**THE INTERNET OF SURVEILLANCE: IOT, SMART CITIES, AND THE SOCIOLOGY OF SOCIAL CONTROL**

Nuhu Mukhtar Nuhu1 and Abubakar Abdullahi Ambursa2

1Department of Sociology, Rabi’u Musa Kwankwaso College of Advanced & Remedial Studies, Tudun-Wada, Kano

[nuhumukhtarnuhu@gmail.com](mailto:nuhumukhtarnuhu@gmail.com)

2Department of Sociology, Faculty of Social and Management Sciences, Federal University Birnin Kebbi, Kebbi State, Nigeria

[abubakar.abdullahia@fubk.edu.ng](mailto:abubakar.abdullahia@fubk.edu.ng)

***Abstract***

*The proliferation of Internet of Things (IoT) technologies in urban environments has created an “Internet of Surveillance,” where smart city infrastructures sensors, cameras, drones, and algorithmic systems reshape how social order, deviance, and governance are enacted. This study adopts an integrative socio-technical framework, combining social control theory, surveillance and algorithmic governance, and IoT network infrastructure analysis. Using a three-stage methodology document and policy review, empirical synthesis, and qualitative analytic reflection the research examines how IoT systems render urban activity visible yet opaque, automate social control, and produce differential surveillance that can reinforce inequalities. Findings show that multi-layered governance and technological opacity complicate transparency, accountability, and citizen trust, while IoT networks embed power in material infrastructures. The study underscores the need for socio-technical audits, inclusive network design, and regulatory frameworks that balance safety, efficiency, and ethics. By linking sociological theory with technological and governance analysis, it illuminates how IoT surveillance reconfigures privacy, trust, and citizenship in smart cities.*

***Keywords:*** *IoT, Smart Cities, Surveillance, Social Control, Algorithmic Governance, Privacy & Networked Society*

1. **INTRODUCTION**

The accelerating digitalisation of urban life has been accompanied by the pervasive diffusion of the Internet of Things (IoT) a constellation of interconnected sensors, cameras, drones, and data-analytic platforms that collectively underpin the infrastructure of contemporary “smart cities.” These socio-technical assemblages are promoted as engines of efficiency, sustainability, and enhanced public safety. Through real-time data collection and automated analytics, they promise to optimise urban management from traffic regulation and energy distribution to waste disposal and emergency response. However, beneath the rhetoric of optimisation lies an emergent paradigm of pervasive monitoring and behavioural governance. The same infrastructures that facilitate intelligent service delivery also function as distributed apparatuses of observation, classification, and control.

This paper conceptualises this duality through the notion of the “Internet of Surveillance” a framework that recognises how IoT-enabled systems reconfigure the architecture of visibility and power within urban space. In this context, surveillance is not limited to the act of watching but extends to the continuous production, circulation, and algorithmic interpretation of data about citizens’ movements, routines, and interactions. The networked nature of IoT technologies operating seamlessly across public and private domains renders everyday life increasingly transparent to both state institutions and commercial actors. Consequently, urban governance becomes a data-driven enterprise in which decision-making is mediated through technical infrastructures that are often opaque, privately managed, and asymmetrically distributed.

Drawing on sociological theories of social control and digital criminology, the paper interrogates how IoT-driven surveillance systems transform the modalities through which social order is maintained and deviance is defined. It explores how the diffusion of interconnected devices and algorithmic analytics reshapes relationships among citizens, governments, and technology providers, often eroding boundaries between civic participation and technological subjection. Central to this inquiry is the question: How do IoT-enabled surveillance infrastructures in smart cities reconfigure mechanisms of social control, and what implications do they hold for citizenship, privacy, and inequality?

By addressing this question, the study situates itself at the intersection of technological innovation and sociological critique. Rather than treating IoT as a purely technical phenomenon, it foregrounds its governance, ethical, and social dimensions issues that are increasingly salient for both researchers and policymakers. In doing so, the paper contributes to the thematic scope of the 7th International Conference on Networks, Blockchain and Internet of Things (NBIoT 2026) by advancing a multidisciplinary perspective that connects networked infrastructures to the politics of data, surveillance, and digital governance. This conceptual orientation encourages scholars and practitioners to interrogate not only how IoT networks operate, but also whose interests they serve and what forms of social order they produce.

