbanisation worldwide have put increasing stress on cities. By 2050, about 68% of the global population is expected to live in urban areas [16, 27]. This rapid urbanisation introduces significant challenges, including traffic congestion, increased demand on energy and water infrastructures, rising crime rates, inadequate housing, and limited social integration. These pressures have motivated growing interest in smart-city initiatives as a scalable and sustainable approach to urban management [25]. While existing literature does not converge on a single definition of smart city, we adopt a working definition drawn from Gracias et al. [28] which state that a smart city is an urban environment that uses digital technologies, communication infrastructures, and data analytics to deliver urban services more efficiently, improve quality of life, and promote sustainability. Smart cities promise to enhance the quality of life by improving public services, infrastructure, and mobility systems while also promoting sustainability, supporting industries, and strengthening local economies [55].

These ambitions rely heavily on the deployment of interconnected technologies and data-driven systems that enable continuous monitoring, seamless service delivery, and real-time decision-making across urban environments [63]. These capabilities depend on the continuous collection, integration, and processing of large volumes of data which is often highly granular and deeply intertwined with residents' everyday lives. Moreover, this data is frequently collected in ambient, always-on, and sometimes opaque ways across public and quasi-public spaces.

Consequently, smart city deployments raise pressing questions and debates around individual and collective privacy, autonomy, and the shifting power dynamics between residents, municipal authorities, and private technology vendors [15, 37, 41]. However, despite the prominence of these debates, we still know little about how the people living and working in these cities actually understand and interpret the data practices that shape these cities. Prior research highlights that urban data ecosystems are often opaque to residents [13, 14, 22, 26, 60], and others have critiqued the viability of meaningful consent in pervasive sensing environments suggesting it may be infeasible or impractical [41, 60, 65]. Moreover, prior work has also documented the limitations of existing consent models and the prevalence of dark patterns online [24, 30, 31]. However, these insights rarely extend to physical, ambient, and multi-operator data ecosystems like smart cities.

Existing work predominantly focuses on technical architectures [20, 21, 43], governance frameworks [4, 61, 64], or ethical analyses [3, 19, 53], and very little empirical evidence examines how residents conceptualise smart cities, how they think data collection and sharing occur, or how they understand consent in these environments. Moreover, there is lack of understanding of how cultural context shapes privacy expectations and perceptions of urban data collection. As smart city initiatives increasingly rely on standardised architectures and consent models, failing to account for cross-cultural variation risks designing systems that are unintentionally exclusionary, misaligned with public expectations, or incapable of supporting meaningful privacy agency across diverse populations.

To address these gaps, we conduct an exploratory semi-structured interview study with residents in Kingdom of Saudi Arabia (KSA) and United Kingdom (UK), two contexts with distinct cultural norms, political structures, and attitudes toward technology and public authority. Through this cross-contextual approach, we aimed to develop a deep understanding of how residents in these smart

Proceedings on Privacy Enhancing Technologies 2026(3), 65–83

https://doi.org/10.56553/popets-2026-0071

cities understand and perceive data collection and data sharing practices. Designing privacy-aware smart city technologies requires understanding both shared patterns and contextual variation in how residents conceptualise risk, consent, and institutional accountability. Moreover, treating privacy expectations as universal risks embedding implicit governance assumptions into technical systems, potentially leading to misalignment between security guarantees and users' threat models. Consequently, we examine their perceptions, expectations, and concerns regarding consent and data practices in smart cities. Where relevant, we highlight meaningful differences between the two contexts. To guide our investigation, we ask the following research questions:

RQ1: How do residents conceptualize and understand smart cities?
RQ2: How do residents perceive and understand the collection, processing, and sharing of data in smart-cities?
RQ3: How do residents perceive consent and control in smart cities?

Our study reveals four primary findings that challenge common assumptions about resident awareness, data practices, and consent expectations in smart cities. Residents hold incomplete and uncertain understandings of what constitutes a smart city. Participants generally described smart cities as automated, interconnected, and government-managed environments, yet many were unsure whether they currently lived in one. This indicates that residents' mental models of smart cities remain fragmented, even in cities where smart technologies are deployed. Residents described data as both an *enabler* of improved services and a *source of risk*, creating a persistent utility–privacy tension. While participants were broadly opposed to the collection of personal data, they accepted limited cases where such collection was strictly necessary for service provisioning. This tension reflects a mismatch between residents' expectations of privacy and the pervasive data demands of smart city infrastructures. Participants lacked clarity about data flows, retention, and responsibility, raising concerns around transparency and accountability in smart city systems. Consent is seen as essential but currently non-functional; they want control but doubt feasibility. Participants agreed that meaningful consent should be required, but felt that no such mechanisms currently exist in practice. They suggested various potential approaches for obtaining consent, including offline methods or one-time authorisation processes. Others wanted to be able to revoke consent but were unsure how it would work in pervasive sensing environments. This highlights the practical challenges of implementing meaningful consent in ambient urban systems. Finally, we also found that cultural differences strongly shape privacy expectations and trust in data custodians. For instance, participants in Saudi Arabia expressed concerns about data that could identify women or link family members. They were more comfortable with government-led data collection and viewed state agencies as trusted custodians. In contrast, participants in the UK were more concerned about government misuse, and expressed strong opposition to private-sector data collection and commercial exploitation. Overall, our findings highlight the importance of cultural context in designing inclusive, privacy-respecting smart city infrastructures, suggesting uniform governance models may not be inclusive.

Summary of our contributions.

- **Characterization of resident perceptions of smart city data practices.** We identify how residents understand (and misunderstand) the collection, processing, and sharing of data in ambient urban environments, uncovering where transparency issues are and accountability gaps across both cities. Our findings show consistent uncertainty across both contexts about who collects data, how it flows across systems, how long it is stored, and whether it can be deleted.
- **Empirical insights into residents' perceptions and expectations for consent in smart cities.** We show that residents view consent as essential yet infeasible within current smart city infrastructures, and we identify their conceptual barriers that make meaningful consent and revocation difficult to achieve. This insight challenges existing privacy frameworks and highlights the need for redesigned consent mechanisms in public infrastructures.
- **Cultural and political influences** We show that trust in smart-city systems is not driven by technical assurances but by sociopolitical context, centralised governance in KSA leads to high institutional trust and low concern, while fragmented governance in the UK amplifies uncertainty and discomfort. This finding highlights the importance of context-sensitive security and privacy design.

2 Background and Related Work

2.1 Smart Cities

The increasing pressures of global urbanisation and rapid technological advances have led to the emergence of smart cities as a contemporary model for urban development and societal improvement [47]. Smart cities are urban environments that integrate diverse technologies, including Information and Communication Technologies (ICT), Internet of Things (IoT) devices, Artificial Intelligence(AI), advanced analytics, and interconnected networks, to monitor and enhance urban operations through data-driven solutions [28]. These integrated digital systems enable cities to improve efficiency, sustainability, and the overall quality of public services.

The continuous collection and analysis of real-time data are fundamental to the operation of smart city initiatives, which are often shared across multiple stakeholders, including municipal departments, private vendors, and law enforcement agencies. Existing research [1, 59] highlights the central role of data as the foundation for developing and sustaining smart city services. For example, IoT sensor systems enable urban areas to detect traffic patterns [2], protecting the environment by monitoring key indicators such as air pollution, water quality, and the efficiency of waste collection and management systems, and manage resources more efficiently [39].

Additionally, smart cities are understood not only as technology-enhanced urban environments, but also as complex socio-technological systems in which digital communication and extensive data flows support and shape everyday urban life. Nevertheless, the same large-scale, continuous data collection practices that enable these efficiencies also introduce new forms of vulnerability. As some studies [22, 34] have noted, citizens may be concerned or uncomfortable about opaque data practices, intense surveillance, or non-transparent consent for data sharing. A clear example of these challenges is the absence of well-defined use cases that help both data providers and data users make effective use of available datasets to develop community-oriented and innovative services in smart

cities [10]. This confirms that a clear gap exists between the actual technologies used in smart cities and what citizens are aware of and believe is happening.

2.2 Privacy Challenges in Smart Cities

Privacy is commonly defined as an individual's right to protect their personal data and control how it is collected, used, shared, and stored [48]. However, this right is increasingly challenged in smart city environments that rely heavily on automation, pervasive surveillance, and data-driven decision-making [42, 52]. Extensive data collection often continues without explicit consent, creating significant privacy risks for residents [57].

Researchers have highlighted several concerns associated with comprehensive sensing infrastructures, including the creation of detailed user profiles, behavioural inference, and continuous location tracking. For example, a case study conducted in Phuket [54] demonstrated how excessive monitoring of personal behaviour, even during private and leisure moments, can threaten personal authenticity and expose individuals to potential technology misuse. In addition to these risks, surveillance has become a central issue in debates about privacy infringement within smart city [60]. The experience in China illustrates this point: widespread deployment of surveillance cameras in urban areas is used to monitor individuals and enforce government regulations, including identifying participants in public protests demonstrating how such systems may be used in ways that violate citizens' privacy rights [9]. In addition to algorithmic surveillance, certain systems deployed in major cities have raised further ethical and practical concerns.

One prominent example is the Social Credit System (SCS), implemented in several Chinese cities as a mechanism for managing society through information and communication technologies. The system aims to assess citizens' trustworthiness, compliance with legal rules, and adherence to ethical and professional standards [17]. However, research has documented substantial privacy challenges associated with the large-scale collection and analysis of personal data within the SCS. These practices may conflict with international data protection principles and raise the risk of misusing individuals' biographical information for purposes of social control. Moreover, concerns have been reported regarding discrimination and the potential denial of educational or employment opportunities, as well as the system's failure to account for variations across different stages of human life, which may have long-term consequences for individuals [62].

2.3 Users' Perceptions and Understanding of Data Collection and Sharing in Smart Cities

Most studies focus on the technical challenges of data collection and privacy in smart cities, such as data processing, storage, and cybersecurity, without considering the perspectives and concerns of individuals. For instance, Choudhry [18] emphasises the volume of data collected and notes that highly connected systems pose extra cybersecurity and privacy risks, as devices designed to enhance or streamline services can also be used for surveillance, persecution, and harassment in smart cities. Furthermore, Alnahari et al. [9] these authors primarily address privacy concerns in smart cities through technical solutions, such as blockchain and homomorphic encryption. Recent studies have started to examine citizens' perceptions and concerns directly. For example, Emami-Naeini et al. [22] conducted surveys to explore attitudes toward city-wide data collection, highlighting the importance of human-centric and privacy-aware smart city designs. However, such studies remain limited compared to the broader technical literature, and most examine citizens' perceptions only within Western cultural contexts. Few insights restrict understanding of how cultural differences shape privacy perceptions and norms in smart cities. This paper addresses this gap by highlighting differences in privacy-related perceptions and concerns across two distinct cultural contexts: Saudi Arabia and United Kingdom. The cultural nature of Saudi society strongly shaped participants' responses, particularly regarding data related to trust, governance, family members and women. These concerns were closely tied to religious norms and conservative social values, consistent with the findings of Haider et al. [32], who noted that privacy expectations in Saudi Arabia are influenced by high levels of religiosity and cultural conservatism. In Haider et al.'s study, Saudi participants expressed heightened digital privacy concerns, especially regarding family-related data, reflecting a broader societal view that privacy is essential for safeguarding cultural and religious identity.

