AI Surveillance Technologies in Smart Cities: Privacy Calculus versus Privacy Paradox

Inga Stankevice and Aaiyushi Baid
School of Economics and Business, Kaunas University of Technology, Lithuania

inga.stankevice@ktu.lt
aaiyushi.baid@ktu.edu

Abstract: Smart cities represent the convergence of technological innovation and urban development, aiming to enhance efficiency, safety, environmental sustainability, and overall well-being through interconnected systems, sensors, and digital devices. At the heart of these innovations lies the deployment of AI-powered surveillance technologies, which contribute to monitoring and managing urban environments more effectively. While such systems promise improvements in security and operational efficiency, they also raise pressing concerns about individual privacy and data security. This study examines the tension between technological progress and privacy preservation in AI-based surveillance systems, focusing on how citizens from seven smart cities perceive and respond to these technologies. Drawing on a quantitative pilot survey conducted in seven smart cities and using a five-dimensional framework of privacy concerns, this paper maps citizen attitudes towards AI surveillance technologies. These are cross-analysed against seven distinct categories of AI surveillance technologies deployed in public spaces. A central question of the analysis is whether individuals' responses reflect the privacy calculus – a rational evaluation of risks and benefits, or are more consistent with the privacy paradox, where expressed concerns do not translate into protective behaviours, often due to insufficient awareness or a lack of options to opt out. In addition to assessing the overall levels of privacy concern, the study ranks five privacy dimensions based on the degree of concern they elicit and evaluates which types of AI surveillance technologies are most and least acceptable when privacy is factored into the adoption equation. We further introduce a privacy-weighted adoption attractiveness metric to measure public receptivity of the seven types of AI surveillance technologies. The findings, derived through descriptive statistical methods, reveal trends and peculiarities across the cities and the respondents' demographic characteristics, such as gender, education level, and age. These insights contribute to a more nuanced understanding of how privacy values interact with the promises of AI surveillance in smart cities.

Keywords: AI surveillance, Privacy concern, Privacy paradox, Privacy calculus, Smart city, Technology adoption

1. Introduction

Smart cities integrate advanced technological infrastructure with data analytics to enhance urban services and infrastructure. These cities leverage information and communication technologies to optimise public services, minimise environmental impact, and improve citizens' well-being (Humayun et al. 2019). As part of this broader digital transformation, artificial intelligence (AI) surveillance technologies have emerged as key enablers supporting real-time monitoring, analysis, and decision-making in traffic control, public safety, or emergency response (Kalenyuk et al. 2023; Sarp et al. 2024).

Defined as applications that utilise artificial intelligence to monitor, analyse, and manage the data "related to individuals or groups, often for security, law enforcement, or governance purposes" (Lyon 2018), AI surveillance technologies encompass a diverse set of tools designed to interpret and respond to dynamic urban scenarios: facial recognition, crowd detection, anomaly tracking, object recognition, and more. However, as these technologies become increasingly integrated into everyday urban systems, they give rise to growing concerns around individual privacy and data protection (Bibri & Allam 2022; Karwatzki et al. 2022; Ooijen et al. 2022; Pronzato & Markham 2023; Sampaio et al. 2023).

In smart cities, continuous monitoring often leaves individuals with limited choice to opt out (Pronzato & Markham 2023), and the aggregation of data across platforms increases the risk of privacy violations (Naik & Jenkins 2020; Tan et al. 2023). These risks are further intensified by issues such as deepfake abuse, non-consensual data harvesting, data poisoning, misuse and lack of transparency in data governance (Johnson 2023; Sanchez et al. 2024).

Against this backdrop, this paper investigates how citizens in smart cities perceive and respond to AI surveillance technologies. It explores the balance between technological promise and perceived privacy risk through a structured survey grounded in the five-dimensional privacy model (Martínez-Ballesté et al. 2013; Machín et al. 2021; Solanas et al. 2021), as well as two behavioural frameworks – privacy calculus and privacy paradox. By identifying which dimensions of privacy concern are most salient and how they influence public receptivity to AI surveillance, the study aims to provide a deeper understanding of how privacy values shape the present and future of smart urban governance.

2. Theoretical Background

2.1 The 5D Privacy Model and Associated AI Surveillance Technologies

We employ the 5D privacy model for structuring and operationalising the concept of privacy. The model was originally proposed by Martínez-Ballesté et al. (2013) and remains conceptually influential in recent scholarship (Machín et al. 2021; Solanas et al. 2021) as a structured categorisation of privacy risks in AI-enabled urban systems.

