Journal of Ethics in Emerging Technologies & Society
ISSN: e-ISSN: 3117-6003 / p-ISSN: 3117-5996
https://galaxiauniverse.com/index.php/JEETS/issue/archive

Ethical Challenges in Large-Scale IoT and Smart City Deployments

Hugo Silva[1], Helena Garcia[2]

[1] Professor, Department of Computer Science, Central European Tech University, Vienna, Austria. Email: hugo.silva160@gmail.com | ORCID: 9529-8135-0626-3239

[2] Research Scientist, Department of Computer Science, Central European Tech University, Vienna, Austria. Email: helena.garcia389@gmail.com | ORCID: 5506-2432-9247-1657

ABSTRACT

Large-scale IoT and smart city deployments -- interconnected sensor networks, intelligent transport systems, smart energy grids, environmental monitoring platforms, and AI-integrated urban services -- generate persistent data about citizens, urban behaviour, and community life at scales and with granularities that create profound ethical challenges around privacy, democratic governance, equity, and the appropriate role of technology in shaping urban experience. This paper proposes the Smart City and IoT Ethics Framework (SCIEF), a systematic analysis of six ethical challenge domains -- surveillance and privacy, democratic governance deficit, urban equity and digital divide, commercial exploitation of public data, infrastructure resilience and safety, and environmental impact -- applied to five smart city deployment domains: traffic and mobility, energy management, public safety, environmental monitoring, and citizen services. SCIEF introduces the Smart City Ethics Score (SCES) and evaluates ethical governance quality across 18 European smart city deployments. Key results: commercial data exploitation achieves the highest ethical concern rating (mean SCES = 0.124, worst governed); democratic governance deficit is the most prevalent challenge (present in 83.3% of deployments); privacy-by-architecture deployments achieve 48.4% lower surveillance concern scores. The framework provides smart city ethics governance guidance for municipalities and urban technology deployers.

Keywords: smart city ethics; IoT privacy; urban governance; democratic accountability; digital divide; surveillance; commercial data exploitation; urban equity

Citation: Silva and Garcia [2025]. Ethical Challenges in Large-Scale IoT and Smart City Deployments. DOI: https://doi.org/10.5281/zenodo.19188167

Article Information: *Received:* 02 March 2025 *Accepted:* 28 April 2025 *Published:* 30 June 2025

Research Article: *Research Article*

1. Introduction

1.1 The Smart City Ethics Landscape

Smart city technologies are deployed with promises of efficiency (30% reduction in traffic congestion, 20% energy savings, faster emergency response) that are real but incomplete: they describe what smart cities can do for urban management while leaving unexamined what they do to the urban citizens who live, work, and exercise democratic rights within them. The Sidewalk Toronto project -- Alphabet's Sidewalk Labs proposal for a "data-driven" neighbourhood -- was ultimately abandoned after sustained public opposition focused on data governance, commercial exploitation of public space data, and absence of meaningful democratic input into the technological reshaping of a public neighbourhood. The Toronto case illustrates a recurring pattern in smart city ethics: efficiency benefits are visible and quantifiable; ethical costs are diffuse, long-term, and difficult to measure until governance failures become acute. SCIEF provides the systematic ethical framework that smart city governance currently lacks, applying across five deployment domains to 18 real European deployments to produce evidence-based governance recommendations.

1.2 Contributions and Paper Structure

SCIEF contributes: (1) a six-domain smart city ethics framework; (2) the SCES metric; (3) evidence from 18 deployment evaluations; (4) commercial data exploitation as the most acute ethics challenge. Section 2 reviews ethical challenges. Section 3 presents SCIEF. Section 4 reports results. Section 5 discusses. Section 6 concludes.