In a different cultural context, Hartley [35] examined public perceptions in Hong Kong using the Smart City Strategy Index (SCSI) framework to assess the impact of smart cities on both governance and quality of life. The results showed that residents are more optimistic about improvements in quality of life than about expected changes in governance. The study employed a range of governance and quality of life indicators, including education and income, to analyze the role of political legitimacy and awareness levels in shaping individual expectations. The findings indicated that higher awareness of smart cities is associated with increased expectations of benefits, although the magnitude of this effect varies according to demographic characteristics such as education level and income. The study also offered policy recommendations to enhance public trust and support smart city initiatives through clearer and more transparent awareness campaigns. However, the data collection methodology, which relied on telephone interviews, presented a significant limitation of the study. This approach contributed to sample bias by excluding individuals without a smartphone or landline, potentially leading to an overrepresentation of groups with specific technical skills or financial means. This bias poses a challenge to achieving a comprehensive understanding of public perceptions. Accordingly, this paper used a different methodology based on personal interviews as a more comprehensive means of data collection.

2.4 Security and Privacy in Non-WEIRD Contexts

Security and privacy research has historically relied heavily on participants from Western, Educated, Industrialized, Rich, and Democratic (WEIRD) contexts, often implicitly treating observed threat models, trust assumptions, and privacy expectations as broadly representative. However, a growing body of work demonstrates that security perceptions and practices are deeply shaped by local

socio-economic infrastructures, governance regimes, religious and cultural norms. Research in Middle Eastern contexts (e.g., Jordan) highlights how privacy concerns extend beyond primary users to surrounding social actors. Previous studies [5–7] show that privacy expectations are negotiated within family and social structures rather than framed entirely as individual control. Moreover, work in South Asian contexts further demonstrates how infrastructural constraints reshape security risks. Haque et al. [33] document privacy vulnerabilities in public digital service centres in Dhaka, Bangladesh, where shared devices, limited technical literacy, and institutional practices create exposure risks that differ significantly from those assumed in personal-device–centric security models. Similarly, Munyendo et al. [49] analyze security and privacy challenges in Kenyan cybercafes, showing how intermediaries frequently select passwords on behalf of users. This practice complicates standard assumptions about individual agency, password hygiene, and user responsibility. Most recently, Herbert et al. [36] provide a large-scale comparison of digital security perceptions in WEIRD versus non-WEIRD contexts, demonstrating systematic variation in threat perceptions, institutional trust, and security behaviors. Overall, these works show that threat models, consent expectations, and institutional trust are situated within broader socio-political and infrastructural contexts. These findings motivate the need to examine smart city data practices across socio-politically distinct environments, particularly where governance structures and accountability mechanisms differ.

3 Methodology

To understand how people living in smart cities understand and perceive data practices and consent in smart cities, we conducted a semi-structured interview study with 19 participants living in smart cities in UK and KSA. We discuss our methodology below.

3.1 Ethics

This study received ethical approval from our Institutional Ethics Board (IEB) prior to data collection. Participation was voluntary. We provided a Participant Information Sheet (PIS) and a consent form to all respondents before the interview sessions. The PIS outlined the purpose of the study, the procedures involved, withdrawal process, and our data handling practices. Participants were assured that all responses would be kept confidential and reported anonymously, and that they could decline to answer any questions that made them uncomfortable. Data was securely stored on a university-hosted server, and we used a GDPR-compliant service for transcriptions.

3.2 Study Context

To understand how residents of smart cities perceive data practices and consent, we conducted our investigation in two cities: Bristol city in the UK and King Abdullah Financial District (KAFD) in Riyadh KSA. We selected these two cities because they represent contrasting national and cultural contexts while both being internationally recognised for their advanced smart-city initiatives. Bristol is widely viewed as a citizen-focused smart city, emphasizing sustainability, open data, community engagement, and experimental digital services [23, 44]. In contrast, KAFD region represents a purpose-built, technology-driven smart district characterised by integrated digital infrastructure, advanced automation, and top-down planning. Bristol shaped by bottom-up, community-oriented innovation, and KAFD by top-down, high-tech planning. These cities offer a valuable opportunity to examine how residents experience smart-city technologies across different cultural, social, and governance settings.

Bristol has been widely positioned as a leading "smart and open" city in the UK. It has invested in urban digital infrastructure, including city-scale data platforms, environmental sensor networks, open data initiatives, and experimental digital services supporting transport, sustainability, and civic participation. Key initiatives include a city-wide programmable digital infrastructure supporting IoT, big data analytics, 5G, AI/ML applications, CCTV analytics, and high-performance computing, positioning the city as a living testbed for urban data experimentation [12]. The public open data platform provides approximately 200 anonymised datasets covering energy usage, pollution, traffic flows, and infrastructure. Additionally, around 1,500 RFID-equipped lampposts and connected infrastructure enable real-world testing of data-driven applications [50]. Smart energy systems (e.g., smart metering and smart grids), intelligent transport, electric vehicle charging networks, and real-time energy monitoring further embed data collection into everyday urban services. Bristol's smart city development has evolved through partnerships among local government, universities, industry, and community organisations, reflecting a bottom-up, citizen-oriented model that foregrounds transparency and community engagement.

In contrast, KAFD is a purpose-built, master-planned smart district developed as part of Saudi Arabia's broader economic and digital transformation strategy. It integrates advanced digital infrastructure at the district level, including centralised building management systems, automated utilities, intelligent transport systems, and integrated surveillance and monitoring technologies. A central smart city platform leverages AI and data analytics to support real-time operational decision-making across energy, water, and traffic systems [51]. The district also deploys smart traffic management and Mobility-as-a-Service (MaaS) platforms that use real-time and predictive data to optimise movement. Ongoing technology pilots include smart building management, smart parking, and real-time digital services for residents and tenants [58]. KAFD region reflects a top-down planning model characterised by centrally coordinated infrastructure and embedded digital systems designed to optimise efficiency, security, and service delivery from inception.

3.3 Study Design

We adopted a qualitative research design using semi-structured interviews to gain an in-depth understanding of residents' perceptions of data collection, data sharing, and consent in smart cities. A qualitative approach is well-suited to examining complex socio-technical phenomena, particularly when prior knowledge is limited and the goal is to uncover mental models, expectations, and lived experiences rather than to measure predefined constructs. This approach also enables culturally grounded viewpoints to emerge, making it especially appropriate for comparing residents across two distinct national contexts. Semi-structured interviews allowed us to probe participants' understanding of smart cities, their perceptions of data collection, processing, and sharing, and their expectations of

consent and control within pervasive sensing environments, while providing the flexibility to follow emerging themes introduced by participants.

Our interview protocol consisted of five parts: (1) introduction, (2) understanding of smart cities, (3) perceptions and understanding of data collection and sharing, (4) consent, and (5) conclusion. ***Introduction***. This section introduced the researcher, explained the aims and goals of the study, and confirmed consent to participate and to allow audio recording. ***Understanding smart cities.*** These questions built rapport and explored how participants conceptualised smart cities. Understanding residents' interpretations was important for revealing underlying mental models and identifying differences in familiarity or awareness of various systems. ***Data collection and sharing.*** The third section examined participants' understanding and perceptions of data practices in smart cities. We explored views on data types, perceived benefits, use cases, retention, and potential sharing across organisations. ***Consent.*** This section focused on participants' perceptions of consent and control in the context of smart cities. We examined their expectations of how consent should be obtained, withdrawn, and the circumstances in which they believed explicit consent should be required. Investigating consent mechanisms in such environments provides insight into public expectations for data governance in pervasive sensing systems. ***Conclusion.*** The closing section thanked participants, invited them to share any additional thoughts, and provided an opportunity to ask questions about the study.

3.4 Pilot Study

We conducted two pilot interviews to evaluate the clarity, timing, and overall effectiveness of our interview protocol. After the pilot interview with one participant, we made several minor revisions. The participant noted that some questions were too long and difficult to answer, so we simplified the wording and combined a few items that asked for similar information. We also adjusted the interview length to approximately 40–60 minutes to reduce fatigue while still covering all key topics. Keeping the session at an optimal duration was important for maintaining participants' focus and engagement. During the second pilot, the participant reported that the questions were clear and that the interview length felt appropriate. As a result, no further changes were made. Data from both pilot interviews were excluded from the final analysis.

3.5 Recruitment

After finalising the interview instrument, we began participant recruitment. Recruitment targeted individuals who lived or worked in smart cities in both the United Kingdom and Saudi Arabia. Participants were eligible if they: (1) lived or worked in one of two selected smart cities (Bristol or KAFD region), (2) were at least 18 years old, and (3) actively interacted with or used smart technologies within their city. To identify suitable participants, we designed a screening questionnaire (See Appendix A). The screener collected various information about participants including their connection to each city, how long they have lived or worked in the city, feeling about data being collected to support city operations and services, demographic information and asked participants to identify the technologies or systems they believed contributed to making their city "smart." Recruitment was carried out through multiple online channels using our social and professional networks. We used platforms such as WhatsApp groups, university social group mailing lists, and Facebook groups associated with Bristol and KAFD. Non-smart city residents or commuters were not targeted or recruited for the study. Interested individuals were also encouraged to share the study within their own networks. In Saudi Arabia, recruitment additionally involved in-person outreach to individuals in the city social spaces like cafes who expressed interest. All interested individuals were asked to complete the screener and told they would be contacted for interviews if they were suitable.

Table 1: Summary of the Participants' Demographics

Smart City Location	UK	KSA
Gender		
Male	2	8
Female	6	3
Did not disclose	-	-
Age		
18–24	3	-
25–34	2	4
35–44	3	5
45–54	-	-
55–64	-	2
65+	-	-
Employment status		
Employed (Full-time)	2	11
Self-employed	1	-
Student	4	-
Unemployed	1	-
Live or work in a Smart City		
Yes	8	11
No	-	-
Preferred interview method		
Online	8	3
In person	-	8

3.6 Participants' Demographics

In total, 25 individuals met the eligibility criteria and were all invited to participate, 12 from Bristol and 13 from KAFD region in Riyadh. However, at the end only 19 attended their scheduled interview sessions: 8 participants from the UK and 11 from Saudi Arabia. The six individuals that expressed interest either did not respond to follow-up messages or did not attend their scheduled interviews. All participants were older than 18, and either lived or worked in their respective smart city. Individuals who did not meet these criteria were not invited.