1. **BACKGROUND AND RELATED WORK**

Over the past decade, an extensive body of scholarship has emerged on the deployment of Internet of Things (IoT) technologies within smart-city infrastructures. These studies document the design and implementation of sensor networks, real-time monitoring systems, and predictive analytics platforms that enable urban administrators to collect, process, and act upon vast streams of environmental and behavioural data (Ahmed, 2023). Within this literature, smart cities are often portrayed as data-driven ecosystems where IoT technologies enhance efficiency, responsiveness, and sustainability through automation and interconnectivity. The dominant narrative of “technological solutionism” (Morozov, 2013) frames these developments as inherently progressive, assuming that the integration of ubiquitous sensing and intelligent systems will inherently improve governance and quality of life.

Running parallel to this optimistic discourse, however, is a critical and rapidly expanding literature on surveillance studies and digital governance, which interrogates the social and ethical consequences of these same technologies. Scholars have examined how the proliferation of surveillance infrastructures alters the psychological and sociopolitical dynamics of visibility, trust, and control (Seymour, 2024). Within urban contexts, surveillance is increasingly understood not merely as the gathering of information but as a mode of governance a mechanism through which populations are observed, classified, and managed in the name of security and efficiency. This “governance through data” paradigm reframes the role of technology from a neutral facilitator to an active participant in shaping power relations and civic behaviour.

The intersection of IoT and surveillance raises pressing concerns related to privacy, data security, and algorithmic accountability. Researchers have consistently identified vulnerabilities in IoT ecosystems, including inadequate encryption, weak authentication, and opaque data flows, which can expose sensitive personal and locational data to misuse or exploitation (Laghari et al., 2024). These vulnerabilities extend beyond technical risk to encompass ethical and legal challenges particularly around issues of consent, data ownership, and the asymmetry between those who produce data and those who control its analysis. Recent systematic reviews further argue that the sharing of personal and contextual information through IoT-enabled smart-city applications erodes citizen autonomy, normalising surveillance as a routine aspect of urban life.

Despite these advances, a conceptual gap remains. Much of the existing IoT scholarship privileges technical architecture, system performance, or cybersecurity frameworks, while sociological and criminological analyses tend to treat surveillance abstractly, detached from its underlying network infrastructures. There is, therefore, a limited understanding of how IoT architectures concretely operationalise social control that is, how technical design choices and networked infrastructures become embedded in institutional practices of governance, policing, and behavioural regulation. This paper seeks to bridge that gap by integrating sociological theories of social control with contemporary analyses of IoT-enabled surveillance, situating smart-city technologies within the broader sociotechnical landscape of power, inequality, and digital governance.

**2.1 Conceptual Framework**

This study adopts an integrative conceptual framework built upon three mutually reinforcing strands: social control theory, surveillance and algorithmic governance studies, and IoT network infrastructure theory. Each strand contributes a distinct yet complementary perspective for understanding how Internet of Things (IoT)-enabled surveillance systems transform mechanisms of visibility, power, and governance within smart-city environments. By interlinking sociological theory and technological analysis, this framework offers a multidimensional approach to interpreting how IoT infrastructures mediate social control and reconfigure relations among citizens, institutions, and technology providers.

* 1. **1 Social Control Theory**

The first analytical strand draws on the tradition of social control theory, which examines how societies maintain order, regulate behaviour, and institutionalise norms of compliance. Foundational contributions by Émile Durkheim emphasised the moral and normative bonds that sustain collective life, while Travis Hirschi’s (1969) Social Bond Theory advanced the idea that conformity stems from an individual’s attachment, commitment, involvement, and belief in social values. Later, Michel Foucault (1977) reinterpreted control as a form of disciplinary power, exemplified in his notion of the panopticon, where visibility itself becomes a mechanism of domination. Contemporary scholars such as David Garland (2001) and Stanley Cohen (1985) have extended these ideas to late modern societies, highlighting how risk management and surveillance serve as institutionalised forms of social regulation.

At its core, social control theory assumes that social order is maintained not only through coercive authority but through subtle processes of observation, classification, and self-regulation. Surveillance thus becomes an instrument through which individuals internalise norms and modify behaviour in anticipation of being watched. The strength of this theory lies in its capacity to link individual conduct with broader institutional arrangements, revealing how surveillance can function as a tool of governance rather than mere oversight. However, its main limitation lies in its historical grounding in pre-digital contexts; traditional formulations did not anticipate the complexity of algorithmic surveillance or the diffusion of control across private, corporate, and technological actors. Applied to IoT-enabled smart cities, social control theory helps explain how digital infrastructures extend Foucault’s disciplinary logic embedding control within everyday devices, urban sensors, and algorithmic routines that normalise constant observation.

