Title

Smart Cities as Social Constructions of Surveillance

Author

Mkheidze, Dachi

Publication Date

2026-03-16

Smart Cities as Social Constructions of Surveillance

Dachi Mkheidze[1]

[1]Civil & Environmental Engineering Department, University of California, Los Angeles

*dmkheidze@ucla.edu

Abstract: Using the Social Construction of Technology (SCOT) framework, this essay analyzes smart city infrastructure as a sociotechnical system that uses citizens as data points, raising critical legal, ethical, and equity concerns around surveillance, governance, and marginalized communities.

INTRODUCTION

Over the past two decades, the concept of the "smart city" has emerged as a dominant standard in urban planning and technological development. Governments and technology corporations increasingly use sensor networks, data analytics platforms, and algorithmic governance systems to optimize transportation, energy use, policing, and public services. Some people argue that these technologies make cities more efficient, sustainable, and responsive to citizen needs. However, scholars in science and technology studies (STS) advise that smart-city infrastructure is not merely a neutral technical upgrade to urban life. Rather, it represents a transformation in how cities govern populations through data-driven systems that continuously monitor, categorize, and analyze human activity. Within this context, citizens increasingly become sources of behavioral data that feed decision-making processes in both public administration and private-sector markets. "This work is in partial fulfillment of the ENGR184 course using the blueprint curriculum in Ref [1,2] and captured in a collection [3]"

METHODS

This study uses a qualitative socio-technical analysis to examine how smart-city infrastructure changes the legal and social status of citizens through continuous data collection and governance systems. Rather than measuring technological performance or efficiency, the research investigates how institutional power structures and political officials influence the design, deployment, and interpretation of smart-city technologies. The analysis is guided by the Social Construction of Technology (SCOT) framework, which views technological systems as socially shaped by competing groups rather than as neutral or inevitable innovations.

The research focuses on case-study analysis of prominent smart-city initiatives, particularly urban data infrastructures that collect and analyze citizen information. Examples include large-scale urban data collection projects such as Sidewalk Labs' Sidewalk Toronto project, municipal surveillance networks, and urban sensor platforms that monitor mobility, environmental conditions, and pedestrian behavior. These cases are selected because they represent widely cited examples of how smart-city systems use public governance, private technology firms, and large-scale data extraction. The goal of the case study approach is to identify how different stakeholders, including municipal governments, technology corporations, residents, and advocacy organizations, frame the purpose and risks of these technologies.

To analyze these cases, the study uses critical discourse analysis and document review of academic literature, policy documents, corporate reports, and public commentary related to smart-city technologies. This method allows the research to identify the dominant narratives surrounding efficiency, optimization, and technological progress, as well as competing critiques centered on privacy, surveillance, and democratic accountability. Particular attention is given to how policymakers and technology developers describe citizens within these systems, which is often as data points or behavioral inputs within algorithmic governance models. In addition to SCOT, the study uses intersectional critical frameworks, including insights from Black Feminist Thought and Disability Justice, to examine how surveillance-based infrastructures may disproportionately affect marginalized groups. These perspectives

are used as analytical tools to evaluate whether smart-city systems reproduce existing inequalities through biased datasets, surveillance targeting, or exclusionary design practices. By combining SCOT with these frameworks, the research investigates how technologies are socially constructed, and whose interests and experiences shape that construction.

