

DATA PRIVACY & GOVERNANCE HUB

Cities Expand Use of AI-Powered Visual Data Systems Amid Growing Privacy Concerns

JULY 27, 2026

Key Takeaways

- U.S. cities are increasingly using AI-powered cameras and visual data systems to enhance public safety, traffic management, and other urban concerns.
- The public and digital privacy advocates have raised concerns about the use of surveillance systems.
- Experts have emphasized the importance of transparency, data governance policies, and safeguards surrounding data collection and sharing.

What Happened

Recently, cities in the United States have been implementing Artificial Intelligence (AI)-powered technologies, such as cameras, sensors, and public systems, to enhance surveillance and security. This practice is already being utilized in Brownsville, Texas, where [SHI International](#), a smart city technology company, has provided them to analyze visual data for particular incidents. Such incidents include illegal dumping, crowd and weapon monitoring, and license plate readers. SHI International has [stated](#) the purpose of providing such technology is to help city officials make faster, more informed decisions.

Like Brownsville, Texas, Las Vegas has adopted a similar strategy, implementing an [“advanced traffic safety analytics”](#) program to collect data on vehicle speeds, traffic volumes, and road safety risks. While city officials and first responders find this useful in improving public safety, members of the public and privacy advocates raise concerns surrounding data privacy,

accountability, and transparency.

Privacy and Governance Concerns

Concerns about privacy and the use of surveillance systems [existed](#) before AI was used for surveillance. The increased use of AI highlights major privacy concerns. Such technologies typically collect data through CCTV, cameras, and sensors, gathering a range of information, from images of individuals and vehicle data to daily activities.

Further, [facial recognition](#) has become another privacy concern, since it is used to aid law enforcement in identifying and tracking individuals. Another concern: [automated license plate readers](#) (ALPRs) for capturing license plates, which are also used to assist law enforcement in reading and gathering hundreds of [images](#) a minute. Both tools can create bias, misidentification, regulatory gaps, and consent and transparency issues.

One substantial concern is the potential for surveillance and profiling. Since these technologies are advanced, they ensure large amounts of data are captured and analyzed promptly, which allows for more efficient surveillance. However, this can be a significant concern if not done properly, such as inadvertently producing [biased](#) outcomes either from specific individuals or certain areas. Other issues related to privacy rights are who has authorization to collect data and how it will be stored and shared with third parties. It raises more concerns about proper safeguards for handling, storing, and collecting necessary data.

While organizations may not intend to monitor individuals perpetually, this is a major issue in privacy rights. Additionally, governance challenges raise privacy concerns about proper safeguards for handling and storing such data.

Why It Matters / Policy Considerations

Current safeguards, while not entirely sufficient, are maintained by several agencies, including the Department of Homeland Security (DHS), which ensures the proper use of AI for surveillance purposes. More specifically, [Directive 139-08](#) and [Directive 026-11](#) both list guidelines about proper oversight, the use of AI technologies in surveillance, and data handling and storage.

These concerns about data privacy bring the need for clear [communication](#) in policies and frameworks. Such policies and frameworks should include how individuals' information and data will be collected, clarification on how these technologies operate, and what safeguards are in place to protect sensitive information. Moreover, data minimization practices can also address privacy concerns.