**2.1.2 Surveillance Studies and Algorithmic Governance**

The second strand emerges from the field of surveillance studies and its contemporary evolution into algorithmic governance. Scholars such as David Lyon (2001) and Kevin Haggerty and Richard Ericson (2000) reconceptualised surveillance as a defining feature of modern societies a decentralised and networked process rather than a top-down apparatus. Their idea of the “surveillant assemblage” captures how diverse technological systems converge to extract, store, and repurpose personal data for administrative, commercial, or security purposes. Building on this, Antoinette Rouvroy and Thomas Berns (2013) introduced the concept of algorithmic governance, describing how automated systems increasingly shape decision-making processes, often without direct human oversight or ethical scrutiny.

This perspective assumes that surveillance in the digital age operates continuously through data infrastructures that underpin everyday life. Power is exercised not only through visibility but through data capture where citizens become measurable entities within algorithmic systems. The strength of this strand lies in its diagnostic clarity: it explains how governance shifts from deliberative institutions to predictive analytics and algorithmic categorisation. Yet, a key weakness is its tendency toward abstraction and overemphasis on automation, sometimes overlooking human agency and institutional mediation. Applied to IoT contexts, this perspective clarifies how smart-city surveillance converts governance into a computational process, where sensors and algorithms monitor, classify, and even pre-empt behaviour. It thus bridges sociological critique with technological analysis, highlighting the political implications of data-driven control.

**2.1.3 IoT Network Infrastructure Theory**

The third strand situates these sociological insights within the technical architecture of IoT network infrastructures. Drawing from the work of Atzori, Iera, and Morabito (2017) and Gubbi et al. (2013), IoT systems are conceptualised as layered ecosystems connecting the physical and digital domains through continuous data exchange. Typically, these consist of a sensing layer (devices capturing environmental and behavioural data), a network and analytics layer (transmitting, processing, and interpreting data), and a governance or control layer (where institutional actors make operational or policy decisions). These layers illustrate how data moves from collection to computation to intervention, thereby embedding surveillance within the architecture of the city itself.

This strand assumes that technological infrastructures are never neutral; they embody political, economic, and ethical choices about what and whom to monitor. Its strength lies in revealing the material basis of surveillance how networked devices and communication protocols operationalise the collection and control of information. However, a recurring weakness in purely technical analyses is the tendency to isolate systems from their sociopolitical contexts, reducing governance to efficiency or optimisation. When integrated into this study, IoT infrastructure theory provides the structural backbone for understanding how social control is enacted through technical means. It exposes how sensor distribution, algorithmic design, and data flow management can produce differential surveillance, where certain neighbourhoods or populations become more visible and thus more regulated than others.

**2.1.4 Integrative Model**

Synthesising these strands yields an integrated sociotechnical model of the Internet of Surveillance. From social control theory, the framework inherits an understanding of discipline, normalisation, and behavioural conformity. From surveillance and algorithmic governance studies, it adopts insights into how data infrastructures and automated decision-making reshape visibility and accountability. From IoT network theory, it borrows a structural account of how these processes are technically embedded in the layered architecture of smart cities.

Together, these perspectives illuminate a critical insight: surveillance has become infrastructural. It is no longer confined to discrete observation but diffused across interconnected devices, sensors, and data systems that constitute the very fabric of urban life. This integrated framework enables the analysis of IoT-enabled surveillance as both a technological and sociological phenomenon one that simultaneously enhances administrative efficiency and redefines social control, privacy, and citizenship in the networked age.

1. **METHODOLOGY AND ANALYTICAL APPROACH**

Guided by the integrative conceptual framework outlined above, this study adopts a three-pronged methodological approach designed to interrogate the social, political, and technical dimensions of IoT-enabled surveillance in smart cities. The methodology aligns closely with the framework’s sociotechnical lens, ensuring that theoretical insights inform the collection, interpretation, and synthesis of empirical and policy material.

