Sharon Azarya*

Data Protection and Privacy in Smart Cities: A Critical Analysis of the IWGDPT Working Paper

1. Introduction

The rapid digitalization of urban environments has transformed cities into complex ecosystems of data collection, analysis, and automated decision-making. The International Working Group on Data Protection in Technology (IWGDPT) addresses this transformation in their working paper "Smart Cities," which provides a comprehensive framework for understanding the data protection challenges inherent in smart city development.[1] This essay examines the paper's key contributions to the discourse on urban digitalization, analyzing its tripartite framework of data collection, analysis, and decision-making, while evaluating the practical implications of its recommendations for cities, industry, and regulators.

2. The Smart Cities Framework: Beyond Definitional Debates

Rather than engaging in the contentious debate over what constitutes a "smart city," the IWGDPT paper adopts a pragmatic approach by focusing on the process of digitalization itself.[2] This methodological choice represents a significant contribution to the field, as it shifts attention from abstract definitions to concrete data protection challenges. The paper's three-stage framework—data collection, data analysis, and decision—provides a structured lens through which to examine the lifecycle of data processing in urban contexts.

The data collection stage encompasses diverse technologies ranging from Internet of Things (IoT) sensor networks and CCTV systems to the reuse of data held by public authorities and municipalities.[3] The analysis stage involves sophisticated processing techniques including data matching, artificial intelligence, profiling, and the construction of digital twins—digital representations of physical cities used for policy experimentation.[4] Finally, the decision stage encompasses the application of these analytical outputs to manage city resources, control urban functions, and inform policy development. This comprehensive mapping of smart city operations provides a foundation for understanding where data protection risks emerge and how they might

* Head of the International Department in the Israeli Privacy Protection Authority.

[1] International Working Group on Data Protection in Technology, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022, Written Procedure Prior to 71st Meeting on 7th-8th June 2023, 1.

[2] Ibid.

[3] Ibid, 2.

[4] Ibid.

be mitigated.

3. Accountability and Governance: The Foundation of Ethical Smart Cities

The paper's emphasis on accountability and governance as preconditions for smart city initiatives represents its most critical contribution. The IWGDPT argues that cities must conduct rigorous accountability assessments, including data protection impact assessments, before commencing any processing activities.[5] This proactive approach challenges the common practice of retrofitting privacy protections onto existing systems—a practice that has repeatedly proven inadequate in protecting individual rights.

The concept of identifiability receives particular attention in the accountability section. The paper correctly identifies that identifiability must be assessed not only in relation to specific processing operations but also in connection with associated processing that may enable indirect identification.[6] This holistic view of identifiability reflects an understanding of the cumulative privacy risks that arise when multiple data systems operate in proximity.

The Enschede case study illustrates the consequences of inadequate accountability measures. The municipality of Enschede implemented 24/7 Wi-Fi tracking in its city center, arguing that its anonymization techniques rendered the data non-personal.[7] However, the Dutch Data Protection Authority determined that the combination of hashed MAC addresses, timestamps, and location information constituted personal data, as the anonymization method did not sufficiently exclude the risk of singling out individuals.[8] This case demonstrates the importance of rigorous pre-implementation assessment and the limitations of technical anonymization measures when applied without adequate consideration of re-identification risks.

4. Data Minimization: Reconciling Innovation with Privacy

The principle of data minimization takes on particular significance in smart city contexts, where the temptation to collect comprehensive datasets for future, undefined purposes conflicts with fundamental privacy protections. The paper argues that when trend analysis is the objective, cities should aggregate data and strip identifiers as early as possible in the collection stage.[9] This approach represents a departure from the data maximalist logic that has dominated much of the technology sector's approach to urban digitalization.

[5] Ibid, 3.
[6] Ibid, 4.
[7] Ibid, 6.
[8] Ibid.
[9] Ibid, 8.

The Transport for London (TfL) Wi-Fi data collection initiative provides a positive example of data minimization in practice. TfL sought to understand customer movement through stations without identifying specific individuals.[10] By implementing automatic hashing using revolving cryptographic functions immediately after collection, and by refraining from matching Wi-Fi data with other datasets such as travel card information, TfL demonstrated that valuable urban insights can be obtained while respecting data minimization principles.[11]

The paper's recommendation that cities embed minimization practices into collection systems through technical measures—such as procuring sensors that strip identifiers before transmission—represents an important contribution to privacy by design discourse.[12] This approach shifts responsibility for data protection from individual choice or post-collection governance to the technical architecture itself, creating systemic safeguards that persist regardless of changes in personnel or organizational priorities.

5. Purpose Limitation: Confronting Function Creep

The multifaceted roles that cities play in citizens' lives create particular challenges for purpose limitation. The paper identifies a significant risk: that data collected for one municipal function—such as traffic management—might be repurposed for another function—such as law enforcement or social benefit determination—without adequate assessment or legal basis.[13] This phenomenon, often termed "function creep," poses serious threats to individual autonomy and institutional trust.