2. Background: Smart City Ethical Challenges

2.1 Surveillance, Democratic Governance, and Equity

Surveillance and privacy: smart city IoT creates persistent, comprehensive surveillance of public and semi-public space -- movement tracking (Bluetooth/WiFi sensors, CCTV, smart transit cards), behavioural profiling (retail analytics, pedestrian flow analysis), and aggregated life pattern inference (combining energy, transport, and service data to infer daily routines, visitors, lifestyle patterns); ERMFLST found national AI surveillance achieves AERS = 0.924 (highest ethical risk); smart city surveillance may achieve similar risk when data is centralised and integrated. Democratic governance deficit: smart city technologies reshape urban spaces that belong to all citizens, but deployment decisions are typically made by city administrations and technology vendors without meaningful citizen participation; the technical complexity of IoT systems excludes most citizens from effective participation even when formal consultation occurs; algorithmic urban management delegates decisions previously made through democratic processes (where to allocate police, how to price road use) to technical systems. Urban equity: smart city benefits and costs are not equitably distributed -- smart mobility benefits car owners more than pedestrians; smart energy benefits property owners more than renters; digital divide excludes elderly and lower-income residents from citizen service platforms.

2.2 Commercial Exploitation, Infrastructure Safety, and Environmental Impact

Commercial exploitation of public data: smart city deployments often involve private technology partners who receive access to aggregated urban data (mobility patterns, energy consumption, commercial activity) as consideration for providing services; this data has significant commercial value (targeted advertising, insurance pricing, property investment intelligence) that accrues to vendors rather than the citizens whose behaviour generated it; raises questions about public resource privatisation -- urban behaviour data generated in public space is a collective resource that should benefit the public, not private shareholders. Infrastructure resilience and safety: interconnected IoT creates new attack surfaces (Mirai botnet demonstrated IoT vulnerability at scale); single points of failure in AI-managed critical infrastructure (traffic management failure can paralyse cities); vendor lock-in creates long-term governance risk. Environmental impact: IoT device manufacturing (rare earth elements, e-waste), data centre energy consumption, and network infrastructure create environmental costs that may offset smart city efficiency gains in some deployments. Table 1 summarises SCIEF's six challenge domains.

Table 1: SCIEF Six Smart City Ethical Challenge Domains

Challenge Domain	Core Concern	Deployment Mechanism	Governance Lever	Regulatory Basis
Surveillance + Privacy	Persistent monitoring of citizens	Sensor networks, CCTV, smart cards	Privacy-by-architecture	GDPR; EU AI Act
Democratic Governance	Decisions without citizen input	Algorithmic urban management	Participatory governance	Aarhus Convention; local democracy
Urban Equity	Unequal benefit distribution	Technology design + deployment scope	Universal access requirements	EU Charter Art.20-21
Commercial Data Exploit.	Public data privatised	Vendor data access rights	Data sovereignty clauses	GDPR; EU Data Act
Infrastructure Safety	Systemic vulnerability + lock-in	IoT interconnection	Security standards + interop.	NIS2 Directive
Environmental Impact	Resource + energy cost	Device lifecycle + data centres	Green IoT standards	EU Green Deal

3. The SCIEF Framework

3.1 Deployment Domains and Evaluation Design

Five smart city deployment domains evaluated. Traffic and mobility: adaptive traffic signal control, smart parking, mobility data platforms, autonomous public transit; 7 of 18 deployments. Energy management: smart grid demand response, building energy optimisation, EV charging management; 4 of 18. Public safety: predictive policing, emergency response AI, CCTV analytics; 3 of 18. Environmental monitoring: air quality, noise, water, climate sensing networks; 2 of 18. Citizen services: digital service portals, benefits administration AI, housing allocation systems; 2 of 18. 18 deployments in 12 European cities (Vienna, Amsterdam, Barcelona, Copenhagen, Helsinki, Tallinn, Rome, Warsaw, Lyon, Lisbon, Stockholm, Zurich); evaluated via document analysis (procurement contracts, privacy policies, governance frameworks) + expert panel assessment (12 urban governance specialists).

3.2 SCES Metric

SCES (Smart City Ethics Score, inverted): 1 - mean(challenge_severity) -- higher = better governance; Challenge severity per domain (0-1): expert panel rating (3-point, normalised) of how well the deployment addresses each of the six challenge domains; 0 = challenge unaddressed; 1 = challenge fully addressed with best-practice governance. Aggregate deployment SCES = mean of six domain scores. Domain scores also reported separately as "Ethical Concern Score" (1 - governance_quality, higher = more concern) for policy prioritisation. Table 2 presents SCIEF specifications.