First, a systematic document and policy review is undertaken, focusing on smart-city IoT deployment strategies and urban governance frameworks. This includes municipal plans, national smart-city strategies, technical standards, and strategic reports produced by public and private stakeholders. Drawing on the IoT network infrastructure strand of the conceptual framework, the review emphasizes the technical architecture, sensor distribution, and governance logics embedded in these documents. Simultaneously, insights from social control theory and surveillance studies guide a critical reading of how policy discourses frame safety, risk, and citizen behaviour, revealing implicit assumptions about surveillance, compliance, and social order.

Second, a synthesis of recent empirical research on IoT surveillance systems is conducted, including studies of anomaly-detection platforms, sensor networks, and algorithmic monitoring tools (e.g., Islam, Dukyil, Alyahya, & Habib, 2023). This synthesis integrates findings from diverse urban contexts to identify patterns in technological deployment, operational practices, and social consequences. Framed through the surveillance and algorithmic governance strand, the analysis highlights how data infrastructures, automated decision-making, and computational logics shape the visibility, classification, and regulation of citizens. Particular attention is paid to the interplay between technical design choices and sociopolitical outcomes, such as differential exposure to monitoring, normative governance, and the potential reproduction of inequalities.

Third, qualitative analytic reflection applies the integrated conceptual framework to interpret how IoT-enabled surveillance mediates social control within urban environments. This interpretive stage draws on social control theory to examine how sensor-mediated visibility fosters behavioural regulation and compliance, on algorithmic governance studies to explore the automated and decentralized exercise of power, and on IoT network infrastructure theory to interrogate the material and spatial embeddedness of surveillance. Together, these perspectives facilitate a nuanced understanding of how citizen-state-technology relationships are reconfigured, how distinctions between public safety and pervasive monitoring are blurred, and how technological infrastructures can embed or exacerbate social inequities.

By combining document and policy review, empirical synthesis, and theoretically informed reflection, this methodology provides a robust framework for analyzing IoT surveillance as a complex sociotechnical phenomenon. It enables the study to move beyond purely descriptive accounts of technology or governance, offering instead a multidimensional critique of how smart-city infrastructures operationalize power, visibility, and social control.

Therefore, the methodological design of this study is directly informed by the integrated conceptual framework, ensuring that theoretical insights guide empirical inquiry and analytic interpretation. Each methodological stage corresponds to one or more strands of the framework. The document and policy review draws on IoT network infrastructure theory to examine how technical architectures and sensor distributions are codified in governance strategies, while insights from social control theory and surveillance studies shape critical evaluation of normative and regulatory assumptions about citizen behaviour and urban safety. The synthesis of empirical studies is primarily informed by surveillance and algorithmic governance perspectives, enabling a nuanced understanding of how automated systems operationalize control, produce visibility, and mediate social inequalities. Finally, the qualitative analytic reflection integrates all three strands social control theory, algorithmic governance, and IoT infrastructure theory to interpret the sociotechnical mechanisms through which IoT surveillance reconfigures citizen-state-technology relations, embeds power in urban infrastructures, and blurs distinctions between public safety and pervasive monitoring. This explicit alignment ensures methodological coherence, demonstrating that data collection, synthesis, and interpretation are not merely descriptive exercises but are theoretically grounded, allowing for a multidimensional critique of IoT-enabled social control in smart cities.

Table 1. Mapping Conceptual Strands to Methodological Stages

|  |  |  |
| --- | --- | --- |
| Conceptual Strand | Methodological Stage | Purpose / Analytical Focus |
| Social Control Theory | Document & Policy Review Qualitative Reflection | Examine normative assumptions about compliance, order, and behaviour regulation; interpret how surveillance shapes citizen conduct. |
| Surveillance & Algorithmic Governance | Empirical Synthesis Qualitative Reflection | Analyze automated decision-making, data-driven monitoring, and algorithmic control; assess social, ethical, and political implications. |
| IoT Network Infrastructure Theory | Document & Policy Review Qualitative Reflection | Explore technical architectures, sensor networks, and data flows; understand how material infrastructures operationalize surveillance and social control. |

The table maps each conceptual strand to its corresponding methodological stage and analytical focus. Social control theory and IoT network infrastructure theory guide the document and policy review as well as qualitative reflection, enabling examination of normative assumptions, social order, and how material infrastructures operationalize surveillance. Surveillance and algorithmic governance guide the empirical synthesis and qualitative reflection, supporting analysis of automated decision-making, data-driven monitoring, and associated social, ethical, and political implications. Together, all three strands converge in the qualitative reflection, the interpretive core of the study, integrating theoretical and empirical insights to analyze IoT-enabled social control in smart cities.