The framework recognises that privacy is a set of overlapping concerns, where each is linked with a spectrum of AI surveillance technologies:

- Identity privacy concerns the protection of personal identifiers such as names, facial biometrics, or other uniquely identifying attributes. Breaches in this dimension can result in profiling, loss of anonymity, and pervasive surveillance (Naik & Jenkins, 2020; Tan et al., 2023). AI technologies that most directly challenge identity privacy include facial recognition, object detection and tracking, crowd detection, anomaly detection, IoT systems, and smart policing.
- Query privacy, which refers to the confidentiality of user inputs and behavioural queries, is particularly at risk when AI systems collect and analyse searches, voice commands, or service interactions. This dimension is closely associated with IoT environments and predictive policing systems, where such data may be used without explicit consent (Tan et al., 2023).
- Location privacy involves the right to anonymity in physical movement and the protection of spatial data from tracking. It is jeopardised by surveillance tools that collect GPS or transit data, including traffic management systems, as well as the technologies linked to identity privacy (Sampaio et al., 2023).
- Footprint privacy relates to digital traces left behind through system usage, such as energy consumption or access logs, which may be aggregated to construct behavioural profiles. All aforementioned AI technologies, except crowd detection, which typically does not involve long-term data retention, pose risks to footprint privacy through persistent and often opaque data collection (Zuboff, 2019; Sanchez et al., 2024).
- Ownership privacy addresses individuals' and institutions' ability to retain control over their data, especially when shared across interconnected infrastructures. In smart cities, IoT platforms and smart policing systems present the most critical challenges to this form of privacy, as data often crosses institutional boundaries with limited oversight.

This dimensional approach aligns with Nissenbaum's (2009) principle of contextual integrity, which stresses that privacy is not absolute but depends on the appropriateness of information flows within specific contexts. For instance, violations of identity or ownership privacy are often perceived as more severe precisely because they breach prevailing social norms around data control and transparency. Building on the dimensional understanding of privacy provided by the 5D model, the concepts of privacy calculus and privacy paradox offer behavioural perspectives on how individuals navigate the trade-offs and contradictions inherent in AI-surveilled smart city environments.

2.2 Behavioural Perspectives Towards Privacy Concerns

2.2.1 Privacy calculus

The privacy calculus theory posits that individuals assess the perceived risks and benefits of data disclosure in a rational, situational manner (Chen et al. 2024). In smart cities, for instance, users may accept facial recognition if it improves safety, or, more often than not, they agree to GPS tracking if it optimises transportation. However, critics argue that the approach oversimplifies privacy behaviour by assuming an entirely rational choice, which is often impossible in complex data ecosystems. For instance, Karwatzki et al. (2022) identify multiple dimensions of privacy risks that users may not fully comprehend or consider. Similarly, Pronzato and Markham (2023) state that despite increased consciousness, individuals struggle to overcome subalternity and make concrete behavioural changes. Hence, even though people are aware of surveillance and privacy risks, they still feel powerless to resist, opt out, or change behaviour because systems are too embedded, opaque, or coercive. Additionally, Ooijen et al. (2022) introduce the concept of privacy cynicism – an attitude of frustration and hopelessness that can moderate how people appraise and respond to privacy threats, which also aligns well with the explanation of subalternity by Pronzato and Markham (2023). As a result, privacy calculus may underestimate the role of emotion, habituation, or structural coercion in shaping privacy behaviour. Taken

together, these critiques resonate with Cavoukian's et al. (2010) Privacy by Design principle, which argues that privacy should not rely on individual decision-making alone but must be built directly into technological and organisational infrastructures.

