International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

The Watched City: Privacy, Surveillance, and the Governance of Smart Urban Mobility

Maulsri Jha

Ph.D., AICP, LEED GA
Senior Project Manager
CDM Smith, Seattle, WA

Abstract:
Smart mobility systems increasingly depend on continuous data collection from fare media, mobile devices, cameras, connected vehicles, license-plate systems, shared-mobility platforms, and urban sensors. These infrastructures can improve network management, safety, reliability, and traveler information, yet they also convert ordinary movement into a persistent stream of potentially identifiable behavioral data. This article develops a planning-centered framework for governing the privacy and surveillance risks of smart urban mobility. Drawing on scholarship on smart urbanism, transport data protection, public-sector technology governance, and recent work on video-based traffic sensing and data sovereignty, the article compares governance logics visible in European, North American, and Asian smart-city contexts. It argues that privacy cannot be treated as a downstream legal compliance issue. Instead, privacy protection must be embedded in transportation planning decisions about purpose, data architecture, procurement, retention, access, sharing, and public accountability. The article proposes a Responsible Smart Mobility Governance Framework organized around necessity, proportionality, minimization, transparency, contestability, security, equity, and institutional stewardship. The framework reframes the smart-city question from whether cities can collect mobility data to what data are legitimately necessary for a defined public purpose and under what governance conditions.

Keywords: smart cities; smart mobility; privacy; surveillance; urban data; transportation planning; data governance.

1. Introduction

Digitalization has altered the informational foundations of transportation planning. Conventional planning depended heavily on periodic household travel surveys, manual counts, fixed sensors, census products, and model-based estimates. Smart-city systems increasingly supplement these sources with continuous and highly granular data generated by travelers themselves or by infrastructures that observe them. Account-based fare systems can record the timing and sequence of trips. Mobile applications can generate location traces. Cameras and automated vehicle-recognition systems can observe movement through streets and intersections. Shared-mobility platforms record origins, destinations, payment relationships, and device identifiers. Connected vehicles and roadside infrastructure create additional streams of operational data. In practical terms, the smart mobility system is also an urban sensing system.

The planning value of these data is substantial. More timely information can support service planning, incident response, curb management, traffic operations, accessibility analysis, safety interventions, and evaluation of policy changes. The same informational richness, however, creates a governance problem. Mobility data are not merely technical observations of a network. They can reveal routines, workplaces, health-related destinations, religious or political activity, social relationships, and other patterns that become sensitive when linked across time and space. Mantelero (2015) warned that intelligent public-transport systems can transform mobility architectures into generalized territorial surveillance if privacy protections are weak. Kitchin (2014) similarly identified the panoptic potential of data-intensive smart urbanism alongside concerns about technocratic governance, corporate lock-in, and system vulnerability. This article asks a planning question that is often displaced into legal or information-technology domains: what would it mean to plan a smart mobility system in which privacy is treated as a core public value rather than an external constraint? The article makes three contributions. First, it distinguishes service-oriented mobility intelligence from surveillance-oriented mobility intelligence. Second, it identifies the institutional choices through which transportation agencies shape privacy outcomes, including procurement, retention, data sharing, and secondary use. Third, it proposes a Responsible Smart Mobility Governance Framework that can be applied during project development and evaluation.

2. Smart Mobility as an Urban Data Infrastructure

The smart-city literature has long emphasized the capacity of ubiquitous computing to produce a real-time representation of urban life. Kitchin (2014) describes this shift as the instrumentation and datafication of the city, in which digital devices generate streams of information that can be analyzed to manage urban systems. Transportation is especially consequential because movement connects nearly every domain of daily life. Unlike many municipal datasets, mobility data are inherently relational and sequential: a single observation may be mundane, but a series of observations can reconstruct a person's routine.

This distinction between isolated and longitudinal information matters for planning. A traffic counter that records aggregate vehicle volumes poses a different privacy risk from a camera system that persistently identifies plates or faces. An anonymous boarding count differs from an account-based fare history associated with a named customer. A shared-bicycle availability feed differs from a trip-level dataset containing precise origins and destinations. Van Zoonen (2016) argues that privacy concern in smart cities varies both with the sensitivity of the data and with the purpose for which data are used. The service-versus-surveillance distinction is therefore not simply rhetorical; it is a useful planning diagnostic.