RESULTS AND INTERPRETATION

To see SCOT and these power dynamics in action, we first consider two case studies of smart-city infrastructure: Sidewalk Toronto (Google Waterfront) and LinkNYC (NYC Wi-Fi kiosks). In 2017–2020, Waterfront Toronto partnered with Google's Sidewalk Labs to build a new "digital" neighborhood on the city's lakefront. The project promised innovations in housing and mobility, but also aimed to "capture and utilize a wide range of individual data, including citizens' daily travel routes and usage history of public facilities" (5). From a SCOT perspective, this smart-neighborhood proposal was contested by different groups. Sidewalk Labs and city planners framed data collection as needed for urban optimization, whereas local activists and residents framed it as a privacy and sovereignty violation. Citizen groups (e.g. #BlockSidewalk) and legal advocates (CCLA) demanded assurances about data storage and use. Initially, Waterfront Toronto had promised to store all collected personal data in Canada under Canadian law, but many citizens remained distrustful (5). This is an example of the fight between "innovation for public good" versus "unaccountable data extraction." It never fully stabilized, and ultimately, public opposition (rooted in concerns over privacy, consent, and corporate control) helped kill the project. In SCOT terms, the conflict among social groups (residents, a Google subsidiary, city officials) prevented a stable "closure" of the technology's meaning and led to its resolution. For the latter example, New York City installed over 7,000 LinkNYC kiosks to provide free Wi-Fi and phone charging. However, privacy advocates long warned that the kiosks, which are run by Intersection (a consortium including Google), are built to "see" passersby. Each kiosk includes cameras, Wi-Fi, Bluetooth sensors, and other trackers. As the NYCLU reports, nearly every New Yorker becomes a walking data point even without using the service; one's MAC address (device ID) and movements can be logged and correlated. Intersection's own presentations boast "hyper-targeting in the physical world" (Fig 1), real-time ads tailored to the age, income, location, etc., of people walking by.

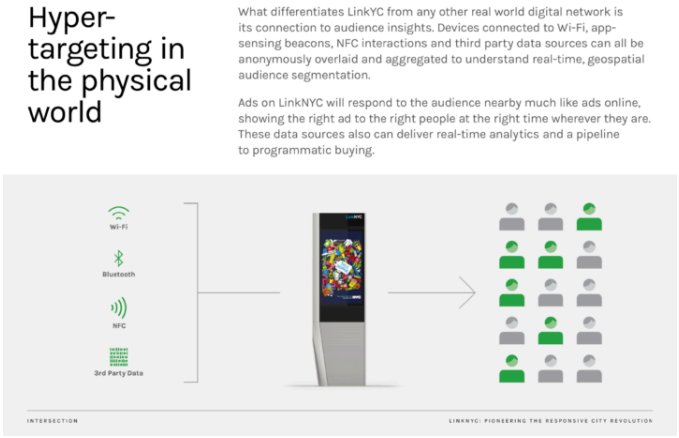

Fig. 1. Hyper-targeting infrastructure in smart city digital advertising networks (Ref. [6], Fig. 2)

In other words, public benches became audience-monitoring devices. From a SCOT standpoint, the relevant social groups, which included city leaders, advertisers, and tech vendors, compared to civil-liberties advocates, hold very different technological frames. Intersection/business interests view LinkNYC as a digital media platform to mine public attention; many citizens see it as intrusive surveillance and consumer profiling. Although LinkNYC remains operational, public backlash (and regulatory audits) have forced some policy changes (e.g., promises to anonymize data) (6). Nonetheless,

the kiosks illustrate how smart infrastructure can turn an entire population into a dense web of data points for corporate profit and municipal analytics.

Across cases, it is clear that powerful people shape smart-city design. As Hollands states, technology companies and entrepreneurial governments dominate the smart-city agenda. These groups set the problems that technology should solve (traffic, crime, and efficiency) and the data to collect. Other interests: privacy advocates, disabled people, women, and racial minorities are often treated as "stakeholders" at best (3). SCOT's concept of technological frames helps explain this: dominant groups see smart sensors as objective tools, whereas marginalized groups see them as tools of control or bias. For instance, Feminist Standpoint Theory tells us that scientific "objectivity" is shaped by perspective. The perspectives of women, racial minorities, and disabled persons can show problems others miss. In the smart-city context, ignoring these standpoints means ignoring how tech can harm marginalized bodies. Research on algorithmic surveillance shows that facial recognition systems are significantly worse at identifying Black and brown women than white men (Buolamwini & Gebru) (7). Feminist and Black feminist scholars (e.g., Simone Browne) have documented that Black people are historically over-surveilled, from slave-era "lantern laws" to modern CCTV (7). A critical scholar maps how Atlanta's "smart corridor" places sensors disproportionately in Black neighborhoods, thus entrenching racial control under the guise of "objectivity" (7). Dortdivanlioglu's feminist mapping project shows that invisible smart-city surveillance "protects and enhances power over marginalized communities" by making surveillance seem normal. In short, a queer or feminist lens would ask: whose safety is served by predictive policing sensors? Whose lives are made legible, and whose are erased?