2.2.2 Privacy paradox

The privacy paradox refers to the disconnect between individuals' stated concerns about privacy and their actual behaviours (Kokolakis 2015; Larson 2023). In smart cities, this paradox is intensified: despite expressing discomfort, residents frequently interact with surveillance systems embedded in transit, lighting, and public services, often without awareness or consent (Naik & Jenkins 2020; Bibri & Allam 2022; Tan et al. 2023). Interestingly, the privacy paradox may not be solely attributed to user laziness, as previously thought: a study on Facebook users (Whelan et al., 2024) found that a person's external locus of control provides a stronger explanation for the privacy paradox than laziness. In addition, limited opt-out options (Pronzato and Markham 2023), institutional opacity, and normalisation of surveillance culture (Tan & Zhao 2003; Sundquist 2023) contribute to passive compliance (Zuboff 2019). From the perspective of contextual integrity (Nissenbaum 2009), this contradiction can be interpreted as a breakdown of transparency and appropriateness in information flows: people comply with surveillance not because they accept it, but because imposed data practices prevent them from exercising meaningful choice. Trust in government institutions may further suppress dissent, especially when surveillance is framed as essential for safety or public service (Sanchez et al. 2024). Emotional responses, such as fear or joy, can override rational privacy concerns, creating a structural contradiction between privacy values and the use of technology.

3. Methodology

3.1 Research Design

This study employs a quantitative descriptive research design to: 1) explore citizens' levels of concern about the adoption of AI surveillance technologies in smart cities, including the segmentation by age, gender, educational level; 2) identify the type of dominating response to privacy concerns; 3) rank the five privacy concern dimensions; 4) compute the attractiveness of 7 AI surveillance technologies.

3.2 Survey Instrument

A theoretically grounded framework, informed by the 5D privacy model, privacy calculus, and privacy paradox, was used to develop the survey instrument. Each dimension of the 5D privacy model was operationalised through five Likert-scale statements, rated from 1 (strongly disagree) to 5 (strongly agree). These dimensions were designed to reflect specific ways in which AI surveillance technologies infringe upon individual informational autonomy.

In addition to the 5D privacy framework, the questionnaire incorporated two theoretically informed constructs – privacy calculus and privacy paradox (four statements each, same Likert scale). To contextualise the results, the questionnaire also included four demographic questions, prompting respondents to indicate their age group, gender, highest level of education attained, and current city of residence. These variables enabled subgroup comparisons and provided insight into how demographic factors might shape privacy perceptions in smart cities.

The survey statements were derived from the literature and aligned with the conceptual definitions as demonstrated in Table 1.

Table 1: Survey constructs, dimensions, and conceptual justification

Construct	Dimension	Number of items	Theoretical basis
5D privacy model	Identity Privacy	5	Machín et al. (2021) Solanas et al. (2021) Martínez-Ballesté et al. (2013)
	Query Privacy	5	
	Location Privacy	5	
	Footprint Privacy	5	
	Owner Privacy	5	
Privacy-related behaviour	Privacy calculus	4	Chen et al. (2024) Karwatzki et al. (2022)
	Privacy paradox	4	Kokolakis (2015)

Construct	Dimension	Number of items	Theoretical basis
			Larson (2023)
Demographics	Age, gender, education, city	4	Used for subgroup comparison and segmentation

3.3 Sampling and Data Collection

The survey was disseminated through social professional networks using a convenience sampling approach. Participation was voluntary and anonymous, with no identifying information collected. Data were gathered over ten days from April 23 to May 3, 2025. A total of 72 responses were obtained from individuals residing in cities listed in the IMD Smart City Index (2024). The reported cities include Dubai, Copenhagen, Helsinki, Hamburg, Munich, Berlin, and Barcelona. While rankings vary, all cities are recognised within the IMD Index as participants in the global smart city landscape, making them relevant for this study's focus on AI surveillance and privacy attitudes and enabling the examination of privacy concerns across various smart city contexts.

Based on the combined population of the surveyed cities, the total estimated urban population is approximately 14.7 million. Given the sample size of 72 respondents, the calculated margin of error is ±11.6% at a 95% confidence level, assuming maximum variability in responses (Memon et al. 2020). On a 5-point Likert scale, this corresponds to approximately ±0.58 points. While this level of precision limits the generalisability of findings to the broader population, it is appropriate for exploratory research aiming to identify patterns related to privacy perceptions in smart cities. In addition, differences between group means or privacy dimensions that exceed the margin of ±0.58 points can be considered potentially meaningful.

3.4 Data Analysis

Descriptive statistical analysis and insights were obtained using Microsoft Excel's PivotTable and Analyse Data functionalities. For the validity analysis, Python programming was employed using Visual Studio Code. To assess how privacy concerns influence public receptivity to specific AI surveillance technologies, a privacy-weighted adoption attractiveness score was computed in Excel. This measure estimates citizens' willingness to accept various AI technologies deployed in smart cities, taking into account the intensity of privacy concerns associated with each.