Recent scholarship has also shifted attention from privacy as individual secrecy toward data sovereignty and institutional control. Anthony and Sarshar (2025) argue that intelligent mobility services depend on citizen-generated data while often leaving individuals with limited control over how those data circulate among service providers and third parties. Biyani and Wimmer (2026) identify data trusts as one possible institutional mechanism for privacy-preserving sharing in smart cities. These approaches suggest that the central problem is not data collection alone, but the governance chain through which data are collected, combined, inferred upon, retained, sold, transferred, or repurposed.

3. Why Transportation Planning Needs a Privacy Lens

Transportation planning traditionally evaluates projects through criteria such as mobility, accessibility, safety, cost, environmental impact, equity, and feasibility. Smart mobility requires an additional criterion: informational impact. A system can improve travel-time reliability while simultaneously creating an unnecessarily intrusive data architecture. Because those outcomes can coexist, operational success is not evidence of responsible governance.

Privacy also has distributive implications. Data-intensive enforcement or monitoring may be concentrated in particular neighborhoods or applied disproportionately to groups that already experience intensive state observation. Digital mobility services can exclude people without smartphones, bank accounts, stable connectivity, or confidence in data-sharing systems. Conversely, eliminating useful data in the name of privacy can make it harder to identify inequities in service or safety. The planning challenge is therefore to avoid a false choice between data and rights. The objective should be fit-for-purpose data systems that generate sufficient information for legitimate planning goals while limiting unnecessary identification and secondary use.

Public trust is operationally relevant. Guazzo et al. (2026), using a large U.S. sample, found that privacy concerns reduce acceptance of video-based traffic sensors and that trust in government shapes acceptance. A technically effective sensor network can therefore become politically fragile when residents do not understand why data are collected, how long they are retained, or who can access them. Trust should not be treated as a communications problem after deployment. It is partly an outcome of system design.

4. Comparative Governance Lessons

European smart mobility operates within a comparatively mature data-protection environment in which purpose limitation, proportionality, transparency, and data-subject rights have become central governance concepts. The significance for transportation agencies is procedural as much as legal. Agencies are pushed to define why personal data are needed, whether less intrusive alternatives exist, and how data flows are documented. Mantelero's (2015) analysis of e-ticketing illustrates the value of privacy-oriented design, anonymization, pseudonymization, and multi-stakeholder governance in public transport.

North American cities have often approached smart mobility through a fragmented combination of municipal policy, vendor contracts, sector-specific rules, and program-level requirements. Docherty et al. (2020), comparing London and Seattle, show that cities retain an important steering role when regulating emerging mobility services. Their analysis emphasizes the need for mode-specific rules, clearly assigned provider responsibilities, consequences for noncompliance, and alignment between private mobility offerings and long-term city strategies. The same logic applies to data governance: cities should not accept vendor-defined data practices as technologically inevitable.

Singapore illustrates a different institutional setting in which extensive digital integration can coexist with distinctive models of consent and public-sector accountability. Recent legal scholarship uses Singapore's Smart Nation program to examine whether conventional consent models are adequate when sensors and digital services are woven into everyday urban environments (Chik, 2025). The broader lesson is that smart-city privacy cannot be reduced to a single universal mechanism such as a privacy

notice. Governance must reflect the asymmetry between residents and the institutions that operate essential urban systems.

5. A Responsible Smart Mobility Governance Framework

The proposed framework contains eight linked principles. Necessity requires an agency to identify the specific public problem that requires data. Proportionality asks whether the sensitivity and granularity of the data are justified by the expected public benefit. Data minimization requires collection of the least detailed information capable of meeting the purpose. Transparency requires intelligible public documentation of collection, retention, sharing, and automated analysis. Contestability gives affected people meaningful routes to challenge erroneous or harmful uses. Security addresses technical and organizational protection throughout the data lifecycle. Equity examines whether data collection, algorithmic inference, or enforcement burdens are distributed unevenly. Institutional stewardship assigns clear responsibility for governance rather than diffusing accountability across agencies and vendors.

These principles should be applied at project initiation rather than immediately before procurement or deployment. A transportation agency considering video analytics, for example, should first specify whether the planning need is aggregate turning counts, conflict detection, enforcement, traveler identification, or some combination. If aggregate counts are sufficient, on-device processing that discards source imagery may be preferable to retaining identifiable video. If trip-level fare data are required for service planning, agencies can evaluate aggregation thresholds, pseudonymization, retention limits, access controls, and whether customer identity needs to be available to analysts at all.

Procurement is a particularly important governance point because smart-city capabilities are frequently embedded in proprietary platforms. Contracts should specify data ownership, permitted uses, subcontractor access, retention, deletion, breach response, audit rights, model documentation where algorithmic tools are used, and restrictions on commercial reuse. A city that does not control these terms may lose practical sovereignty over an infrastructure funded for public purposes.

