the journal of CIVIC INFO

The Journal of Civic Information

Volume 6 | Number 3 October 2024

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Editor's Note: In Defense of Freedoms: Decentralized Networks as a Shield Against AI-Powered State Surveillance in Smart Cities

Ahmed Alrawi, Ph.D., Associate Editor, University of Virginia *

As artificial intelligence (AI) continues to advance, its integration into both state security agencies and urban infrastructures, specifically in smart city projects, has sparked significant concern. While AI surveillance tools are often praised for enhancing the monitoring, prediction, and prevention of threats, they also pose substantial risks to individuals' privacy and civil liberties. In recent years, AI-powered tools such as PredPol and Clearview AI have amplified the reach and efficiency of government surveillance, both virtual and physical, raising the crucial question of how we can protect our privacy in an age where AI enables unprecedented levels of surveillance. Our research article in this issue of the Journal of Civic Information, by Amy Kristin Sanders, Daxton "Chip" Stewart, and Steven Molchanov, demonstrates how difficult it can be for the public to acquire basic information about these technologies. More transparency, not opacity, is critical, given the ramifications of this technology on individuals' privacy and civil liberties.

U.S. state security agencies and municipal governments, including but not limited to the FBI, CIA, NSA, and urban administrative bodies, utilize AI-enhanced surveillance tools to track citizens' movements, communications, and behaviors within city spaces. These systems are undeniably capable of collecting, analyzing, and processing vast amounts of data in real-time, predicting patterns that may indicate potential high-security threats. However, the same technologies can also be used to infringe on personal privacy, suppress dissent, or target marginalized communities, particularly in urban areas where smart city technologies are prevalent.

Centralized surveillance systems, as typically seen in smart cities, raise concerns due to the vast power they consolidate within a single entity—often a city's administration or a contracted private company. This centralized control allows for deep monitoring of sensitive user information with little to no transparency in how this information is managed, sorted, and stored. Widely used surveillance processes on centralized networks like PRISM, XKeyscore, or Carnivore—utilized by agencies such as the NSA and FBI, are paralleled by smart city technologies that monitor everything from traffic patterns to pedestrian behavior. Such monitoring processes create a chilling effect on individuals' civil rights, including the fundamental freedoms of speech, religion, and assembly, thereby undermining the democratic principles that the government is supposed to protect. In its nature, the chilling effect within the surveillance context is defined by the Supreme Court as any state law or action that could hinder individuals' First Amendment rights (see, e.g., *Dombrowski v. Pfister*, 380 U.S. 479 (1965)).

On the other end of the spectrum, decentralized networks present an alternative to the centralized model of surveillance that *could be* employed in smart cities. In a decentralized network, the management, storage, and flow of data are governed by multiple entities rather than a single centralized authority. This reduces the likelihood of any one party, including state security agencies or municipal governments, gaining access to and control over large volumes of private data. By design, decentralized networks limit the possibilities of surveillance and make it more challenging for any central authority to control citizens on a massive scale. Further, decentralized networks are embedded with robust encryption and privacy-preserving layers, including algorithms that shield data from unauthorized access. Zero-Knowledge Proofs, Federated learning, and Distributed Ledger technology are considered vital techniques used in decentralized networks, allowing for the verification of certain information without revealing the data itself. This adds another layer of security against surveillance risks inherent in smart city technologies.

Decentralized systems not only make it more difficult for government security agencies and urban administrators to conduct widespread surveillance but also empower individuals with greater control over their personal data. Users can decide when, how, and with whom their information is shared, significantly decreasing the risks associated with data centralization typical in smart city frameworks. By shifting the power dynamics in favor of users, decentralized networks offer a more secure and privacy-respecting environment. The decentralization of data undoubtedly counteracts the chilling effect by reducing the ability of a single authority to control and suppress individual freedoms within urban spaces. When individuals feel confident that their communications and activities are protected from unwarranted surveillance, they are more likely to exercise their rights to free speech, assembly, and religion without *anxiety*. As such, decentralized networks play a crucial role in upholding the democratic principles that centralized surveillance systems in smart cities often threaten.

DOI: 10.32473/joci.6.3.137570

** Send correspondence about this article to Ahmed Alrawi, Postdoctoral Research Fellow, Digital Technology for Democracy Lab, University of Vir*ginia, *jkt5fv@virginia.edu*