Each AI surveillance technology was mapped to the privacy dimensions it affects (as outlined in section 2.1). The privacy score for each technology P_n was calculated by summing the mean concern scores for only those privacy dimensions that were impacted by that specific technology:

$$P_n = \sum_{i \in D_n} \mu_i \tag{1}$$

, where

P_n – privacy score for AI surveillance technology *n*,

D_n – the set of AI surveillance dimensions affected by technology *n*,

μ_i – the mean concern score for privacy dimension *i*.

Next, the privacy score for AI surveillance technology was scaled against the theoretical maximum P_{max}, which equals 25, assuming all five dimensions are rated at the maximum score of 5. The resulting score was inverted and expressed as a percentage to represent the relative attractiveness of each technology from a privacy-sensitive standpoint:

$$A_n = \left[1 - \frac{P_n}{P_{max}}\right] \times 100 \tag{2}$$

, where

A_n – privacy-weighted adoption attractiveness of AI surveillance technology T_n,

P_n – privacy score for AI surveillance technology *n* as calculated in equation (1),

P_{max} – maximum possible privacy impact score, representing the worst-case scenario in which all five privacy dimensions are affected with the highest concern level.

This method enabled the ranking of AI surveillance technologies based on their perceived privacy burden. In addition to the sum-based approach, an average-based method was applied to evaluate the intensity of privacy concern per affected dimension. Rather than summing the mean concern scores, this approach calculates the average concern across only the dimensions impacted by each technology:

$$A_n^{adj} = \left[1 - \frac{\sum_{i \in D_n} \mu_i}{|D_n| \cdot 5}\right] \times 100 \quad (3)$$

, where

$A^{adj}{}_n$ – privacy-weighted adoption attractiveness of technology *n*, adjusted by the number of privacy dimensions it impacts,

$\sum_{i \in D_n} \mu_i$ – privacy concern score across affected dimensions (equals P_n in equation (1)),

|Dn| · 5 – maximum possible total score if all affected dimensions had the highest possible concern, i.e., 5.

The comparison of the results using both methods enables a complementary interpretation of public sensitivity, capturing whether a technology is perceived as broadly intrusive (sum-based) or intensely concerning in specific areas (average-based).

3.5 Results

3.5.1 Descriptive statistics

As shown in Table 2, the highest level of concern was observed in the identity privacy dimension (M = 4.628, SD = 0.263), followed closely by owner privacy (M = 4.594, SD = 0.336) and location privacy (M = 4.324, SD = 0.459). In contrast, concern for query privacy was markedly lower (M = 3.333, SD = 0.526), suggesting that search- or inquiry-related monitoring is perceived as less invasive.

Table 2: Descriptives of privacy concerns and responses to them

Theoretical construct	Composites	Mean	Standard deviation
Privacy concern	identity	4.628	0.263
	query	3.333	0.526
	location	4.324	0.459
	footprint	3.819	0.442
	ownership	4.594	0.336
Response to privacy concern	calculus	2.993	0.496
	paradox	4.038	0.76

These findings align well with recent findings. As evidenced by the growing demand for data and digital sovereignty (Tan et al. 2023), people are increasingly protective of control over their digital assets. This is also reflected in the development of technologies like Self-Sovereign Identity (SSI) systems, which offer users entire control over their personal data (Naik & Jenkins 2020). Similarly, a survey-based study on AI and geolocation/video data collection risks (Sampaio et al. 2023) highlights that surveillance technologies accessing identity traits are perceived as most intrusive. Contrarily, when inquiry-related monitoring is perceived as a regular part of the organisational culture (Tan & Zhao 2003) or is normalised through routine exposure and habitual use (Sundquist 2023), it may be seen as less invasive. In addition, citizens view search or anonymised data collection as less threatening, particularly when spatial or identity elements are absent (Johnson 2023).

Composite construct scores reflected distinct patterns. The privacy paradox construct yielded a high mean score (M = 4.038, SD = 0.760), indicating that many respondents acknowledged the discrepancy between their stated concerns and their actual behaviour. In contrast, the privacy calculus construct averaged near the midpoint of the Likert scale (M = 2.993, SD = 0.496), suggesting ambivalence or weak endorsement of rational risk-benefit trade-offs.

3.5.2 Scale reliability

When treated as a single composite construct, the set of 25 items measuring the five privacy dimensions yielded a Cronbach's alpha of 0.718. This indicates acceptable internal consistency for exploratory purposes and suggests that, despite variation in individual items, the overall construct of "privacy concern" was interpreted coherently by respondents as a multi-faceted but unified experience.