Finally, the framework requires governance of secondary use. Data collected for traffic operations may later appear attractive for policing, commercial analytics, immigration enforcement, litigation, or unrelated research. Secondary uses should not be assumed legitimate merely because data already exist. They should undergo a new purpose, proportionality, legal, and equity review.

6. Planning Applications

The framework can be incorporated into existing transportation planning processes without creating an entirely separate bureaucracy. Alternatives analysis can include informational impacts alongside cost, operations, and environmental criteria. Pilot projects can establish explicit sunset dates and deletion requirements. Performance dashboards can report not only mobility outcomes but also data-retention compliance, security incidents, public complaints, and the proportion of datasets processed in aggregated or de-identified form. Advisory committees can include privacy, civil-rights, accessibility, and community representatives alongside technology and transportation specialists.

Integrated command-and-control centers deserve particular scrutiny because they concentrate streams from multiple urban systems. Integration can produce operational benefits during emergencies and network disruptions, but it also increases the possibility of function creep. The informational power of a system grows nonlinearly when datasets are linked. A transit record, camera observation, parking transaction, and mobile-device identifier may each be limited in isolation but highly revealing when

combined. Governance should therefore evaluate data linkage as a distinct action rather than treating it as a routine technical step.

7. Discussion

The smart-city narrative often equates more information with better governance. That assumption is incomplete. Better planning depends on appropriate information, institutional competence, legitimate authority, and public accountability. Excessive data collection can create costs, cybersecurity exposure, legal risk, chilling effects, and political opposition without materially improving planning decisions.

A rights-respecting approach does not imply technologically conservative transportation planning. Privacy-preserving computation, edge processing, aggregation, differential access controls, data trusts, and carefully structured sharing agreements can enable sophisticated analysis while reducing exposure. The deeper shift is institutional: agencies should treat data architecture as part of transportation system design. Just as planners consider the physical footprint of a roadway or station, they should consider the informational footprint of a smart mobility intervention.

This perspective also changes how innovation is evaluated. A technology should not be called smart merely because it is automated, connected, or data-rich. A genuinely smart mobility system should be capable of producing public value while remaining governable, explainable, secure, and proportionate.

8. Conclusion

Smart urban mobility is becoming inseparable from urban data governance. As transportation systems acquire the capacity to observe movement continuously, planners face choices that shape not only network performance but also the relationship between residents, public institutions, and private technology providers. Privacy is therefore a planning issue.

The Responsible Smart Mobility Governance Framework proposed here offers a practical basis for evaluating data-intensive transportation systems through necessity, proportionality, minimization, transparency, contestability, security, equity, and stewardship. Its central proposition is simple: cities should begin with the public problem, not with the available data. The future of smart mobility should be measured not by how completely a city can observe movement, but by how effectively it can improve mobility while preserving the conditions of trust and autonomy on which legitimate urban governance depends.

REFERENCES:

1. Anthony, B., Jr., & Sarshar, S. (2025). Enhancing data sovereignty to improve intelligent mobility services in smart cities. Urban Governance Journal. https://doi.org/10.1016/j.ugj.2025.02.002
2. Biyani, S., & Wimmer, M. A. (2026). Data trusts in smart cities: Secure and redacted data sharing. Datenbank-Spektrum, 26, 129–134. https://doi.org/10.1007/s13222-026-00540-0
3. Chik, W. B. (2025). Comparing smart city data protection approaches: Digital consent and the accountability framework in Singapore. International Data Privacy Law, 15(1), 48–65.
4. Docherty, I., Marsden, G., & Anable, J. (2020). A preliminary assessment of regulatory efforts to steer smart mobility in London and Seattle. Transport Policy, 98, 170–177.

5. Guazzo, G. M., Rosati, P., Troisi, O., & Lynn, T. (2026). Balancing privacy and trust: Social acceptance of video-based traffic sensors in smart city initiatives. Government Information Quarterly, 43(1), 102099. https://doi.org/10.1016/j.giq.2025.102099
6. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. GeoJournal, 79, 1–14. https://doi.org/10.1007/s10708-013-9516-8
7. Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach.
8. Mantelero, A. (2015). Data protection, e-ticketing, and intelligent systems for public transport. International Data Privacy Law, 5(4), 309–320. https://doi.org/10.1093/idpl/ipv016
9. Ni Loideain, N. (2017). Cape Town as a smart and safe city: Implications for governance and data privacy. International Data Privacy Law, 7(4), 314–334. https://doi.org/10.1093/idpl/ipx018
10. Van Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472–480.