Our final sample consisted of eight (8) participants from Bristol and 11 from KAFD region. In the UK sample, two participants identified as male and six as female. Three were aged 35–44, two were aged 25–34, and the remaining participants fell into other adult age categories. Employment backgrounds varied and included two full-time employees, four students, one self-employed participant, and one unemployed participant. All UK interviews were conducted online. In the KSA sample, eight participants identified as male and three as female. Five were aged 35–44, four were aged 25–34, and two were over 54 years old. All KSA participants were employed full-time. Eight interviews in KSA were conducted in person, while three were conducted online.

The sample was slightly larger in KSA (n=11) than in the UK (n=8). The UK sample included a higher proportion of female participants, whereas the KSA sample included a higher proportion of male participants. Additionally, employment status was uniform in the KSA sample (all full-time employed), while the UK sample reflected more varied employment circumstances. Table 1 summarises participant demographics. We discuss how these factors may have shaped our findings in Section 3.9.

3.7 Study Procedure

To accommodate participants' preferences and ensure accessibility, interviews were conducted either online or in person. Each session began with a brief introduction, a reminder of the study's purpose, and confirmation of informed consent, including consent for audio recording. All participants agreed to take part and provided permission for their interview to be recorded. The lead researcher conducted all interviews in both the UK and Saudi Arabia.

In Bristol, all interviews took place online using Microsoft Teams. Participants were sent the meeting link along with the Participant Information Sheet (PIS) and the consent form. They were encouraged to review and sign the consent form ahead of the interview. Once consent was confirmed, the researcher started the recording and began the interview. All interviews in the UK were conducted in English. Each session lasted around 45 minutes, and participants received £15 voucher as compensation. Before ending the call, the researcher thanked the participants and explained how the payment would be processed.

In KAFD, most interviews were conducted face to face (n = 8). Five participants who responded to the study advert arranged to meet the researcher in cafés or workplaces, while three others were recruited on the spot and agreed to be interviewed immediately. The three were asked to complete the screening form and then interviewed. As with the UK interviews, the researcher introduced themselves, explained the purpose of the study, and confirmed consent before starting the recording. Three additional participants preferred or required an online interview because the researcher had already returned to the UK; these followed the same procedure as the UK sessions. Interviews were conducted either in Arabic or English or a mixture of both. At the end of each interview, participants were thanked for their time and encouraged to share the study with others in their networks. All participants in Saudi Arabia were offered financial compensation. However, all explicitly declined the compensation, citing various reasons such as religious considerations, personal beliefs about research participation and charitable motivations.

3.8 Data Analysis

All interview recordings were transcribed by a GDPR-compliant professional transcription service to ensure accuracy and privacy. Interviews conducted in Arabic were then translated into English by a hired translator. Since one of the coders is a native Arabic speaker familiar with the cultural context, they were able to review translations to ensure that linguistic and cultural nuances were preserved. As this study was not designed as a formal comparative investigation, in which data are collected and analyzed separately, we combined datasets/transcripts from both contexts for analysis. We conducted an inductive, reflexive thematic analysis following Braun and Clarke's approach [11]. The primary researcher then started the coding process. First, going through each script and integrating their notes from the interview sessions. Then, the first and another researcher (i.e., experienced in qualitative research) began collaborative coding. As recommended for reflexive thematic analysis, the aim was not to quantify coder agreement but to engage in interpretive dialogue that supports deeper insight development. Accordingly, we did not calculate inter-coder reliability, as such metrics are not conceptually appropriate for reflexive TA and can obscure rather than enhance analytic rigor [40].

The two researchers independently coded two transcripts (one from Bristol and one from KAFD) to generate an initial set of inductive codes, then met to compare interpretations, merge overlapping codes, and agree on terminology. This process resulted in the initial codebook [29]. The two researchers then jointly coded two additional scripts (again, one from each city) to ensure shared understanding of the codebook and analytic approach. Discrepancies were resolved through reflexive discussion [29], and the codebook was refined as new codes emerged. Since our initial aim was not to compare cities, so including transcripts from both contexts early in the analysis ensured that the developing codebook captured the diversity of participants' understandings and perceptions. The differences between two cities were captured whenever possible. Both researchers then independently coded five additional transcripts and compared interpretations. After coding these transcripts, no new codes emerged from either city. We observed code saturation after the eighth transcript, meaning no new codes or concepts appeared, and continued coding beyond that point to ensure analytic robustness. This iterative, collaborative, and reflexive approach ensured that the final themes were coherent, well-developed, and grounded in the data, while avoiding direct cross-city comparison. Our approach aligns with established qualitative methodologies and mirrors practices used in prior studies published in top security venues [45].

3.9 Limitations

As with all qualitative research, this study is shaped by several methodological considerations.

Focus on resident perspectives. Our analysis reflects the views of residents with varying levels of interest in privacy and differing awareness of smart city infrastructures. While this approach provides valuable insight into lived experiences, it may not capture the full diversity of views within either country. Our findings should therefore be understood as indicative rather than exhaustive.

Absence of institutional and technical perspectives. We did not interview policymakers, system designers, data protection officers, or technical staff responsible for operating smart city systems. As a result, we were unable to compare resident perceptions with institutional practices. For instance, how consent mechanisms are designed, how data flows are managed, or what assumptions system operators make about public awareness. We believe that incorporating these viewpoints would allow for comparison between individual experiences and institutional practices, and help identify weaknesses in the design and implementation of systems.

Reliance on self-reported experiences and personal interpretations. Participants' understandings of smart cities and data practices were based on their current mental models, which were often incomplete or uncertain because smart city infrastructures are often opaque or poorly communicate. It remains unclear to what extent these perceptions align with actual policies, technical architectures, or operational practices. Our analysis therefore interprets these understandings as perceptions rather than factual descriptions of deployed systems.

Potential response biases. As with any interview-based research, participants' responses may have been influenced by social desirability, recall bias, or their previous experiences with technology and public services. It is also possible that expressed trust or acceptance of data collection and sharing may reflect the government-led nature of many smart city initiatives, which could discourage the open expression of mistrust due to cultural norms or perceptions of authority. Though we stressed anonymity, voluntary participation and encouraged participants to respond openly, these influences cannot be entirely removed or eliminated.

Scope and generalisability. This study was exploratory in nature and not intended to achieve statistical generalisation. While the overall sample size (n = 19) aligns with established qualitative research practices, the small number of participants per city limits the extent to which findings can be interpreted or generalized. First, the small number of participants per city especially in the UK means that city-specific observations should be treated as indicative rather than representative. In addition, differences in sample composition across locations, including gender distribution, age, educational background, and professional status, constrain the interpretation of cross-country contrasts. Our goal was to provide a deep understanding of resident perceptions in two specific smart city contexts. For this reason, interviews from both locations were analysed together as a deliberate methodological choice, reducing the risk of overinterpretation based on limited city-level data. Future work involving larger or more diverse populations may further validate or nuance these findings.

4 Findings

In this section, we present our findings. We begin by examining participants' understanding of smart cities, followed by their perceptions of data collection and sharing, including the benefits they associate with these practices and the concerns they raise. We then discuss their views on consent and control, including how they believe consent should be provided, managed, and improved within smart city environments. To illustrate these perspectives, we include quotations from participants in both countries. These excerpts are used to highlight variations in response patterns rather than to draw direct comparisons between regions. Quotes from participants in the United Kingdom are labeled (Px_UK), and those from Saudi Arabia are labeled (Px_KSA), where x denotes the participant ID.

4.1 Understanding of Smart Cities

The analysis revealed several key insights into how participants perceive and interpret the concept of smart cities:

Smart cities are automated and connected. Most participants familiar with smart cities describe them as automated, connected through infrastructure, as P7_UK said, "The smart city is connected everything together from lights, fire alarms, generating power," and incorporating advanced AI and technology. Participants commonly highlighted how sensors, digital systems, and devices communicate with each other to enable smooth operations. Participants described a range of smart technologies including automated lighting, smart waste systems, digital parking guidance, CCTV networks, and real-time transport information. This automation was consistently framed as central to smartness, with a smart city expected to perform tasks that traditionally required human input such as detecting traffic congestion, adjusting building access, or regulating environmental conditions. For instance, P5_UK: "Automated processes... things happen without people interfering." P8_KSA: "Technology... multitasking... self-operated."

Time-saving and improvements to quality of life. Both UK and KSA participants strongly associated smart cities with efficiency, speed, and reduced effort. Many contrasted smart and traditional cities by describing the latter as slow, manual, and disorganised. Participants described smart services as enabling tasks that once took hours to be completed within minutes. P4_KSA: "One hour becomes five minutes in a smart city." Participants in both contexts conceptualised smart cities as modern, comfortable, and convenient places to live. Interviewees described smart cities as environments that improve the "quality of life" (P8_UK) and "improve lifestyle" (P10_KSA) by simplifying daily routines, reducing stress, and making access to services more intuitive. This notion of improved quality of life encompassed safety, convenience, comfort, and accessibility. Participants described smart cities as places where citizens feel supported by their environment, and where technology acts as an enabler for a smoother everyday experience. "more sustainable and healthier to live in" (P4_UK)

Degree of awareness and familiarity. While majority of our participants were aware that they lived in smart cities, three participants showed uncertainty that they lived in smart cities, despite living and being in them, due to a lack of understanding of what smart cities entail, as the P1_UK said "I think it's lacking that though because I when you said that my city is smart city, you see I didn't have any idea and if it is collecting [my] data... I have no idea what kind of data it's collecting from and about me" and P3_KSA was wondering and said "Yeah, I honestly feel like, we're talking about a smart city. Because talking to you. I'm having trouble with some of this, visualising the data being pulled from the where you are while you're there?"

Contrast with traditional cities. Across all interviews, participants described traditional cities as lacking automation, requiring extensive human effort, and being less organised than smart cities. Traditional cities were seen as more time-consuming, dependent on manual processes, and offering limited technological support. For instance, P5_UK noted "traditional cities rely on people to do things.". P10_KSA added that everything in traditional city were manual "do everything manually."

Differences between the two contexts. Our analysis suggested some differences with regards to awareness, purpose of smart cities, examples used, role of technology, and responsibility for implementing smart cities. While three participants were not sure about whether they were in a smart city, majority of KSA participants showed high awareness of smart city features due to

living or working in a purpose-built district. They provided detailed descriptions of systems, including those still being developed or not yet active. In contrast, several UK participants often expressed uncertainty around specific systems. KSA participants focused on engineering, infrastructure, waste systems, security, structural design, parking towers, and city control. Their understanding was strongly shaped by the physical environment of City B, where smart systems are visible, structural, and broadly government-led. In contrast, UK participants viewed smartness through the lens of everyday services, such as transport information screens, mobility apps, sustainability, energy-efficient heating, and public-space sensors. Their focus was more on functional benefits within daily routines rather than on large infrastructural systems.