The two theoretical constructs appended to the privacy dimensions exhibited diverging reliability patterns. The privacy calculus scale produced a low Cronbach's alpha of 0.135, reflecting poor internal consistency. This supports theoretical critiques that the rational trade-off model becomes unrealistic in complex technological environments (Ooijen et al. 2022; Pronzato & Markham 2023), such as smart cities, where citizens may lack the information to weigh privacy risks against perceived benefits consciously (Karwatzki et al. 2022). Thus, rather than reflecting a failure in survey design alone, the low alpha may signal the conceptual fragility of applying the calculus model in highly interconnected AI-driven urban contexts.

By contrast, the privacy paradox scale demonstrated strong internal reliability, with Cronbach's alpha of 0.823. This suggests that the construct was internally coherent and easily recognisable to respondents, likely because it captures a behavioural contradiction (concern vs. action) that individuals routinely encounter (Sundquist 2023). The high reliability of this scale supports its conceptual validity and relevance in assessing public responses to AI-enabled surveillance.

3.5.3 Demographic subgroup comparisons

Descriptive comparisons of privacy concerns across education levels are visualised in Figure 1.

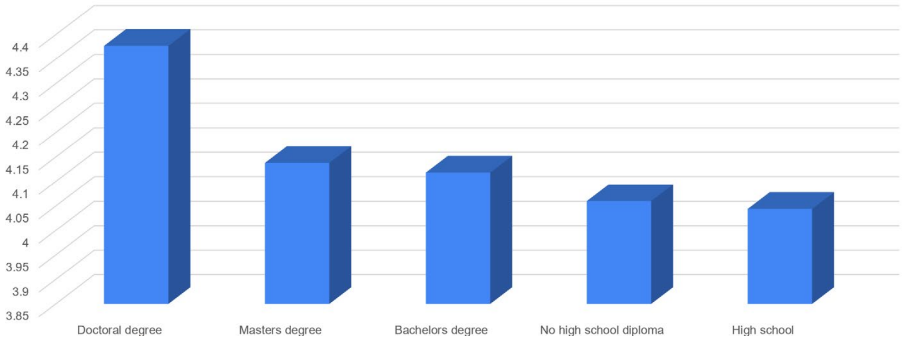

Figure 1: Average privacy concern across education levels

Respondents with doctoral degrees reported the highest average concerns across most dimensions, particularly in location privacy (M = 4.54) and ownership privacy (M = 4.77). Individuals without a high school diploma also showed high concern in identity privacy (M = 4.90) and ownership privacy (M = 4.90), but scored lower on query privacy (M = 2.70). The statistics revealed several differences in privacy behaviour as well, as shown in Figure 2.

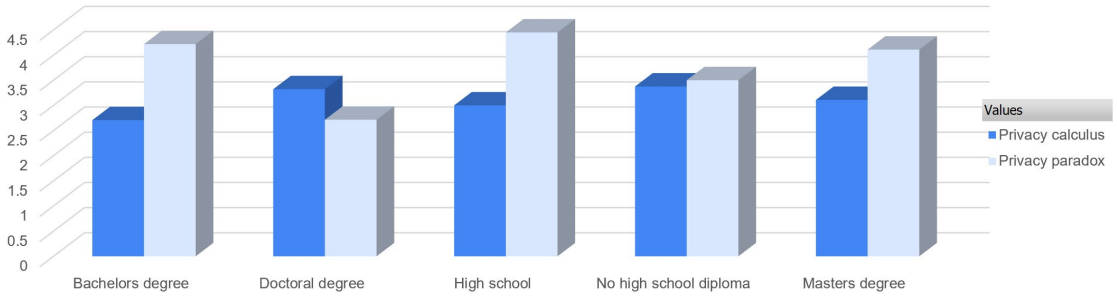

Figure 2: Average response to privacy concerns across education levels

The privacy calculus score was highest among the less-educated groups (M = 3.38) and lowest among those with a bachelor's degree (M = 2.71). The privacy paradox showed the opposite pattern: strongest among high school graduates (M = 4.45), but weaker among PhD holders (M = 2.71), possibly indicating more self-consistency in behaviour among highly educated individuals.