Similarly, Disability Justice critiques show that smart-city data often excludes disabled needs. A recent study from ResearchGate found that U.S. city open-data portals rarely include information on curb cuts, crosswalk signals, or other features that disabled pedestrians require (8). What data we do collect reflects the city's default (able-bodied) norms. Indeed, Kate Crawford and disability scholars argue that algorithmic "fairness" research tends to flatten disabled people's varied experiences. If smart cities neglect accessibility data, they perpetuate disabling barriers. For example, sensors that optimize traffic flow might assume standard walking speeds, endangering people with mobility devices. A disability-informed SCOT analysis would highlight how "data points" of mobility leave out the thousands who never appear in datasets because they cannot use the same infrastructure. The "crip time" concept also tells us that time and movement are lived differently by disabled bodies, but smart systems rarely account for this variance.

From the viewpoint of Native Feminist/Settler Colonial analysis, smart cities often continue colonial logics. City infrastructure is built on land with colonial histories, and data collection can re-inscribe those injustices. For example, Smart City "open data" initiatives often ignore Indigenous Data Sovereignty: universal open-data mandates clash with Indigenous rights to govern their own information (9). Evergreen's analysis notes that smart-community projects usually did not involve Indigenous peoples in their planning, meaning "the goals of universal open data…conflict with the rights of Indigenous people to govern and steward their own data". In practice, this might mean sensor networks ignore tribal land boundaries or erode First Nations' control over environmental monitoring. A settler-colonial lens would question whether smart-city technologies treat the land (and its original stewards) as data resources without consent.

Treating people as data points also raises legal and ethical questions. In Sidewalk Toronto, citizens demanded that personal data be stored locally and kept under Canadian law (5), but large-scale data flows are hard to contain. Intersection's LinkNYC originally violated its own privacy pledges by storing unique MAC addresses and sharing data with third parties (10). Such practices show the lack of meaningful consent: most people never explicitly agree to constant location and behavioral tracking. Legally, questions arise: Who "owns" the data one generates by merely walking in public? Data-protection laws (e.g. GDPR) grant some rights over personal data, but smart-city systems often operate in legal gray zones or push new frontiers of interpretation. For example, U.S. police have used automated license-plate readers in low-income neighborhoods as revenue tools (10), not to prevent

crime, but to generate fines from those with few resources. Facial recognition bans in some cities only came after grassroots pressure highlighted their racial bias (10). SCOT reminds us that law and policy are themselves social constructions: rules are written by powerful groups and may lag behind technology. The question "can people be identified, monitored, followed? If so, how and by whom?" becomes political, not just technical. one report argues our cities have become "feudal data mines" where citizens' personal data (locations, communications, transactions) are "private property to be extracted…for prediction and social control" . In this context, calls for data sovereignty arise: advocates demand that data governance prioritize community interests, transparency, and civic oversight, not just corporate profit. Questions about race, gender, disability, or income become entangled with these legal-ethical issues, as marginalized people face both over-surveillance and exclusion from the promised benefits.

Critically engaging with smart cities means demanding community involvement at every stage. A SCOT analysis would tell policymakers: involve the relevant social groups, especially those usually marginalized, in the design and deployment of urban tech. This could look like citizen advisory boards on data ethics, participatory mapping of sensors (à la Dortdivanlioglu's activist maps) (7), and inclusive public comment processes. For example, after Sidewalk Toronto's failure, some experts recommended that future projects guarantee transparency and clear redress for data misuse. Data trusts or cooperatives have been proposed to give citizens actual control over how their data is used, a form of collective governance instead of private ownership. Other community initiatives could include data literacy workshops (so residents understand what is collected and why), neighborhood audits of existing infrastructure for bias, and partnerships with universities or non-profits to monitor smart systems. The University of Texas "Good Systems" project, for example, works directly with homeless-service groups and city agencies to ensure AI tools meet on-the-ground needs, rather than imposing one-size-fits-all fixes (10). Writing accessible reports or press releases (for local stakeholders, city councils, or mainstream media) can raise public awareness. Activists might lobby for legislation mandating Algorithmic Impact Assessments, which report on how smart-city tech affects privacy and equity. Tech-community events (hackathons, forums) could co-create open-source, community-controlled alternatives (for example, open GIS data projects that include disability and language accessibility features).