In terms of the role of technology, participants from KSA described smart city tech as tech that replaces human effort and systems functioning autonomously (i.e., systems being predictive, using behavioural insights, and being automatic). P9_KSA explained "In a [smart city] systems learns behaviour and adapt..." UK participants described technology supporting human tasks and decision making. They stressed that systems were assisting but not replacing decision-making. P3_UK noted "intuitive technology that helps with tasks." Finally, participants' views on who is responsible for implementing smart cities differed. KSA participants described smart cities as state-led or government projects, planned and implemented through national initiatives and managed by a unified authority (centralized responsibilities), while UK participants did not report a single body/entity being responsible for implementing smart cities. They believed that smart cities are delivered by multiple entities (decentralised responsibility) including council, private companies, transport agencies, and universities. P11_KSA explained "The management and development company is responsible... it is 100% owned by the government," and P1_UK said "Smart systems come from different services, not one owner."

4.2 Perceptions and Understanding of Data Collection and Sharing in Smart Cities

4.2.1 Data, Data Collection, Data Sharing. This section explores how residents understand and interpret the collection and sharing of data within smart cities. Participants described a wide range of beliefs about who collects their data, why it is collected, how it is shared, and what benefits or risks these practices create. Our analysis reveals both areas of confidence where participants recognise visible sensors that collect data and also a lot of uncertainties about the broader data ecosystem that operates behind the scenes.

Widespread of data collection. Participants in both countries viewed data collection as a required mechanism, stating that without data, the city cannot function or provide smart services. For instance, P4_KSA noted "Systems use data so residents can complete tasks in five minutes instead of one hour." They also highlighted that smart cities collect extensive data through cameras, sensors, apps, Wi-Fi systems, transport systems, and building access. They explained that this is an inherent part of how smart cities function. P3_UK: "Sensors at university... streets... they collect a lot [of data]." Both groups also expected monitoring in streets, buildings, transport, shops, and workplaces. This was seen as normal in a smart city, though some participants did not have complete understanding of how it happens. Both groups assumed smart cities collect CCTV footage, movement/location data, number plates, Wi-Fi data, building access logs, and behavioural data. P7_UK said, "A lot of data... cameras can detect if you're on your phone while driving."

Reasons for data collection (perceived purposes) Regarding data collection and sharing, participants from both regions strongly associated data collection with safety and security. Participants also believed data was used for city planning, traffic and congestion management, emergency response, operational efficiency in public services. They believed automatic data collection was beneficial for automation, reducing time, minimising effort, and streamlining movement and services. Majority viewed surveillance as essential for monitoring activities, preventing crime, and ensuring order. P6_UK mentioned, "CCTV, which is keeping crime from keeping crime to a minimum" and P8_KSA explained that "More security for people, of course. If there are public places, and government-specific cameras, I don't have to worry about my life." Other participants stated data collection was for improving the quality of life by offering smart, high-efficiency solutions and services to the residents as P5_UK said, "I think the benefits are obviously the more data they've got, the better solutions they can find."

Who participants believe collects smart-city data. Participants across both cities believe data in smart cities is collected by public authorities such as government, police, councils, and city management organisations. Majority of KSA participants viewed the government or city operator (e.g., [redacted] management company) as the central collector. P11_KSA "The government is responsible for everything... they collect data." On the other hand, UK participants viewed data collectors as various entities such as councils, police, universities, transport companies, and sometimes private contractors. P8_UK "I assume the council or government collects the data." Few participants mentioned private technology vendors, cloud providers, or analytics companies: P2_UK mentioned "companies that provide the services for the people living in smart cities" P8_KSA added "All companies want data... All the business owners in my eyes are dying for their data especially with the analysis that you can do a lot of things."

Who should access data in smart cities. Regarding who should have access to collected data or whom should receive data, participants mentioned various government entities and law enforcement agencies. For instance, they believed that government entities needed the data to improve the city, while law enforcement such as the police needed to access data for ensuring safety. P6_UK said "I want, you know, I want to say the police." Participants mentioned various benefits of allowing data to be accessed by these entities, most cases their willingness or openness to allowing access or sharing of data is when they perceived benefits. P5_UK said "Yes, definitely. If I knew what the benefits are, yes, they can [access data]" and P2_KSA said "If there is a benefit for a person, it's then normal."

Some participants felt that their data should remain confidential and not be shared with unauthorized entities. Furthermore, five participants specifically mentioned that their data should not be shared with private companies. P8_KSA, said "Government only, but commercial companies, no, totally no." On the other hand, many

participants stated that their data should be shared only with authorized persons, and some emphasized they would only share data if they gave explicit consent. As Participant P5_UK noted, "To share my data, I feel like it's a matter of consent more than anything, no, not without consent, no'.' Similarly, Participant P5_KSA stated, "I don't think it is appropriate to share it unless there is a clear consent." Our analysis also suggests that KSA participants were supportive of the government collecting data than the participants from UK. They expressed trust in the government's response. For example, P5_KSA stated, "The government, of course... this is in the case of a request from the government." Thus, they believe that sharing data with the government is both mandatory and beneficial. Unlike some participants from the UK, who expressed the opposite opinion, P5_UK said, "I'm willing to share my bank and my GP and me, but not the government," and P1_UK said, "I hope that the government wants just to improve life in the city, but I think most data is just sold."

Sensitive data should not be collected or shared in smart cities. Participants expressed their feelings about data collection and sharing in two main ways. First, they felt comfortable sharing certain types of data they consider less personal, such as movement, environment, and transportation usage, since these do not reveal their identities, such as P3_UK revealed "I think foot traffic is like the amount of people that use that service" and P5_KSA said "Kind of like temperatures and data about transportation use. I think anything that's not very personal like again movement I feel is fine." Second, they argued against sharing personal data, which they consider sensitive. This group pointed out that data like biometric information, identification, financial records, health data, and location or daily activity details can directly identify them. P1_KSA mentioned "photos or ID, my personal data" and P5_UK said "maybe data like more personal things like locations and things like that." They also worry about data related to their shopping habits (visiting physical stores), internet use (connecting to city wifi), and lifestyle (e.g., visiting gyms or libraries), as these could lead to targeted ads based on their behaviors, such as P7_UK said "lifestyle data of the people there and their shopping" and P6_KSA mentioned "And what's my habit, do I go for a library to pick up a book, or do I go out for a smoke? They can capture this data and make some sort of an analysis."

Understanding data processing and sharing. Participants from both regions generally believed that data flows automatically in smart cities, it gets collected by the systems then stored and shared between agencies for safety and operational reasons. Participants in KSA assumed that it is automatically collected and kept centrally by the government. P7_KSA explained what happens to data: "It goes to one place to the government." In contrast, UK participants assumed that data collection and sharing is dispersed and is potentially shared with many entities: P8_UK showed uncertainty about sharing "Who even sees it? Police? Council?"

4.2.2 Concerns Around Data Collection and Sharing in Smart Cities: Participants across both KSA and the UK expressed a range of concerns about smart-city data practices, focusing on security risks, privacy violations, misuse, and the potential for data-driven control. These concerns reveal uncertainties about how data is processed and shared, the opacity of smart-city infrastructures, and the ethical implications of pervasive surveillance.

Security concerns: Data breaches and misuse. Participants in both contexts identified security threats as a major worry, particularly the risk that personal data could be accessed or exploited by malicious actors. They did not describe specific attack vectors, but their comments reflect a generalised fear of system vulnerability and the consequences of large-scale breaches. For instance, this concern was popular among residents who rely on digital accounts or mobile services connected to the smart city services. P6_KSA was worried their account associated with services could be hacked; "My concern is there may be... somebody may try hacking into my account that I use to get services," while P4_KSA added "It could also be something that puts you at risk, for example, if someone hacked into the data." Several participants also believed that smart-city data might eventually be used against residents either by authorities, corporations, or other actors. Some framed this in terms of commercial exploitation. For instance, P1_UK was worried that residents were likely to be treated as "products" based on their data. Others raised concerns about anticipatory profiling or future misuse, explaining that right now they may not misuse it but in the future it might change. For instance, P10_KSA noted "When they know a lot of our living, that may change a lot in the future." P5_UK explicitly linked data collection to bad purposes: "There could be parties using it for not so good things as well"

Privacy concerns: Sensitive data exposure. Participants worried that smart-city systems may collect, store, or leak sensitive personal information, including images, financial details, or health data. Concerns were heightened when participants felt uninformed about the extent of data capture. P3_KSA said, "My concern is that data may be leaked... personal images may also be used..." P5_UK further explained that they would not want to share their personal data with the fear of it being exposed. P5_UK: "I wouldn't want to share how much money I make, or health stuff."

Fears of data-driven control or manipulation Some participants described scenarios where data collection could enable forms of behavioural control, profiling, or unwarranted or inappropriate influence. These concerns were not always technically precise but reflected anxiety about power asymmetries and the potential misuse of detailed personal data. For instance, P2_UK noted "The idea of someone controlling everything" was a central worry. P3_KSA further added "Concerns influence consumer behaviour... and indirectly influence opinion as well." P7_UK echoed this sentiment, expressing concern "if they are using the data to control my needs."

Gendered and cultural privacy concerns (KSA Only). Participants expressed concerns around the collection or sharing of women's facial data or images, noting that this is against their cultural norms and gender expectations. This concern is tied to social norms around modesty and visibility and did not emerge in the UK interviews. P6_KSA explained, "Many girls and women don't want to be photographed; yes, it's part of Saudi culture. I can understand that. It's very subjective, and I'm sure many would oppose having their faces captured." In addition, participants highlighted that such data practices may negatively affect women's job opportunities. Participant P8_KSA stated, "There is too much concern when our data is in the owner's hands. Today you are an open book. These things are personal, and they have harmed some people's interests.

For example, my wife... if they know you have many children, you may lose job opportunities that could provide a better life. I feel there are many sides to this." Notably, this concern did not emerge in the UK interviews.

Family member data should not be collected and shared in smart cities (KSA Only) Another notable cultural difference regarding sensitive data in the context of smart cities in Saudi Arabia was the perception among participants that data relating to family members was particularly sensitive and required strict privacy measures. This was reflected in statements such as P5_KSA: "Smart cities [are] collecting data, but for example, I can't imagine the date of birth or family members' data being collected because I don't want them to collect this data," and P6_KSA: "They can collect my picture, they can collect my video, but they should respect Saudi culture... I'll say no." Unlike participants in the UK, those in Saudi Arabia mentioned specific concerns related to family members and women, whereas UK participants did not highlight such issues.

4.2.3 Understanding and Perception of Data Storage and Retention. Understanding where smart-city data is stored and how long it is retained was one of the least developed areas of participants' knowledge. While residents could readily describe what data is collected, they struggled to articulate what happens to it after collection. Their responses revealed significant uncertainty about storage locations, retention timelines, and deletion practices.

Limited awareness around storage. Across both KSA and UK participants, there was a consistent and substantial gap in understanding where smart-city data is stored. Participants acknowledged that data was being collected but reported no knowledge of its physical or digital destination, such as whether it resides in local servers, government systems, cloud platforms, or third-party infrastructures. P4_KSA noted "I have no idea where data is stored." No participant described any concrete understanding of data storage infrastructure. This uncertainty contributes to broader feelings of lack of transparency and control, as participants perceived the data environment as a "black box" with invisible processes behind it.