In terms of gender distribution, the survey sample consisted of 53% female and 47% male respondents, with no participants identifying as another gender. The gender-based comparison did not reveal any strong patterns in

privacy concerns. The gender gap is small, but it favours higher privacy concerns among males (M = 4.16 vs. M = 4.12). This result reverses the common pattern observed in some prior literature, where females are typically more concerned with privacy (Le et al. 2024).

Privacy paradox scores were also nearly identical across genders, suggesting a shared level of ambivalence regarding benefit-risk trade-offs. Males reported a greater degree of privacy paradox (M = 4.15) compared to females (M = 3.94). Similarly, the privacy calculus score was also higher among males (M = 3.11) than female respondents (M = 2.89). The results suggest that males in the sample were both more aware of behavioural contradictions and more likely to engage in privacy-related decision-making processes.

The differences across the surveyed age groups are minimal, as observed in Figure 3.

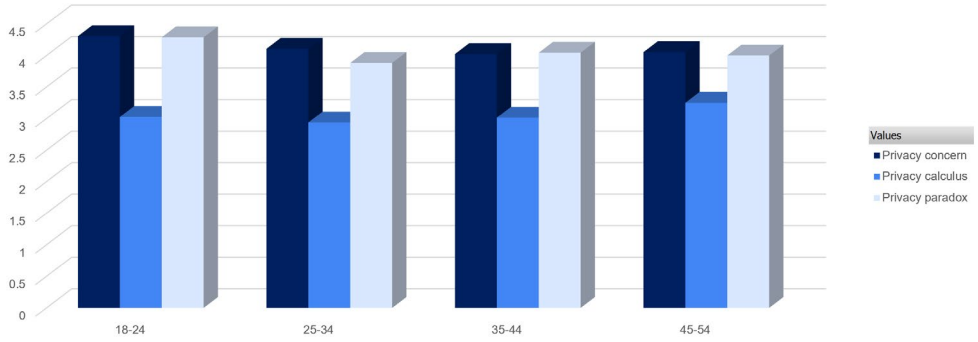

Figure 3: Average privacy concern and response to it across age groups

Respondents in the 18-24 age range reported the highest overall privacy concerns, particularly in identity (M = 4.72) and location privacy (M = 4.44). These findings suggest that younger respondents may be most sensitive to privacy concerns and more likely to experience cognitive dissonance, i.e., the privacy paradox. In contrast, other respondents may be more accepting or less aware of the privacy implications of AI surveillance in smart cities. However, the differences are negligible.

3.5.4 Privacy-weighted attraction of adoption of AI surveillance technologies

Privacy-weighted adoption attractiveness scores vary substantially across the AI surveillance technologies, depending on both the breadth and intensity of privacy concerns. The results are summarised in Table 3.

Table 3: Privacy-weighted attraction of adoption of AI surveillance technologies

Technology	Affected Dimensions	Sum concern	Average privacy concern	Sum-based attractiveness	Average-based attractiveness
Facial recognition	Identity, location, footprint	12.768	4.256	48.9%	14.9%
Internet of Things	Identity, query, location, footprint, ownership	8.903	4.451	17.2%	17.2%
Object detection and tracking	Identity, location, footprint	11.428	3.809	48.9%	14.9%
Smart policing systems	Identity, query, location, footprint, ownership	8.141	4.071	17.2%	17.2%
Crowd detection and recognition	Identity, location	3.333	3.333	64.2%	10.5%
Anomaly detection	Identity, location, footprint	13.225	4.408	48.9%	14.9%
Traffic management systems	Location, footprint	12.236	4.079	67.4%	18.6%

As can be observed, traffic management systems, which are associated with location and footprint privacy, achieved the highest adoption attractiveness in the sum-based model (67.6%), reflecting their relatively narrow

scope of privacy intrusion. In the average-based model, their attractiveness dropped to 18.6%, but still remains the highest.

By contrast, Internet of Things and smart policing systems triggered concern across all five privacy dimensions, resulting in the lowest attractiveness scores in the sum-based model. These technologies represent the broadest potential for privacy intrusion from the perspective of the affected privacy dimensions, leading to the strongest perceived resistance. However, leveraged by the number of affected dimensions, their attractiveness is one of the highest, i.e., 17.2% in the average-based model.

Facial recognition, object detection, and anomaly detection affected three high-sensitivity dimensions each – identity, location, and footprint – and received identical scores of 48.9% (sum-based) and 14.9% (average-based). Crowd detection, which affects identity privacy and location privacy, scored relatively high in the sum-based model (64.4%), but dropped to 10.5% in the average-based model due to the elevated concern associated with these two specific dimensions.