Crucially, engagement means listening to diverse standpoints. Drawing on Feminist Standpoint Theory, planners should see that women, people of color, disabled people, and queer communities experience the city differently. Design workshops with these groups can reveal insights (e.g. sensor networks might need different placements to aid transit-dependent wheelchair users). Black feminist methods would center on stories of how policing algorithms or commercial targeting have affected Black neighborhoods and women's safety. Disability justice approaches would insist on equal consideration of accessibility data (ramps, audio signals, etc.) and question any tech that excludes rather than empowers disabled people. Native/Indigenous perspectives would demand respect for land and data sovereignty: any "smart" mapping or sensor on ancestral land must have tribal consent and control (9).

CONCLUSIONS

Smart cities don't need to be surveillance cities. From Bridging Barriers, "We do not want smart cities to be code for surveillance cities, in which innovation compromises freedom, civil rights, and privacy". Achieving this requires rethinking the paradigm: instead of treating technology as destiny, we use SCOT's critical frame to ask "who benefits, who is harmed?" and to propose alternative visions of technology. Strategies could include privacy-preserving tech (differential privacy, local data storage), genuine opt-in citizen data commons, and legal guardrails enforced by active citizens. Activist scholars advocate for "data dignity," the idea that individuals maintain sovereignty over their own information by implementing methods like anonymization, encryption, and distributed computing. Blockchain or decentralized models ("crypto-cities") have even been floated as long-term visions to give residents more control. A SCOT-informed, intersectional critique of smart cities shows that these infrastructures reshape citizenship. When individuals become streams of data, their legal and social status is transformed – for better or worse, depending on who designs the system and whose values it encodes. By continually asking the critical questions above and engaging communities in governance,

we can challenge dominant technoscientific paradigms and steer smart-city development toward equity and justice rather than only efficiency or profit.

REFERENCES

1. "Participation Matters: The Social Construction of Digital Twins for Cities." ResearchGate, www.researchgate.net/publication/388398255_Participation_matters_The_social_construction_of_digital_twins_for_cities. Accessed 13 Mar. 2026.
2. "ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. X-4/W3-2022." Copernicus Publications, 2022, https://isprs-annals.copernicus.org/articles/X-4-W3-2022/205/2022/isprs-annals-X-4-W3-2022-205-2022.pdf Accessed 13 Mar. 2026.
3. "Critical Interventions into the Corporate Smart City." ResearchGate, www.researchgate.net/publication/273499619_Critical_interventions_into_the_corporate_smart_city Accessed 15 Mar. 2026.
4. "Digital Surveillance Capitalism and Cities: Data, Democracy and Activism." Humanities and Social Sciences Communications, Nature Publishing Group, https://www.nature.com/articles/s41599-024-03941-2 Accessed 13 Mar. 2026.
5. "Social Acceptance of Smart City Projects: Focus on the Sidewalk Toronto Case." Frontiers in Environmental Science, Frontiers Media, https://www.frontiersin.org/articles/10.3389/fenvs.2022.898922/full Accessed 13 Mar. 2026.
6. "LinkNYC Is a Privacy Disaster. Here's Why." New York Civil Liberties Union, www.nyclu.org/commentary/linknyc-privacy-disaster-heres-why Accessed 13 Mar. 2026.
7. "Mapping Invisible Surveillance on the North Avenue Smart Corridor, Atlanta." *Catalyst: Feminism, Theory, Technoscience*, https://catalystjournal.org/index.php/catalyst/article/view/36687 Accessed 13 Mar. 2026.
8. "Disability's Right to the Smart City." *ResearchGate*, www.researchgate.net/publication/385409170_Disability's_right_to_the_smart_city Accessed 13 Mar. 2026.
9. "Open Smart City Initiatives as Tools for Indigenous Data Sovereignty." Evergreen Resource Hub, https://evergreen.ca/resource-hub/resources/open-smart-city-initiatives-as-tools-for-indigenous-data-sovereignty/ Accessed 13 Mar. 2026.
10. "Smart Cities Cannot Be Surveillance Cities." Bridging Barriers, University of Texas at Austin, https://bridgingbarriers.utexas.edu/news/smart-cities-cannot-be-surveillance-cities Accessed 14 Mar. 2026.