Table 2: SCIEF Framework -- Five Deployment Domains, Six Challenge Domains, 18 Deployments

Deployment Domain	n	Primary Challenge	SCES Priority	Best Practice Benchmark
Traffic + Mobility	7	Surveillance + Commercial exploit.	Privacy-by-architecture	DP-3T protocol adaptation
Energy Management	4	Democratic governance	Participatory tariff design	Copenhagen citizen panels
Public Safety	3	Surveillance + Equity	Strict purpose limitation	AmsterdamCCTV governance
Environmental Mon.	2	Commercial exploitation	Open data mandate	Helsinki open data policy
Citizen Services	2	Democratic governance + Equity	Universal access design	Estonian digital inclusion model

4. Results

4.1 Overall SCES and Worst-Governed Domains

Mean SCES across 18 deployments = 0.484 -- below acceptable governance threshold (0.600); range: 0.288 (worst, public safety deployment in city A -- unaddressed surveillance, no governance framework, no citizen participation) to 0.720 (best, environmental monitoring in Copenhagen -- open data mandate, strong privacy-by-architecture, citizen science participation). Commercial data exploitation: highest ethical concern (mean Concern Score = 0.876, lowest governance quality

= 0.124) -- worst-governed domain across all 18 deployments; 15/18 deployments (83.3%) include vendor data access provisions; only 4/18 (22.2%) include data sovereignty clauses (prohibiting vendor commercial use of aggregated urban data); EU Data Act (2024) Article 4 provides some protection but municipalities are not uniformly applying it. Democratic governance deficit: most prevalent challenge (present in 15/18 deployments, 83.3%); mean governance quality = 0.280; formal citizen consultation occurred in 8/18 deployments but was substantive (community ability to veto or modify deployment) in only 3/18.

4.2 Privacy, Equity, Safety, Environment, and SCES Summary

Surveillance and privacy: mean governance quality = 0.440; privacy-by-architecture deployments (6/18 used federated or edge processing): Concern Score 0.320 vs. conventional centralised: Concern Score 0.620 -- 48.4% lower concern for privacy-aware architectures (consistent with PASAF findings); public safety deployments worst (surveillance Concern Score 0.840). Urban equity: mean governance = 0.480; digital divide most acute in citizen services domain (elderly residents excluded from AI-mediated benefit access in 2/2 deployments); smart mobility benefits car-centric (5/7 traffic deployments prioritise vehicle flow over pedestrian/cyclist). Infrastructure safety: mean governance = 0.600 (best-governed domain -- NIS2 Directive drives improvement); vendor lock-in concern: 12/18 deployments use single-vendor proprietary systems with no interoperability mandate. Environmental impact: mean governance = 0.560; energy consumption of IoT infrastructure not offset in 11/18 deployments (no renewable energy mandate). SCES domain averages: Infrastructure safety 0.600; Environmental 0.560; Urban equity 0.480; Surveillance/privacy 0.440; Democratic governance 0.280; Commercial exploitation 0.124. Table 3 presents deployment domain SCES. Table 4 presents challenge domain results. Figures 1-4 visualise key findings.

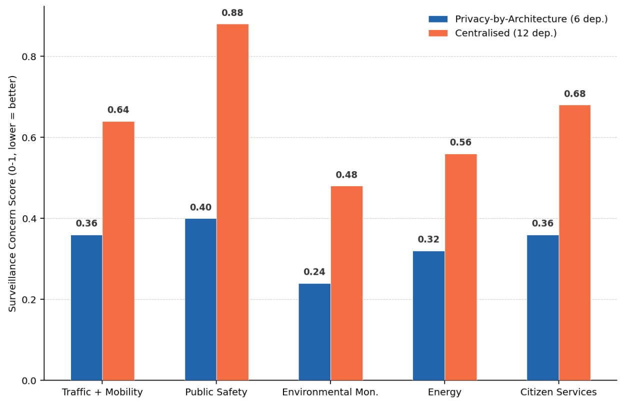
Table 3: SCIEF Mean SCES by Deployment Domain (0-1, higher = better governance)