4. Conclusion

The identified distinction between concern levels implies that not all forms of privacy concern are given equal weight. Among all the investigated privacy dimensions, identity and ownership privacy are the most concerning, indicating that individuals are most vulnerable to risks that compromise their control over personal data. In contrast, query privacy emerged as the least concerning, likely due to the habituation in digital interactions or insufficient awareness of more subtle forms of data profiling. These findings are consistent with recent scholarly literature on digital sovereignty and the normalisation of surveillance.

The findings contribute to the behavioural understanding of privacy dynamics and highlight the more substantial presence of the privacy paradox, compared to relatively low endorsement of privacy calculus. This suggests that while people express strong privacy concerns, their behaviours do not always align, which is driven by limited alternatives, perceived inevitability, and structural constraints. The low internal consistency of the privacy calculus scale further supports the critique that rational trade-off models, more often than not, fail in highly integrated urban systems.

Demographic subgroup comparisons provide little additional granularity to the aforementioned conclusions and largely follow the general patterns of privacy concern and response to it. The characteristic which most stands out is the educational background. While concern about privacy is present across all educational levels, the rational trade-off logic of privacy calculus is more accepted by the least and most educated respondents. In contrast, middle-educated groups more commonly acknowledge paradoxical behaviour. Another interesting finding is that male respondents expressed marginally higher concern and greater recognition of paradoxical behaviour. This finding challenges conventional trends in privacy literature, which typically suggest that women are more likely to exhibit paradoxical privacy behaviour.

Regarding the privacy-weighted adoption attractiveness of AI surveillance technologies, traffic management systems scored highest, indicating broad public support. At the same time, IoT and smart policing technologies were perceived as the most intrusive, particularly when the number of affected privacy dimensions is not adjusted for. A key insight here is the distinction between the breadth of privacy impact and the depth of concern associated with specific dimensions. Thus, IoT affects many dimensions, but the intensity of concern across them is more distributed, resulting in relatively higher adjusted attractiveness. Conversely, crowd detection, despite affecting fewer dimensions, targets those associated with the high privacy concerns. As a result, although crowd detection ranks second in unadjusted attractiveness, it becomes the least attractive option when the concern level of affected dimensions is taken into account.

Taken together, the findings suggest that the privacy paradox remains a dominant lens for interpreting public responses; however, structural theories, such as contextual integrity, highlight why specific dimensions are more significant. From a practical perspective, embedding Privacy by Design principles into AI surveillance systems would help address paradoxical behaviours, build trust, and ensure that smart city innovation does not come at the expense of citizens' autonomy.

The study opens several avenues for further research. For instance, future studies could incorporate multivariate or regression-based models to examine relationships between specific privacy dimensions and attitudes toward AI technologies, as well as the correlations between the smart city index and privacy dimensions, or between the smart city index and the attractiveness of AI technologies. Additionally, cross-cultural comparisons and larger

samples would enhance generalizability and allow for testing whether findings hold across different smart city implementations and cultural attitudes toward surveillance.

Ethics declaration: The authors declare that they have no conflict of interest and that all ethical standards regarding research integrity and participant consent were strictly observed throughout the study.

AI declaration: The authors utilised R Discovery to identify relevant literature and Grammarly to enhance the readability of the article. The authors reviewed and edited the content and take full responsibility for the content of the published article.

References

Bibri, S. E., & Allam, Z. (2022). The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism. Smart Cities, 5(2), 715–727. https://doi.org/10.3390/smartcities5020037

Chen, X., Wu, M., Cheng, C., & Mou, J. (2024). Weighing user's privacy calculus on personal information disclosure: the moderating effect of social media identification. Online Information Review, 49(2), 353–372. https://doi.org/10.1108/oir-03-2024-0135

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society, 3(2), 405–413. https://doi.org/10.1007/s12394-010-0053-z

IMD (2024). Smart City Index. https://www.imd.org/smart-city-observatory/home/rankings/

Johnson, A. (2023). Balancing Privacy and Innovation in Smart Cities and Communities. Information Technology & Innovation Foundation. https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/

Kalenyuk, I., Bohun, M., & Djakona, V. (2023). INVESTING IN INTELLIGENT SMART CITY TECHNOLOGIES. Baltic Journal of Economic Studies, 9(3), 41–48. https://doi.org/10.30525/2256-0742/2023-9-3-41-48