Indefinite or extended retention of smart-city data Some participants expressed uncertainty about data retention practices in smart cities. Several were unsure how long their data would be stored, as P4_UK noted, "I'm not sure about how long data is kept." Others believed data might be kept indefinitely, with P4_KSA stating, "Maybe forever...," and P5_UK adding, "I'm assuming it's many years to forever." Some participants, however, assumed a fixed retention period, such as P8_UK and P7_KSA, who both stated, "For five years."

Perception that data cannot be deleted. Several participants believed that once data is collected in a smart city, it cannot be deleted, regardless of individual preferences or withdrawal of consent. P8_UK: "I think that they wouldn't delete the data." This suggests a broader perception that smart-city infrastructures are one-way systems, they ingest or take-in and store data, but do not provide mechanisms for removal, correction, or revocation.

4.3 Perceptions Around Consent and Control

Regarding Consent and Data control, participants shared various views on existing consent mechanisms, who should obtain consent, how it should be obtained, and how it should be revoked. Our analysis highlighted lack of visible consent mechanisms or that most participants were not aware of consent mechanisms for smart cities, and their desire as to how consent can be obtained.

Notification is very important for collection and sharing of data in smart cities. Most participants stated that consent is very important because it helps them understand what data will be collected, shared, and for how long it will be kept. P1_UK explained, "It [consent] would improve information about data collection we will know that we have some data being collected and shared, whether it's sensitive, or if it's not sensitive, we would know more information about it." Others explained that it would also clarify the reasons for data collection, empowering individuals to make an informed decision about whether to grant or deny consent based on this knowledge. P6_KSA mentioned, "Consent-wise, it's like if you're going to see a doctor. They should ask consent for the data that they will put into their database," and that data should not be shared without consent.

Consent is not actively given or sought. Across both countries, residents agree that smart-city systems operate without explicit user consent. Consent is assumed rather than requested. They described it as implicit and unavoidable. Most participants reported that they were rarely or never asked for consent regarding data collection in smart cities. P3_UK stated, "Consent... oh, I think it's quite absent." Similarly, P6_KSA noted, "I haven't signed any consent form here." Participants argued that simply being in the city means you have given consent "being present is agreeing" P1_KSA explained, "If you are in City B, it's automatic." P8_UK "Just by living here, I guess you consent." Participants resolve the lack of consent by relying on trust in authorities (KSA) or accepting surveillance as inevitable in such environments (UK). Regardless of context, participants express acceptance that consent is not part of smart-city systems. P2_UK noted "You just have to accept it... that's how cities are now."

While participants across both cities agreed on implicit consent, we also observed that for KSA participants there was a strong belief that authorities have legitimate permission to collect data without explicit consent. Data collection was seen as expected and acceptable. P11_KSA argued "Government is responsible for data collection so they can collect it... It is okay" and later added, "It's for safety... so it's fine." Others from KSA framed consent as unnecessary because the city is inherently a managed environment and they are not involved in everyday decisions about it. They believed control should remain with authorities. P1_KSA explained, "No need for us to control it." In contrast, some participants in UK showed some discomfort with non-consensual collection. They believe consent should be explicit or at least communicated. Consent was framed as a right that should be preserved even in smart cities. They desired for transparency, choice, or regulation. P8_UK expressed, "Shouldn't they ask us or tell us about it [data collection]?" and P2_UK added "We should choose what we agree to."

Low sense of control over data. Residents in both regions feel they have almost no control over data collection, how long data is retained, or who accesses it. They feel unable to modify, restrict, or delete data. Several participants stated they do not recall meaningful interactions, settings, or notifications where they were asked to decide on what data can be collected hence they feel like

data in smart cities is out of their control. P10_KSA and P8_UK stated respectively, "You can't change anything, even if you wanted to," and "We can't control what they take or keep." Despite both groups acknowledging less control over data, we observed that high expectation of transparency in UK participants. Residents believe that they should be told what is collected, why, and by whom. They desired for greater oversight, settings, or information to regain agency. For instance, P8_UK noted "Right now it's unclear... they should explain this to us," P3_UK expressed desire to have controls to decide their data sharing preferences: "There should be some settings or something."

Control is seen as structurally impossible. Our analysis shows that some participants believe smart cities are designed and built in ways that fundamentally remove user control. They explained that sensors are embedded into streets, buildings, transport, and infrastructure. As a result, there is no technical or social mechanism for opting out. P7_UK: "Being part of infrastructure means you can't avoid it. You can't do anything." Participants in KSA showed some neutral or positivity despite this, they tended to focus on safety, order, and efficiency while the UK participants were a bit uneasy and critical. KSA participants held the assumption that systems act in residents' best interests. KSA_P9 explained" It's safe... everything is under control." KSA_P11 added "it makes me feel safer." However, UK participants showed some feelings of being watched or lacking privacy. For instance, P7_UK noted "It's a bit uncomfortable... like being monitored all the time."

Participants' desire: Awareness around data collection and sharing. Most participants stated that smart cities should raise awareness by offering clear and easily understandable consent options for residents. P10_KSA mentioned, "they should raise awareness among the people about what they are gonna use from our data and how they gonna use it. Then they gonna give [us] the chance if we want to be a part of this or not." Participants believed majority of individuals in their cities were not aware of data collection and they need awareness. P4_UK, "I think we need to be more aware, like I don't think the awareness is really there, to be honest, and I want the awareness."

Participants' desire: Consent should be sought by all service providers. Participants believed that responsibility for requesting consent should lie with the entity managing the smart-city systems. They mostly cited the government, the city council, building owners or the service provider operating the infrastructure. Residents expected these bodies to inform them, request consent, and provide clear mechanisms for accepting or declining data collection. KSA participants gave examples around government or state-owned company seeking for consent: P11_KSA "The government is responsible for everything... so yes, they should tell us." P7_KSA added, "There should be one party responsible... where we give approval or consent." UK participants also mentioned government (or council) and various service providers offering services in the city: P5_UK "The City Council should tell me this data is being collected..."

Participants' desire: Consent should be obtained digitally. Most participants believe that consent should be obtained digitally through various mechanisms such as mobile apps, email, and text messages. P1_UK mentioned, "it should be an app and then everybody will have access to it." And, a few participants suggested that consent in smart cities should be obtained through a unified interface, P3_KSA mentioned that, "It is supposed to be coordinated between all the organisations working in the city with the policymakers. There should be, as we say, a unified interface." Additionally, some explained that the method of consent should be brief and easy to understand. P3_UK "By making disclaimers more obvious, you know improving transparency, letting people know what their data is used for, and also increasing the accessibility of these so-called terms and conditions, and you know. Whatever the the fine print is maybe like it could be inserted as a link that is forever present on the screen"

Participants' desire: Consent should also be sought by offline means. While other participants suggested that consent should be sought and given digitally, others suggested that offline consent mechanisms like mail and offline forms. Some participants, particularly UK-based explained they could be sent paper-based forms which could explain what data is collected and by whom. P1_UK noted "Could they use an old way and send us a mail in the post? Can we not be smart?" and later added "I think it should be more clear that from time to time they send something to the house... explaining what kind of data they share and if we consent." Others discussed having signage at entry as consent mechanism. For instance, P7_KSA said, "If it is really collecting data... a sign is supposed to be in one place... you see while you are here that we are capturing your data... we put a sign that says be careful, there are cameras. So you know." Some participants saw consent as contextual and place-based, not global in smart cities. They explained consent could occur when entering smart buildings, gated district or high-monitoring areas. P3_KSA, "the legislation should be clear... then the residents [can] give their consent. For example, if residential housing is one of the smart district... signing the housing [contract] means we agree to the collection of data when entering." P6_KSA also added, "If we are entering the city... there should be some place saying I am providing my consent at the entry point."

Participants' desire: Participants should have the choice to withdraw consent. While majority of participants acknowledged implicit consent, several participants expressed the desire to be able to withdraw from data collection and sharing. For instance, P5_UK argued, "The City Council should tell me this data is being collected and allow me to withdraw my unique information out of that data if I don't want to be in it." They also stated that consent revocation could be implemented through digitally or offline mechanisms. P1_UK "[digitally] same way that we would be consenting to collection". P9_KSA added, "Of course. The way should be clear in the privacy notices, a way to withdraw data. We should have a way of not consenting, or withdrawing our consent."

While desire to withdraw consent, participants also highlighted this may not be feasible in reality. Residents recognise structural constraints and technological limitations, they explained sensors are embedded into public space throughout the city, making control technically infeasible. Many participants implied the only way to opt-out is "not living there." Some explained revocation is infeasible because systems are interconnected and in some cases systems are government enforced. Others explained that this is the reason why they cannot refuse or reject data collection and sharing. P7_UK and P11_KSA both said respectively, "There's no way to say no." and "You cannot go around switch off cameras." Some participants

believe society "expects" monitoring, making refusal socially deviant or impractical. P4_KSA: "You can't refuse... but why would you?" Between the two groups, our analysis suggests majority of our participants in KSA do not expect revocation of consent to be possible given the need to collect data to protect the society (security purposes). UK participants want revocation but recognise it is structurally impossible. P3_UK said "I know [its impossible] but there should be some settings or something to say no."

5 Discussion

Perceptions of Smartness, Automation, and Responsibility. The findings showed that most participants in both cities associated "smartness" with increased automation, interconnection between systems, and reduced reliance on human intervention. Participants often contrasted their current cities with previous "traditional" cities that lacked technological integration and data sharing across systems. For many, automation and efficiency were taken as indicators of progress. Participants also emphasized that governments play a fundamental role in operating and maintaining smart cities and are primarily responsible for their functionality. However, some participants were uncertain whether their city was truly "smart," possibly due to limited awareness of available systems or limited personal engagement with them.

Implications. These findings suggest that residents often equate smartness with efficiency rather than accountability. Designers and policymakers should therefore ensure that narratives of automation and optimisation are accompanied by clear communication about data governance, oversight mechanisms (e.g., regulatory bodies), and accountability structures. Smart city branding should not only focus on the benefits or gains, but also articulate how data practices are monitored, audited, and regulated.

Conditional Acceptance of Data Collection. Our findings suggest participants' understanding of data collection and sharing maybe influenced by governmental narratives framing data collection as beneficial, scientific, or necessary for improving the society, regardless of any potential harm they may perceive. While most participants initially expressed displeasure towards the collection of sensitive data, several reconsidered when tangible benefits were presented particularly relating to safety. This aligns with prior work showing that individuals may accept data collection when perceived benefits are clear [56]. This pattern is also consistent with Emami-Naeini et al. [22], who found that residents in U.S. smart city contexts often weigh perceived civic benefits against privacy risks when evaluating data collection. Our findings extend this work by showing that such trade-offs may also be influenced by governance context and institutional trust, rather than being purely individual cost–benefit calculations. Participants' willingness to share data only with trusted or relevant authorities also reflects their awareness of privacy issues and their hope that such entities would protect it. However, such trust was not unconditional.