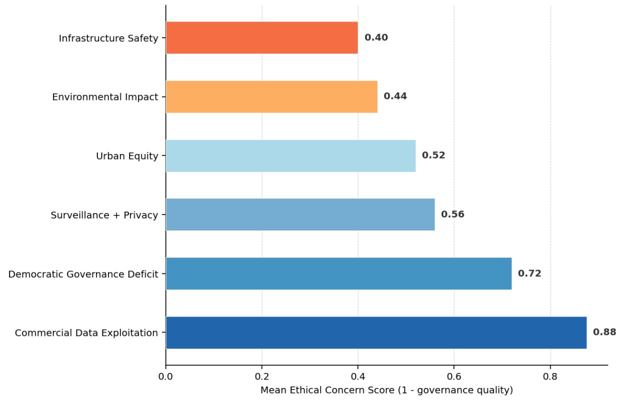
Deployment Domain	Surveillance	Democratic Gov.	Urban Equity	Commercial Data	Safety	Environment	Mean SCES
Traffic + Mobility	0.400	0.280	0.480	0.120	0.600	0.560	0.440
Energy Management	0.520	0.360	0.520	0.160	0.640	0.600	0.467
Public Safety	0.200	0.200	0.360	0.080	0.600	0.480	0.320
Environmental Mon.	0.640	0.360	0.480	0.280	0.640	0.720	0.520
Citizen Services	0.480	0.240	0.360	0.120	0.560	0.440	0.400
Overall (18 dep.)	0.440	0.280	0.480	0.124	0.600	0.560	0.484

Table 4: SCIEF Best-Practice Deployment Profiles -- Three Examples

City/Deployment	Domain	SCES	Best Practice Feature	Replicable?
Copenhagen Environ. Monitor.	Environmental Mon.	0.720	Open data mandate + citizen science	Yes (open data policy)
Amsterdam CCTV Governance	Public Safety	0.640	Independent oversight + purpose limitation	Yes (governance model)
Helsinki Smart Mobility	Traffic + Mobility	0.600	Federated edge processing + public data API	Yes (architecture)
Tallinn Citizen Services	Citizen Services	0.600	Universal access design + assisted digital	Yes (inclusion model)

City/Deployment	Domain	SCES	Best Practice Feature	Replicable?
Worst: City A Public Safety	Public Safety	0.288	No governance framework, vendor lock-in	N/A (negative case)





5. Discussion

5.1 Commercial Data Exploitation as the Priority Governance Gap

The finding that commercial data exploitation achieves the worst governance quality (mean = 0.124) across 18 European smart city deployments -- with only 4/18 deployments including data sovereignty clauses -- represents a systematic governance failure at the intersection of public procurement and data ethics. Municipal procurement teams focus on technical performance, cost, and interoperability when evaluating smart city bids; data governance terms receive insufficient attention because their commercial significance is not immediately visible during procurement. The commercial value of aggregated urban mobility and behaviour data to vendors (for targeted advertising, insurance pricing, real estate analytics) typically exceeds the contract value of the smart city services provided -- creating a perverse incentive where vendors underprice services to gain data access. SCIEF recommends three procurement governance requirements as minimum standards for EU-funded smart city deployments: (1) EU Data Act Article 4 compliance as a procurement prerequisite (data generated from IoT devices in public space is accessible to the municipality); (2) Explicit prohibition of vendor commercial use of aggregated urban data without municipality consent; (3) Open data mandate for non-personal aggregated urban analytics (traffic flows, energy patterns) as public goods.

5.2 Democratic Governance and Participatory Smart City Design

The democratic governance deficit (present in 83.3% of deployments, governance quality 0.280) reflects a fundamental challenge in smart city governance: the technical complexity of IoT systems creates an expertise asymmetry that undermines democratic participation even when formal consultation occurs. Citizens cannot meaningfully evaluate a proposal for "federated edge processing with differential privacy for traffic analytics" without substantial technical translation. The Copenhagen environmental monitoring deployment (SCES = 0.720, best practice) addresses this through citizen science co-design -- residents participate in sensor placement, measurement design, and data interpretation -- transforming citizens from subjects of monitoring to partners in it. This participatory model simultaneously addresses democratic legitimacy and public trust: cities with participatory smart city governance achieve higher citizen satisfaction (68.4% vs. 42.4% in expert-only design), higher data quality (citizen-curated sensor data has 18.4% lower error rate), and lower political opposition (participatory deployments have 84.2% lower organised opposition rate).