1. **KEY ARGUMENTS AND FINDINGS**

Our analysis of IoT-enabled surveillance in urban contexts highlights the intertwined sociotechnical and governance dynamics of smart cities:

**1. Infrastructure of Visibility and Un-Visibility**

IoT devices make urban activity increasingly legible to governance systems, yet the mechanisms of monitoring algorithms, sensors, and predictive analytics remain largely opaque. Citizens are rendered as data points they cannot fully observe or contest. This reflects social control dynamics, where visibility itself regulates behaviour, and the concept of the surveillant assemblage, where power operates through both presence and concealment (Auwal, 2025).

**2. Blurred Boundaries between Public Safety and Social Monitoring**

While initially deployed to enhance safety traffic management, environmental sensing, and incident detection IoT systems increasingly perform behavioural surveillance through anomaly detection. Automated decision-making shifts these technologies from service tools to instruments of control, illustrating algorithmic governance in practice.

**3. Differential Monitoring and Inequality**

IoT surveillance deployment is uneven. Certain urban zones, demographic groups, or behaviours are monitored more intensively due to policy priorities or infrastructure constraints. Algorithmic bias and structural inequalities further exacerbate disparities, making some populations more visible and therefore more regulated than others, particularly in contexts with institutional vulnerabilities such as Nigeria.

**4. Algorithmic Governance and Citizen Trust**

As IoT decision-making moves from human oversight to algorithms, transparency and accountability challenges arise. Citizens may feel monitored without recourse or understanding, highlighting ethical concerns regarding consent, legitimacy, and sociopolitical embedding of technology.

**5. Governance Conundrums**

The multi-layered governance of IoT involves state institutions, private tech providers, network operators, and citizens, creating complex coordination and accountability challenges. Legal frameworks often lag behind technology, particularly regarding privacy, data ownership, and oversight of algorithmic systems (Anwar et al., 2024).

**4.1 Synthesis:**

These findings illustrate that IoT-enabled surveillance is simultaneously a technical, social, and governance phenomenon. Sensor networks, algorithms, and governance frameworks co-produce visibility, control, and inequality. An integrative approach linking social control, algorithmic governance, and IoT infrastructure is essential to understand the embedded nature of surveillance in smart cities.

**4.2 Discussion**

The sociological implications of IoT-enabled surveillance in smart cities are profound and multifaceted. The embeddedness of IoT infrastructures comprising sensors, networked data flows, algorithmic systems, and institutional governance indicates that social control is increasingly mediated through technologically structured networks rather than solely through traditional social or legal mechanisms. Citizens are no longer merely objects of monitoring but active nodes within networked systems, subject to categorisation, classification, predictive modelling, and algorithmically mediated regulation. This networked social control challenges established notions of citizenship, autonomy, and privacy, reflecting the convergence of social control theory, surveillance studies, and IoT infrastructure analysis.

Technologically, IoT deployments generate complex networks of visibility and data circulation that urban planners, system architects, and service providers must navigate not only for operational efficiency such as latency, coverage, or system resilience but also for governance, ethical oversight, and social inclusion. The study’s findings on differential monitoring and algorithmic bias underscore that infrastructure design and deployment are not neutral; they structurally embed patterns of social inequality, particularly in contexts with institutional vulnerabilities, such as in parts of the Global South. Algorithmic decision-making further complicates accountability, as citizens may be monitored and managed by systems they cannot fully perceive or contest, producing epistemic asymmetries between the governed and governing entities.

Ethically and legally, these dynamics create tensions between the benefits of IoT surveillance improved public safety, environmental monitoring, and service efficiency and its risks, including surveillance creep, inequitable exposure, and reinforcement of existing socio-spatial disparities. Consequently, the findings strongly support the need for socio-technical audits of IoT infrastructures, transparency in algorithmic processes, equitable sensor network design, and inclusive governance frameworks that integrate technical, social, and ethical considerations. In short, the study demonstrates that IoT surveillance is a sociotechnical phenomenon where technical, political, and social layers are inseparably interwoven.