Karwatzki, S., Veit, D., & Trenz, M. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. Information Systems Journal, 32(6), 1126–1157. https://doi.org/10.1111/isj.12386

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Larson, R. B. (2023). Privacy concerns and social desirability bias. International Journal of Market Research, 66(4), 428–450. https://doi.org/10.1177/14707853231222810

Le, C., Zhang, Z., & Liu, Y. (2024). Research on Privacy Disclosure Behavior of Mobile App Users from Perspectives of Online Social Support and Gender Differences. International Journal of Human–Computer Interaction, 41(2), 861–875. https://doi.org/10.1080/10447318.2024.2305988

Lyon, D. (2018). The Culture of Surveillance: Watching as a Way of Life. London: Polity Press, 239 p. ISBN: 978-0-745-67173-4.

Machín, J., Martínez-Ballesté, A., Solanas, A., & Batista, E. (2021). Privacy and Security in Cognitive Cities: A Systematic Review. Applied Sciences, 11(10), 4471. https://doi.org/10.3390/app11104471

Martinez-Balleste, A., Perez-Martinez, P., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. IEEE Communications Magazine, 51(6), 136–141. https://doi.org/10.1109/mcom.2013.6525606

Memon, M. A., Ting, H., Thurasamy, R., Cheah, J.-H., Chuah, F., & Cham, T. H. (2020). Sample Size for Survey Research: Review and Recommendations. Journal of Applied Structural Equation Modeling, 4(2), i–xx. https://doi.org/10.47263/jasem.4(2)01

Naik, N., & Jenkins, P. (2020). Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity. 1–6. https://doi.org/10.1109/besc51023.2020.9348298

Nissenbaum, H. (2009). Privacy in Context (Vol. 58). Stanford University. https://doi.org/10.1515/9780804772891

Pronzato, R., & Markham, A. N. (2023). Returning to critical pedagogy in a world of datafication. Convergence: The International Journal of Research into New Media Technologies, 29(1), 97–115. https://doi.org/10.1177/13548565221148108

Sampaio, S., Sousa, P. R., Martins, C., Ferreira, A., Antunes, L., & Cruz-Correia, R. (2023). Collecting, Processing and Secondary Using Personal and (Pseudo)Anonymized Data in Smart Cities. Applied Sciences, 13(6), 3830. https://doi.org/10.3390/app13063830

Sanchez, T. W., Brenman, M., & Ye, X. (2024). The Ethical Concerns of Artificial Intelligence in Urban Planning. Journal of the American Planning Association, 91(2), 294–307. https://doi.org/10.1080/01944363.2024.2355305

Sarp, S., Kuzlu, M., Jovanovic, V., Polat, Z., & Guler, O. (2024). Digitalization of railway transportation through AI-powered services: digital twin trains. European Transport Research Review, 16(1). https://doi.org/10.1186/s12544-024-00679-5

Solanas, A., Papageorgiou, A., Batista, E., Patsakis, C., & Casino, F. (2021). Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach (pp. 201–213). Springer. https://doi.org/10.1007/978-3-030-10591-4_12

Sundquist, P. W. (2023). Surveillance Normalization. Harvard Civil Rights – Civil Liberties Law Review. https://journals.law.harvard.edu/crcl/wp-content/uploads/sites/80/2023/04/Surveillance-Normalization.pdf

Tan, H. H., & Zhao, B. (2003). Individual- and Perceived Contextual-Level Antecedents of Individual Technical Information Inquiry in Organizations. The Journal of Psychology, 137(6), 597–621. https://doi.org/10.1080/00223980309600637

Tan, K. L., Lam, K.-Y., & Chi, C.-H. (2023). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. ACM Computing Surveys, 56(3), 1–36. https://doi.org/10.1145/3616400

Van Ooijen, I., Opree, S. J., & Segijn, C. M. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. Communication Research, 51(2), 146–177. https://doi.org/10.1177/00936502211060984

Whelan, E., Lang, M., & Butler, M. (2024). Beyond lazy; external locus of control as an alternative explanation for the privacy paradox. Internet Research, 35(1), 349–379. https://doi.org/10.1108/intr-04-2023-0282

World Population Review (2025). https://worldpopulationreview.com/search?query=d

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs. ISBN: 978-1610395694