The smart homes case study illustrates the complexity of purpose limitation in practice. When sensors installed in social housing to monitor moisture and damp levels—a maintenance purpose—are proposed for use in identifying households eligible for fuel poverty benefits—a social welfare purpose—fundamental questions of compatibility arise.[14] The paper correctly identifies that even well-intentioned interventions into individuals' lives require either clear legal authorization or valid consent when they deviate from the original purpose.[15]

The recommendation for compatibility assessments when using data for purposes other than those for which it was originally collected provides a practical framework for addressing function creep.[16] However, the paper could have provided more detailed guidance on how cities should conduct such assessments, particularly when the new purpose might be characterized as serving the public interest.

[10] Ibid.
[11] Ibid, 9.
[12] Ibid, 8.
[13] Ibid, 10.
[14] Ibid, 11.
[15] Ibid.
[16] Ibid, 12.

6. Security and Transparency: Emerging Challenges

The paper's discussion of integrity and confidentiality highlights the security vulnerabilities inherent in the proliferation of IoT devices in urban environments. The reference to emerging legislative initiatives, such as the United Kingdom's Product Security and Telecommunications Infrastructure Bill, demonstrates growing recognition of IoT security deficiencies.[17] The prohibition of default passwords, requirements for vulnerability disclosure, and mandated security update periods represent important steps toward addressing these systemic weaknesses.

The transparency recommendations are particularly noteworthy for their recognition that smart city data collection is often "passive"—occurring without individual opt-in and potentially invisible to those affected.[18] The paper's advocacy for multiple transparency mechanisms, including signage at collection points, public registers of processing activities, and algorithm registers, acknowledges that different contexts and audiences require different communication strategies.[19]

The Amsterdam Algorithm Register is cited as an innovative approach to transparency, providing a publicly accessible listing of algorithmic processing occurring in the city.[20] Such initiatives represent a significant advancement over traditional privacy notice approaches, which typically provide information only to individuals directly affected by specific processing operations. By creating city-wide transparency mechanisms, municipalities can foster broader public understanding and democratic debate about the trajectory of urban digitalization.

7. Implications and Future Directions

The IWGDPT paper provides comprehensive and valuable guidance for data protection in smart cities, establishing a solid foundation for responsible urban digitalization. The paper's structured approach and practical recommendations offer cities, industry, and regulators a clear roadmap for implementing privacy-respecting smart city initiatives.

The paper's emphasis on accountability and governance reflects a forward-thinking approach that recognizes the complexity of modern urban data ecosystems. By placing data protection considerations at the forefront of smart city planning, the framework encourages cities to adopt proactive rather than reactive approaches to privacy protection. This preventive stance has the potential to build and maintain public trust, which is essential for the long-term success of smart city initiatives.

The incorporation of real-world case studies, such as the Enschede Wi-Fi tracking and Transport for London's privacy-preserving data collection, provides practical

[17] Ibid, 13.
[18] Ibid, 14.
[19] Ibid, 15-16.
[20] Ibid, 15.

illustrations that can guide cities in their implementation efforts. These examples demonstrate both the challenges and opportunities inherent in smart city development, offering valuable lessons for municipalities at various stages of digitalization.

Looking forward, the principles outlined in this paper provide a foundation for continued dialogue and development in smart city governance. The paper's invocation of Aristotle's assertion that cities exist to grant citizens "a complete and self-sufficient life"[21] reminds us that technological advancement must ultimately serve human flourishing. As smart city technologies continue to evolve, the framework established by this paper can serve as a touchstone for ensuring that innovation proceeds in alignment with fundamental rights and democratic values.

The collaborative approach advocated by the paper—involving cities, industry, regulators, and citizens—recognizes that successful smart city development requires multi-stakeholder engagement.[22] This inclusive vision suggests that the future of smart cities will be shaped not only by technological capabilities but by collective commitment to ethical principles and human-centered design.

8. Conclusion

The IWGDPT working paper on smart cities represents a significant contribution to the literature on urban digitalization and data protection. By providing a structured framework for analyzing data flows, identifying privacy risks at each stage of processing, and offering concrete recommendations for cities, industry, and regulators, the paper advances both theoretical understanding and practical implementation of data protection in urban contexts.

The paper's emphasis on proactive accountability, data minimization, purpose limitation, and transparency provides a foundation for developing smart cities that respect individual privacy while pursuing legitimate urban management objectives. The case studies, particularly the contrasting examples of Enschede's inadequate anonymization and Transport for London's privacy-preserving approach, offer valuable lessons for municipalities embarking on digitalization initiatives.

However, as cities continue to evolve into increasingly data-intensive environments, ongoing research and policy development will be necessary to address emerging challenges. The recommendations in this paper should be viewed not as a complete solution but as an initial framework that requires continuous refinement in response to technological developments, regulatory evolution, and lived experience of smart city initiatives. The ultimate success of smart cities will depend not only on their technical sophistication but on their ability to maintain the trust and support of the citizens they serve—a goal that can only be achieved through rigorous attention to data protection and respect for fundamental rights.

[21] Ibid, 1.
[22] Ibid, 5.

Bibliography:

1. *International Working Group on Data Protection in Technology*, Working Paper on "Smart Cities", Adopted at the 70th Meeting on 29th-30th November 2022.