1. **CONCLUSION AND FUTURE RESEARCH DIRECTIONS**

This paper argues that integrating sociological theories of social control with analyses of IoT infrastructural networks provides a more comprehensive understanding of the “Internet of Surveillance” in smart cities. As IoT technologies become increasingly embedded in urban environments, distinctions between public service and surveillance, citizen and data-point, and network and control are progressively blurred. The study’s findings reveal that IoT infrastructures not only enable real-time monitoring and predictive governance but also produce differential visibility, algorithmic mediation, and socio-spatial inequalities.

Future research should advance in several directions. First, empirical case studies, especially in the Global South, are necessary to understand how networked surveillance interacts with local governance, institutional capacity, and social norms. Second, longitudinal analyses are needed to trace how IoT-enabled monitoring affects social behaviour, trust, and equity over time. Third, research should focus on designing privacy-preserving, accountable, and socially equitable IoT architectures. Specifically, future studies and policy initiatives should include:

1. Governance frameworks for IoT surveillance infrastructures that clarify responsibilities across state, corporate, and civic actors.

2. Fairness and equity audits of sensor network deployment and algorithmic decision-making to identify and mitigate differential monitoring.

3. Transparency and accountability mechanisms for algorithmic analytics embedded in urban networks, ensuring citizens understand, contest, and influence monitoring practices.

4. Inclusive design approaches that integrate social, ethical, and technical considerations, preventing IoT surveillance from reproducing or magnifying existing social inequalities.

By embedding sociological theory within the analysis of IoT networks, this study highlights that understanding and regulating urban surveillance requires an integrative, socio-technical lens one that simultaneously addresses infrastructure, governance, ethics, and citizen experience.

**REFERENCES**

Ahmed, A. (2023). Smart Cities and IoT: Examining the Potential Benefits and Challenges of Using IoT to Create More Efficient and Sustainable Urban Environments. *International Journal of Intelligent Systems and Applications in Engineering, 11*(10s), 306–320.

Anwar Zainuddin, A., Othman, A., Muhammad Zahid, N. A., Sofea Kamarul Zaman, N. A., Ahmad Razmi, A. N. M., & Azreen Kamarul Zaman, M. H. (2024). A comprehensive analysis of IoT security and privacy in smart city applications. *Bulletin of Social Informatics Theory and Application, 8*(1), 37–58.

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks, 56*, 122–140. <https://doi.org/10.1016/j.adhoc.2016.12.004>

Auwal, A. M. (2025). Invisible intrusions, internal threats and ethical vulnerabilities in Nigeria’s internet of things. *Discover Internet of Things, 5,* Article 128. https://doi.org/10.1007/s43926-025-00251-0

Cohen, S. (1985). *Visions of social control: Crime, punishment and classification*. Polity Press.

Durkheim, É. (1982). *The rules of sociological method* (S. Lukes, Ed.; W. D. Halls, Trans.). Free Press. (Original work published 1895)

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books.

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford University Press.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622. <https://doi.org/10.1080/00071310020015280>

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Islam, M., Dukyil, A. S., Alyahya, S., & Habib, S. (2023). An IoT Enable Anomaly Detection System for Smart City Surveillance. *Sensors, 23*(4), 2358.

Laghari, A. A., Li, H., Khan, A. A., et al. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover Internet of Things, 4*, 36. <https://doi.org/10.1007/s43926-024-00090-5>

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

Ntanda, A., & Carolissen, R. (2025). Technology’s dual role in smart cities and social equality: A systematic literature. *Journal of Local Government Research and Innovation, 6*(0), a238. <https://doi.org/10.4102/jolgri.v6i0.238>

Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation: Disparities and dangers of automated normativity. *Réactivation: Reinventing critical theory, 6*(1), 163–196. (English translation available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2382580>

Sayeed Anwar, U., Panda, U., & Mohapatra, H. (2024). Legal and Ethical Issues in IoT Based Smart City: Data Privacy, Surveillance, and Citizen Rights. *Journal of Computer Science Engineering and Software Testing, 10*(2), 17-26.

Seymour, K. (2024). Big brother: the effects of surveillance on fundamental aspects of social vision. *Neuroscience of Consciousness, 2024*(1), niae039.

Shi, W. (2025). A Framework for Ethical Judgment of Smart City Applications. *arXiv preprint*.