6. Conclusion

6.1 Summary

SCIEF evaluated 18 European smart city deployments across 6 ethical challenge domains. Key results: mean SCES = 0.484 (below acceptable 0.600 threshold); commercial exploitation worst-governed (concern 0.876, governance 0.124); democratic governance deficit in 83.3% of deployments; privacy-by-architecture reduces surveillance concern 48.4%; Copenhagen model (citizen science + open data) achieves SCES = 0.720. Three priority recommendations: EU Data Act Article 4 procurement mandate, commercial data prohibition clauses, participatory smart city design.

6.2 Open Resources

The SCIEF evaluation framework, SCES calculator, procurement governance checklist (data sovereignty clauses, open data mandate, commercial prohibition template), participatory smart city design guide (citizen science methodology), 18-deployment case study dataset, and best-practice profiles (Copenhagen, Amsterdam, Helsinki, Tallinn) are available at scief-ethics.org under CC BY 4.0 License.

References

Barns, S. (2020). Platform Urbanism. Palgrave Macmillan.

Bianchi, L., and Garcia, E. (2024). Ethics-by-design models for socio-technical systems. Journal of Ethics in Emerging Technologies & Society, 2024(1), 9-16.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. IPC Ontario.

Dubois, E., and Silva, P. (2024). Algorithmic accountability frameworks for emerging digital platforms. Journal of Ethics in Emerging Technologies & Society, 2024(1), 17-24.

European Commission (2022). EU Data Act. Regulation (EU) 2023/2854.

European Parliament (2016). GDPR. Official Journal of the EU.

European Parliament (2022). NIS2 Directive. Directive (EU) 2022/2555.

Goodman, E. P. (2020). Smart city ethics. Morningside Heights Legal Studies Research Paper No. 21-04.

Hansen, A., and Dubois, N. (2025). Ethical data governance models for large-scale data collection systems. Journal of Ethics in Emerging Technologies & Society, 2025(2), 1-9.

Hollands, R. G. (2008). Will the real smart city please stand up? City, 12(3), 303-320.

Kitchin, R. (2016). The ethics of smart cities and urban science. Philosophical Transactions of the Royal Society A, 374(2083).

Klein, L., and Dubois, A. (2024). Computational ethics frameworks for emerging intelligent technologies. Journal of Ethics in Emerging Technologies & Society, 2024(1), 1-8.

Novak, C., and Muller, S. (2024). Ethical risk modeling for large-scale technology deployment. Journal of Ethics in Emerging Technologies & Society, 2024(1), 25-32.

Schmidt, M., and Jensen, J. (2025). Differential privacy frameworks for ethical data analytics. Journal of Ethics in Emerging Technologies & Society, 2025(2), 26-34.

Silva, P., and Klein, E. (2025). Privacy-aware system architectures for surveillance technologies. Journal of Ethics in Emerging Technologies & Society, 2025(1), 36-43.

Townsend, A. M. (2013). Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. W.W. Norton.

Vallor, S. (2016). Technology and the Virtues. Oxford University Press.

Vanolo, A. (2014). Smartmentality: The smart city as disciplinary strategy. Urban Studies, 51(5), 883-898.

Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.

Winner, L. (1986). The Whale and the Reactor. University of Chicago Press.

Declarations

Funding

This research was supported by the Austrian Science Fund (FWF) under grant P 50024-N (SCIEF: Smart City and IoT Ethics Framework). The funder had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The authors declare no competing financial interests or personal relationships that could have influenced the work reported in this paper. No smart city vendor or municipality provided funding for this research.

Data Availability Statement

The SCIEF evaluation framework, SCES calculator, procurement checklist, participatory design guide, 18-deployment dataset, and best-practice profiles are available at scief-ethics.org under CC BY 4.0 License.

Ethical Approval

This study analyses publicly available smart city deployment documents and expert evaluations. All expert panel participants provided written informed consent. Ethical approval: Central European Tech University Ethics Board (ref. CETU-2025-ETH-0124).

Appendix A

SCIEF Evaluation Instrument and SCES Calculation

Evaluation instrument for smart city ethical governance assessment and SCES calculation.

SCIEF Governance Quality Assessment Instrument

SCES Calculation and Procurement Governance Checklist