Implications. Our findings suggest that consent in smart city environments cannot rely only on complicated privacy notices or legal compliance. Consent and transparency mechanisms need to be clearer, more understandable, more genuinely informative, clearly articulating the specific benefits, purposes, and limits of data use in context. In public and semi-public spaces where traditional opt-in consent models are often impractical alternative mechanisms such as layered transparency notices, real-time disclosure dashboards, and publicly accessible data-use registries may better support meaningful awareness. *Future Studies.* Given the rapid development of technologies and changing patterns of use, there is an urgent need for long-term studies that track shifts in individuals' understanding, levels of trust, and ways of interacting with these technologies over time. These efforts would help determine whether trust increases with the expansion of smart city systems, or whether it declines as a result of increased awareness of privacy risks.

Cultural Dimensions of Privacy and Gendered Concerns. A clear cultural contrast was evident in the strong emphasis placed on protecting data related to women and family members in Saudi Arabia. These concerns may be partly rooted in religious considerations as well as social customs and traditions embedded within conservative societies, making privacy issues particularly sensitive. Importantly, such concerns resonate with findings by Mahera et al. [38], who highlight heightened privacy risks faced by women in the Global South, particularly in contexts of surveillance and unequal power. Moreover, our findings also resonate with Albayaydh et. al.'s works on Jordan contexts [5, 7], which highlights how privacy is negotiated relationally within households rather than framed only as individual control. They also demonstrate how power dynamics shape privacy expectations in Jordanian households. Together with our findings, this suggests that smart city consent models grounded in Western individualistic notions of autonomy may fail to account for relational and culturally embedded privacy norms.

Implications. Smart cities must consider fairness and be equitable. Surveillance and data systems can affect women and marginalised groups differently, so cities should assess these impacts and involve diverse communities in decision-making to ensure privacy concerns are properly understood and addressed.

Institutional Trust and Contextualised Threat Models. Saudi participants generally showed greater trust in sharing data with the government entities, while UK participants were more likely to express reservations, including concerns about secondary use (e.g., electoral contexts) or third-party sharing. This aligns with prior work showing contextual variation in institutional trust [8]. Herbert et al. [36] provide further empirical evidence that digital security perceptions differ systematically between WEIRD and non-WEIRD contexts. Our findings align with their argument that threat perceptions and institutional trust are socio-politically situated rather than culturally invariant. By extending this insight to smart city infrastructures, we demonstrate how governance context shapes not only general security practices but also expectations surrounding urban data collection and consent.

Implications. These differences suggest that user threat models are context-dependent. Security mechanisms deployed in smart cities should therefore make explicit which adversaries they address (e.g., external attackers, insider misuse, third-party sharing, or state overreach) and align communication strategies accordingly. Designing globally deployable infrastructures without accounting for contextual trust dynamics risks misalignment between technical guarantees and user expectations.

Surveillance, Manipulation, and Commodification Concerns. The results also revealed concerns related to security and

privacy arising from the collection of sensitive data, such as financial information and personal identity details, which may lead to potential privacy breaches. Participants also expressed fears regarding the ability of governments and companies to control their needs by tracking the details contained in the collected data. Some participants interpreted this as a form of manipulation, where their data are used against them by treating them as commodities or targets for commercial advertising. These findings also closely align with Mandal et al. [46], who document tensions between perceived benefits and privacy concerns in the context of city-wide WiFi services. Both Mandal et al. and our study identify discomfort with opaque or indefinite data retention practices, as well as resistance to third-party data sharing, particularly for advertising or commercial profiling purposes. However, our study extends this work by examining these tensions across multiple smart city services rather than a single infrastructure and across distinct sociotechnical and governance contexts. This broader scope allows us to show that such concerns are not tied to one specific service model, but emerge as recurring patterns in data-intensive urban environments. Moreover, our findings suggest that privacy risks in smart cities may similarly stem from infrastructural configurations and governance arrangements rather than only from technical flaws. *Implications.* To address these concerns, smart city infrastructures should prioritise data minimisation, purpose limitation, access controls, and audit logging. Independent auditing mechanisms and publicly documented data impact assessments may further enhance credibility and mitigate fears of manipulation or opaque secondary use.

Explicit Consent in Smart City Deployments. Majority of participants from both cities reported not having engaged with any form of explicit consent regarding the collection of their data within their smart cities. This result indicates a clear absence of informed consent mechanisms in the implementation of smart city applications, which aligns with Rob Kitchin's [41] view regarding ethical governance in smart cities, despite their crucial role in fostering trust between individuals and institutions. This mirrors findings from Mandal et al. [46], who report that users of city-wide WiFi services often lack clarity regarding data practices despite formal privacy policies. Together, these findings suggest that notice-and-consent paradigms may be structurally ill-suited to ambient, infrastructure-level data collection in urban environments. *Implications.* Rather than relying only on individual consent, smart city governance should incorporate participatory engagement mechanisms, such as citizen advisory boards, community consultations, and transparent reporting frameworks. Moving from studying residents to actively involving them in shaping privacy policies may help align governance models with residents' expectations and enhance perceived legitimacy.

Takeaways

- **Smart-city data practices are largely invisible to residents.** Participants understand that smart cities collect "a lot of data," but they do not know how, where, or by whom it is processed. This invisibility produces uncertainty, speculation, and diminished trust in the overall ecosystem.
- **Consent in smart cities is experienced as automatic and unavoidable.** Most residents believe that consent is implied, they believe they have already "agreed" simply by being present in the city. They rarely encounter explicit consent mechanisms and feel unable to meaningfully participate in decisions about data use.
- **Data control feels structurally impossible due to embedded infrastructure.** Since sensors and systems are built into streets, buildings, transport, and public spaces, residents feel they cannot opt out or delete data. This structural inevitability reduces perceived agency and shapes attitudes toward privacy.
- **Residents want transparency, awareness, and choice** Across both contexts, people ask for clear explanations, accessible consent options (digital and offline), and the ability to understand or manage their data. These are seen not as optional extras but as necessary components of living in a smart city.

6 Conclusion

Smart cities promise increased efficiency, safety, and urban intelligence, yet our findings show that residents' understanding of their data environments remains fragmented, incomplete, and deeply shaped by trust, cultural norms, and governance expectations. Across both KSA and the UK, participants recognised pervasive data collection but had limited visibility into the less tangible layers of processing, storage, and sharing. They relied on assumptions, often inaccurate, about centralised authorities, benign intentions, and continuous data retention. This highlights important gaps. When residents cannot articulate who collects their data, how it is used, or where it flows, they lack the ability to meaningfully evaluate risks or exercise agency. The absence of clear consent mechanisms and the widespread belief that participation is unavoidable contribute to privacy resignation, reducing public capacity to challenge harmful practices or identify misuse. Our cross-city study suggest that while trust can mitigate some concerns, perceived lack of transparency may amplify it. However, neither context provides residents with real control or reliable information about smart-city data practices. For security and privacy researchers, these findings highlights the urgent need for transparent, intelligible data governance in public infrastructures. Smart-city systems cannot rely on invisible data flows, implicit consent, or assumptions of public trust. For smart cities to be successful, they require accountable data pathways, explicit and revocable consent mechanisms, and communication models that make backend processes comprehensible to non-experts. Without such measures, they risk embedding asymmetries of power, normalising surveillance, and undermining the very public trust they depend on. Our paper also highlights that advancing smart-city security is not only a technical challenge but a socio-technical one.

Acknowledgments

We thank the anonymous reviewers for their helpful feedback. We are also deeply grateful to our participants. Wejdan Alsarih is a PhD student supported by Kingdom Of Saudi Arabia Ministry Of Education. Ramokapane's time was supported by REPHRAIN EPSRC EP/Y036611/1 and EPSRC Equitable Privacy EP/W025361/1.

References

[1] Mohammad Abu-Matar and John Davies. 2017. Data driven reference architecture for smart city ecosystems. In *2017 IEEE SmartWorld, Ubiquitous Intelligence*

& Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, IEEE, San Francisco, CA, USA, 2017, 1–7.

[2] Aditi Agrawal and Rajeev Paulus. 2020. Intelligent traffic light design and control in smart cities: a survey on techniques and methodologies. *International Journal of Vehicle Information and Communication Systems* 5, 4 (2020), 436–481.

[3] Dirk Ahlers. 2025. Open Urban Innovation Ecosystems-Integration of Data, Services, and Stakeholders. In *WWW'25: Companion Proceedings of the ACM Web Conference 2025*. ACM, Association for Computing Machinery, New York, NY, USA, 1715–1718.

[4] Muath Mohammed Alashqar, Ahmed FS Abulehia, Ahmad Ali Atieh, Mo'men Hani Mahmoud, and Mohammad Mahmoud Saleem Alzubi. 2025. Legal Framework for Regulating AI in Smart Cities: Privacy, Surveillance, and Ethics. In *2025 International Conference for Artificial Intelligence, Applications, Innovation and Ethics (AI2E)*. IEEE, 2025 International Conference for Artificial Intelligence, Applications, Innovation and Ethics (AI2E), 1–6.

[5] Wael Albayaydh and Ivan Flechais. 2023. Examining power dynamics and user privacy in smart technology use among jordanian households. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4643–4659.

[6] Wael Albayaydh and Ivan Flechais. 2024. {Co-Designing} a Mobile App for Bystander Privacy Protection in Jordanian Smart Homes: A Step Towards Addressing a Complex Privacy Landscape. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4963–4980.

[7] Wael S Albayaydh and Ivan Flechais. 2022. Exploring bystanders' privacy concerns with smart homes in Jordan. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–24.

[8] Khaled Almotairi, Bilal Bataineh, et al. 2020. Perception of Information Sensitivity for Internet Users in Saudi Arabia. *Acta Informatica Pragensia* 9, 2 (2020), 184–199.

[9] Wael Alnahari and Mohammad Tabrez Quasim. 2021. Privacy concerns, IoT devices and attacks in smart cities. In *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*. IEEE, 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 1–5.

[10] Rebekka Alvsvåg, Anthony Bokolo Jr, and Sobah Abbas Petersen. 2022. The role of a data marketplace for innovation and value-added services in smart and sustainable cities. In *International Conference on Innovations for Community Services*. Springer, I4CS – Innovations for Community Services, 215–230.

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[12] Bristol City Council. n.d.. *Bristol is Open*. https://www.bristol.gov.uk/council/policies-plans-and-strategies/companies-owned-by-the-council/bristol-is-open Accessed: 7 March 2026.

[13] Vivien Butot, Gabriele Jacobs, Petra Saskia Bayerl, Josué Amador, and Pendar Nabipour. 2023. Making smart things strange again: using walking as a method for studying subjective experiences of smart city surveillance. *Surveillance & Society* 21, 1 (2023), 61–82.

[14] Zekun Cai and Aiping Xiong. 2023. Understand users' privacy perception and decision of {V2X} communication in connected autonomous vehicles. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 2975–2992.

[15] Paolo Cardullo and Rob Kitchin. 2019. Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused'smart cities in Europe. *Environment and planning C: politics and space* 37, 5 (2019), 813–830.

[16] Shiyin Chen, Qingxu Huang, Raya Muttarak, Jiayi Fang, Tao Liu, Chunyang He, Ziwen Liu, and Lei Zhu. 2022. Updating global urbanization projections under the Shared Socioeconomic Pathways. *Scientific data* 9, 1 (2022), 137.

[17] Yongxi Chen and Anne SY Cheung. 2017. The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system. *J. Comp. L.* 12 (2017), 356.

[18] Arnav Choudhry. 2022. Smart mobility: challenges and opportunities for the next generation of transportation. *XRDS: Crossroads, The ACM Magazine for Students* 28, 3 (2022), 14–19.

[19] Eric Corbett and Graham Dove. 2024. Signs of the Smart City: Exploring the Limits and Opportunities of Transparency. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–14.

[20] Cansu Demir, Nicola Leschke, Glenda Hannibal, Mahdi Akil, and Alexander Meschtscherjakov. 2025. Understanding Driver Expectations and Preferences Around Data Transparency in Vehicular Digital Twins. In *Adjunct Proceedings of the 17th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. Association for Computing Machinery, New York, NY, USA, 227–232.

[21] Jiafei Dong, Lu Ning, Rongbo Xiao, Xiangyun Cao, Chen Song, Haobo Gao, and Yichen Fan. 2025. Research on Technical Solution and Implementation Mechanism of Wechat Ecosystem-Based Air Quality Program. In *2025 6th International Conference on Computer Engineering and Application (ICCEA)*. IEEE, 2025 6th International Conference on Computer Engineering and Application (ICCEA), 1473–1478.

[22] 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*. Association for Computing Machinery, New York, NY, USA, 1–24.

[23] Aksel Ersoy. 2017. Smart cities as a mechanism towards a broader understanding of infrastructure interdependencies. *Regional Studies, Regional Science* 4, 1 (2017), 26–31.

[24] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–16.

[25] Oliver Gassmann, Jonas Böhm, and Maximilian Palmié. 2019. Smart cities. In *Smart cities*. Emerald Publishing Limited, 25–66.

[26] Athanasios Georgiadis, Panayiotis Christodoulou, and Zinon Zinonos. 2021. Citizens' perception of smart cities: A case study. *Applied Sciences* 11, 6 (2021), 2517.

[27] Paolo Gerli, Luca Mora, Fabio Neves Da Rocha, and Huong Nguyen. 2024. World Smart Cities Outlook 2024. (2024).

[28] Jose Sanchez Gracias, Gregory S Parnell, Eric Specking, Edward A Pohl, and Randy Buchanan. 2023. Smart cities—a structured literature review. *Smart Cities* 6, 4 (2023), 1719–1743.

[29] Greg Guest, Kathleen M MacQueen, and Emily E Namey. 2011. *Applied thematic analysis*. sage publications.

[30] Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for dark patterns privacy harms? A case study on consent interactions. In *Proceedings of the 2022 symposium on computer science and law*. Association for Computing Machinery, New York, NY, USA, 181–194.

[31] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An empirical analysis of data deletion and {Opt-Out} choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 387–406.

[32] Waseem Haider, Justin D Martin, Ali Farooq, Joni Salminen, and Bernard J Jansen. 2025. The effect of religiosity and cultural conservatism on digital privacy concerns: A comparative longitudinal study of five Arab countries. *International Communication Gazette* (2025), 17480485251374883.

[33] SM Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. 2020. Privacy vulnerabilities in public digital service centers in Dhaka, Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*. Association for Computing Machinery, New York, NY, USA, 1–12.

[34] Scott Harper, Maryam Mehrnezhad, and John C Mace. 2020. User privacy concerns and preferences in smart buildings. In *International Workshop on Socio-Technical Aspects in Security and Trust*. Springer, Springer-Verlag, Berlin, Heidelberg, 85–106.

[35] Kris Hartley. 2023. Public perceptions about smart cities: Governance and quality-of-life in Hong Kong. *Social Indicators Research* 166, 3 (2023), 731–753.

[36] Franziska Herbert, Collins W Munyendo, Jonas Hielscher, Steffen Becker, and Yixin Zou. 2025. Digital Security Perceptions and Practices Around the World: A {WEIRD} versus {Non-WEIRD} Comparison. In *34th USENIX Security Symposium (USENIX Security 25)*. 1455–1474.

[37] Jose L Hernandez-Ramos, Juan A Martinez, Vincenzo Savarino, Marco Angelini, Vincenzo Napolitano, Antonio F Skarmeta, and Gianmarco Baldini. 2020. Security and privacy in internet of things-enabled smart cities: Challenges and future directions. *IEEE Security & Privacy* 19, 1 (2020), 12–23.

[38] Mahera Imam, N Manimekalai, S Suba, et al. 2025. From Data to Discrimination: Gender, Privacy, and the Politics of Digital Surveillance. *Synergy: International Journal of Multidisciplinary Studies* 2, 2 (2025), 52–64.

[39] Elvira Ismagilova, Laurie Hughes, Yogesh K Dwivedi, and K Ravi Raman. 2019. Smart cities: Advances in research—An information systems perspective. *International journal of information management* 47 (2019), 88–100.

[40] Jessica L Johnson, Donna Adkins, and Sheila Chauvin. 2020. A review of the quality indicators of rigor in qualitative research. *American journal of pharmaceutical education* 84, 1 (2020), 7120.

[41] Rob Kitchin. 2016. The ethics of smart cities and urban science. *Philosophical transactions of the royal society A: Mathematical, physical and engineering sciences* 374, 2083 (2016), 20160115.

[42] Ze Shi Li and Colin Werner. 2022. Ongoing Challenges and Solutions of Managing Data Privacy for Smart Cities. In *Smart Cities in Asia: Regulations, Problems, and Development*. Springer Nature Singapore Singapore, 23–32.

[43] Tianen Liu, Shuai Wang, Zheng Dong, Borui Li, and Tian He. 2025. From Perception to Computation: Revisiting Delay Optimization for Connected Autonomous Vehicles. *Comput. Surveys* 57, 8 (2025), 1–45.

[44] Freyja Lockwood. 2020. Bristol's smart city agenda: vision, strategy, challenges and implementation. *IET Smart Cities* 2, 4 (2020), 208–214.
[45] Kathleen M MacQueen, Eleanor McLellan, Kelly Kay, and Bobby Milstein. 1998. Codebook development for team-based qualitative analysis. *Cam Journal* 10, 2 (1998), 31–36.
[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), 527–544.
[47] Emile Mardacany. 2014. Smart cities characteristics: Importance of built environment components. In *IET Conference on Future Intelligent Cities*. IET, IET Conference on Future Intelligent Cities, 4.
[48] Deirdre K Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083 (2016), 20160118.
[49] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2023. " In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023 IEEE Symposium on Security and Privacy (SP), 570–587.
[50] National Centre for Universities and Business. 2016. *How Bristol is Open provides a platform for IoT innovation.* https://www.ncub.co.uk/insight/how-bristol-is-open-provides-a-platform-for-iot-innovation/ Accessed: 7 March 2026.
[51] Orange Business. 2023. *Orange Business to deliver Smart City Platform to optimize KAFD Smart City experience.* https://www.orange-business.com/en/press/orange-business-deliver-smart-city-platform-optimize-kafd-smart-city-experience Accessed: 7 March 2026.
[52] Anna Papaiakovou, Christina Nika, and Dimitrios D Vergados. 2022. E-Privacy Issues in the Smart Cities Environment. In *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*. IEEE, IEEE Computer Society, Los Alamitos, CA, USA, 1–7.
[53] Sunyup Park and Jessica Vitak. 2024. Who Gets Left Behind in the Push for Smart Cities? Insights from Marginalized Communities. In *International Conference on Information*. Springer, Springer-Verlag, Berlin, Heidelberg, 90–104.
[54] Visakha Phusamruat. 2022. The promise and challenges of privacy in smart cities: The case of Phuket. In *Smart Cities in Asia: Regulations, Problems, and Development*. Springer Nature Singapore Singapore, 65–77.
[55] Rini Rachmawati. 2020. Smart cities: Progress and challenge in establishing liveable cities. In *AUC 2019: Proceedings of the 15th International Asian Urbanization Conference, Vietnam*. Springer, Springer, Singapore, 307–316.
[56] Kopo Marvin Ramokapane, Caroline Bird, Awais Rashid, and Ruzanna Chitchyan. 2022. Privacy design strategies for home energy management systems (hems). In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15.
[57] S Sujith Roy and A Kannammal. 2019. PRIVACY CHALLENGES IN SMART SURVEILLANCE. *Emerging Technologies and Innovative Research (JETIR)* (2019), 104–106.
[58] SenseTime. n.d.. *King Abdullah Financial District Development & Management Company (KAFD DMC).* https://www.sensetime.com/en/case-detail?categoryId=51134285&gioNav=1 Accessed: 7 March 2026.
[59] Stefano Silvestri and Mario Ciampi. 2023. A Platform to Support the Implementation of Smart City Systems. *Institute of High Performance Computing and Networking (ICAR), National Research Council of Italy (CNR)* (2023).
[60] Liesbet Van Zoonen. 2016. Privacy concerns in smart cities. *Government Information Quarterly* 33, 3 (2016), 472–480.
[61] Aik Wirsbinna, Libor Grega, and Michael Juenger. 2023. Assessing factors influencing citizens' behavioral intention towards smart city living. *Smart Cities* 6, 6 (2023), 3093–3111.
[62] Fan Yang and Jian Xu. 2018. Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia & the Pacific Policy Studies* 5, 3 (2018), 533–543.
[63] Jingmin Yang, Trong-Yen Lee, and Wenjie Zhang. 2021. Smart cities in China: A brief overview. *It Professional* 23, 3 (2021), 89–94.
[64] Yujie Yuan, Shiqi Zhou, Xiaoyue Ji, Zhekang Dong, and Chun Sing Lai. 2025. A Critical Review on Technical Standards of Unmanned Aerial Vehicles in Smart Cities. In *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025 IEEE International Conference on Consumer Electronics (ICCE), 1–6.
[65] Wenxi Zhang, Sharanya Shanmugam, and Jason Grant Allen. 2025. Comparing smart city data protection approaches: digital consent and the accountability framework in Singapore. *International Data Privacy Law* 15 (2025), 48–6.

.1 Positionality

As a multi-disciplinary research team, we recognise that our backgrounds, identities, and professional experiences shape how we designed this study, interpreted participants' accounts, and represented their perspectives.

Researcher A was born and raised in Saudi Arabia and identifies as Saudi. As a bilingual Arabic-English speaker who has lived in both the Kingdom of Saudi Arabia and the United Kingdom, they conducted the interviews and led the initial stages of data analysis. We believe that their linguistic fluency and cultural familiarity enabled deeper engagement with participants' narratives, particularly in recognising implicit cultural references, social norms, and contextual nuances around trust, consent, and authority in both settings. At the same time, they acknowledge that their own position as a Saudi citizen and as a researcher currently based in the UK may have influenced participants' comfort levels in discussing institutional power, surveillance, and data governance, and also shaped the interpretations they brought to the analysis. Researcher B is a system-security specialist with extensive experience in privacy-related research. They informed the study design, particularly in framing questions around data flows, infrastructures, and the technical realities of data collection in smart cities. We recognise that their perspective can highlight threat models that may differ from how residents themselves think about privacy or control. Researcher C is an expert in usable security with many years of experience conducting user studies on security, privacy, and HCI. They helped to shape the methodological decisions of the study, including interview protocol, and the interpretation of residents' understandings of user perceptions of data practices.

A Screening Questionnaire

Q1. Which of the following best describes your connection to the area?

Bristol

- I live in Bristol
- I work in Bristol
- I regularly visit Bristol
- None of the above

KAFD in Riyadh

- I live in KAFD
- I work in KAFD
- I regularly visit KAFD
- None of the above

Q2. How long have you been connected to this area?

- Less than 6 months
- 6–12 months
- 1–3 years
- 4+ years

Q3. Which of the following have you personally used or encountered in this area? (Select all that apply)

- Smart access systems (badges, facial recognition, gated entry)
- CCTV or monitored public spaces
- Energy and water smart meters
- Smart parking or traffic systems
- Public Wi-Fi or city apps
- Smart buildings (energy, lighting, climate control)
- Environmental sensors (air quality, noise, heat)
- None of the above

Q4. Which types of data do you think cities may collect about residents? (Select all that apply)

- Location or movement data
- Transportation usage
- Energy or water usage
- Video or images in public spaces
- Personal or demographic information
- I am not sure

Q5. Overall, how do you feel about data being collected in this area to support city operations or services?

- Very positive
- Somewhat positive
- Neutral
- Somewhat negative
- Very negative

Q6. Some people classify their cities as smart cities, what makes a city a "smart city"?

- _____

Q7. What technologies do you think makes a city a "smart city"?

- _____
- _____
- _____

Q8. How comfortable are you with this data being shared between organizations involved in managing the area (e.g., city authorities, developers, service providers)?

- Very comfortable
- Somewhat comfortable
- Neutral
- Somewhat uncomfortable
- Very uncomfortable

Q9. What is your age range?

- 18–24
- 25–34
- 35–44
- 45–54
- 55–64
- 65+
- Prefer not to say

Q10. How do you describe your gender?

- Woman
- Man
- Prefer to self-describe: _____
- Prefer not to say

Q11. What is the highest level of education you have completed?

- Secondary school or equivalent
- Diploma / vocational training
- Bachelor's degree
- Master's degree
- Doctorate
- Prefer not to say

Q12. Are you willing to take part in a 45–60 minute interview about your experiences and views?

- Yes
- No

If your answer is "YES," please provide your email so that we can contact you to arrange an interview session: _____

B Interview Protocol

Hello, thank you for taking the time to participate in this interview.

With your permission, I will record this interview to ensure the accuracy of your responses. The recording will be securely stored and only accessible to the research team. If at any point you feel uncomfortable, please let me know, and we can stop the recording or the interview altogether.

Before we begin, can you confirm that you have read and signed the consent form? Do you have any questions or concerns about the consent form or the interview process before we start?

Great, if you are ready, we can begin the interview now.

RQ1: What is users' understanding of smart cities?

- What does 'smart' mean when it comes to technology?
  - **Prompt** In terms of smart technology like cars, lights, roads, and homes?
- Would you say you live in a smart home?
- If they live in a smart home
  - **Follow-up:** What smart device do you use?
- What is a smart city?
- What are the benefits of living in Smart Cities?
- What services/platforms/devices can be found in Smart Cities?
- What services/platforms/devices in Smart Cities do you use?
- Who do you think is responsible for implementing and maintaining Smart Cities?

RQ2: Users' perceptions and understanding of data collection and sharing in smart cities

Data types.

- What data do you think is collected around smart cities?
- Which data do you think should not be collected in a smart city?
  - **Follow-up:** What are your reasons?
- What personal data is collected in the smart city?
  - **Prompt:** What examples of personal data are collected in a smart city?
  - **Follow-up:** Do you consider this data sensitive?
  - **Follow-up:** What are your reasons for considering these data sensitive?
  - **Follow-up:** If I explain how sharing this data can improve your service, would you reconsider sharing it?
- What data types can be considered appropriate to share within a smart city environment?

Collector.

- Who collects these data?
- **Follow-up:** How collects and shares these data?
- What are the reasons for collecting these data?
- Who should not have collected these data?
  - **Follow-up:** What is your reason for saying that?

Benefits and concerns.

- What are your benefits and concerns about collecting and sharing data in Smart Cities?

Location.

- Where is this data stored?

Data retention.

- How long is the data kept?

Recipients.

- Who do you think these data are shared with?
  - **Follow-up:** Is there any specific reason for saying that?
- Who should not have access to these data?
  - **Follow-up:** What is your reason?
  - **Follow-up:** Who do you think sharing your data with without your consent is reasonable?

RQ3: Users' perceptions about consent in smart cities

Consent.

- What do you think about data consent around smart cities?
- How should consent be collected in smart cities?
- How should people withdraw their consent in the smart city?
- Can you list some examples or situations where you think you should provide consent for your data to be used in a smart city?
- Do you feel that your consent was used against you?
  - **Follow-up:** How do you think that happened?
- What do you think will improve the consent in smart cities? We are finished. Thank you very much for your time.

C Final Codebook

Table 2: Summarized codebook

Sub-theme	Description	Example Quotes
Smart cities as automated and connected	Smart cities viewed as automated environments where systems, sensors, and AI operate without human input.	"Automated processes... things happen without people interfering." (P5_UK); "Technology... multitasking... self-operated." (P8_KSA)
Time-saving and improved quality of life	Smart cities perceived as efficient, fast, convenient, and improving lifestyle and comfort.	"One hour becomes five minutes in a smart city." (P4_KSA); "More sustainable and healthier to live in." (P4_UK)
Awareness and familiarity varies	Some participants knew they lived in a smart city; others were uncertain or confused about what makes a city smart.	"I didn't have any idea… what kind of data it's collecting." (P1_UK); "I'm having trouble visualising the data being pulled…" (P3_KSA)
Contrast with traditional cities	Traditional cities seen as manual, slow, and less organised compared to automated, efficient smart cities.	"Traditional cities rely on people to do things." (P5_UK); "Do everything manually." (P10_KSA)
Contextual differences (UK vs KSA)	Differences in awareness, examples used, and views on responsibility. KSA = infrastructure and automation; UK = service-based and assistance-oriented.	"Systems learn behaviour and adapt." (P9_KSA); "Intuitive technology that helps with tasks." (P3_UK)
Widespread data collection	Participants believe data is collected via sensors, CCTV, apps, Wi-Fi, access systems; seen as essential for smart-city functioning.	"Sensors… collect a lot of data." (P3_UK); "Cameras can detect if you're on your phone." (P7_UK)
Perceived reasons for data collection	Data used for safety, security, service improvement, planning, automation, and efficiency.	"CCTV… keeping crime to a minimum." (P6_UK); "More security for people… I don't have to worry." (P8_KSA)
Who participants think collects data	KSA: government or city operator. UK: multiple entities such as council, police, universities, private providers.	"The government… collects data." (P11_KSA); "I assume the council or government collects the data." (P8_UK)
Who should access data	Generally acceptable for authorised entities if there are perceived benefits; strong concerns about private companies.	"If I knew the benefits… yes they can." (P5_UK); "Government only… commercial companies no." (P8_KSA)
Sensitive data should not be collected	Non-personal data seen as acceptable; personal, biometric, financial, and identification data viewed as sensitive.	"Foot traffic… is fine." (P3_UK); "Photos or ID… my personal data." (P1_KSA)
Understanding of processing	Data believed to flow automatically; KSA = centralised, UK = dispersed and uncertain.	"It goes to one place to the government." (P7_KSA); "Who even sees it?" (P8_UK)
Security concerns	Fear of hacking, misuse, or exploitation of personal data.	"Somebody may try hacking into my account." (P6_KSA); "Used for not so good things." (P5_UK)
Privacy concerns	Worry about leakage of images, health, finances, or personal information.	"Data may be leaked… personal images used." (P3_KSA); "I wouldn't want to share… health stuff." (P5_UK)
Data-driven control concerns	Concerns about profiling, manipulation, behavioural influence.	"Someone controlling everything." (P2_UK); "Influence opinion as well." (P3_KSA)
Gendered/cultural privacy (KSA only)	Concern about capturing women's images and negative impacts on social norms or opportunities.	"Many girls don't want to be photographed." (P6_KSA)
Family-data sensitivity (KSA only)	Family-related information seen as highly sensitive.	"I can't imagine family members' data being collected." (P5_KSA)
Limited awareness of storage	Participants unsure where data is stored and describe a "black box" system.	"I have no idea where data is stored." (P4_KSA)
Unclear or indefinite retention	Data believed to be stored indefinitely or for many years.	"Maybe forever…" (P4_KSA); "Many years to forever." (P5_UK)
Perception that data cannot be deleted	Participants assume deletion is impossible.	"They wouldn't delete the data." (P8_UK)

Table 3: Codebook: Perceptions around Consent and Control in Smart Cities

Sub-theme	Description	Example Quotes
Consent is important	Consent seen as necessary for understanding what data is collected and why.	"Consent would improve information about data collection." (P1_UK)
Consent not actively sought	Consent is implicit, assumed, and rarely requested.	"Consent... absent." (P3_UK); "If you are in City B, it's automatic." (P1_KSA)
Low sense of control	Participants feel no ability to change or influence data collection or use.	"You can't change anything." (P10_KSA); "We can't control what they take." (P8_UK)
Control structurally impossible	Sensors embedded in infrastructure make opting out infeasible.	"Being part of infrastructure means you can't avoid it." (P7_UK)
Desire for awareness	Participants want greater transparency and understanding of data collection and sharing.	"They should raise awareness… how they gonna use it." (P10_KSA)
Who should seek consent	Responsibility should lie with government, councils, city operators, or service providers.	"The government… should tell us." (P11_KSA); "The City Council should tell me." (P5_UK)
Digital consent mechanisms	Preference for apps, emails, digital interfaces, and unified systems.	"It should be an app accessible to everyone." (P1_UK)
Offline consent mechanisms	Support for paper forms, mail, signage, and contextual consent.	"Send us mail in the post." (P1_UK); "Put a sign… capturing your data." (P7_KSA)
Desire to withdraw consent	Participants want ability to revoke consent, though many view it as technically impossible.	"Allow me to withdraw my information." (P5_UK); "There's no way to say no." (P7_UK)