SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

1350 Ave of the Americas
Fl 2, Box 1089
New York, New York 10019
www.StopSpying.org | (212) 518-7573

TESTIMONY OF
CORINNE WORTHINGTON
ADVOCACY AND COMMUNITY ENGAGEMENT MANAGER
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

BEFORE THE
NEW YORK ASSEMBLY STANDING COMMITTEES ON CONSUMER AFFAIRS AND PROTECTION, GOVERNMENTAL OPERATIONS, AND LOCAL GOVERNMENTS

FOR A HEARING CONCERNING,
THE USE OF AUTOMATED LICENSE PLATE READERS

DELIVERED
November 9, 2026

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

1350 Ave of the Americas
Fl 2, Box 1089
New York, New York 10019
www.StopSpying.org | (212) 518-7573

Good morning, my name is Corinne Worthington, Advocacy and Community Engagement Manager at the Surveillance Technology Oversight Project ("STOP"). STOP advocates and litigates for New Yorker's privacy rights, fighting discriminatory surveillance. I thank the Chairs and members of the Committees for the opportunity to give testimony today. S.T.O.P. urges the legislature to pass Assembly Bill 10808-A enacting much needed regulations on the use of automated license plate readers in the State.

Every day, automatic license plate readers (ALPRs) track the movements of millions of innocent New Yorkers every day. These systems are not just capturing isolated snapshots, they are building a detailed record of where people go: their daily commutes, their doctors' offices, places of worship, political rallies, and social activities. Across the country, this technology has been repeatedly abused by law enforcement officers to stalk romantic partners, harass subordinates, and locate victims of intimate partner violence on behalf of their abusers.[1][2][3] But the problems enabled by the vast data collection of these systems are not limited to the actions of rogue officers. Without common sense guardrails, this extensive surveillance infrastructure can be easily turned against vulnerable populations and those exercising their civil liberties, including healthcare seekers, immigrant communities, and protesters.

Risks to Civil Rights and Privacy

Unlike targeted investigative tools, ALPRs function as a dragnet, collecting data on the general public, not just suspects. Under current law, there are virtually no limits on how long this data can be kept, who can access it, or how it can be shared. Such warrantless surveillance undermines our constitutional protections, in particular our rights to freedom of association, speech, religion, and privacy under the First and Fourth Amendments. Courts are beginning to agree. In October, a federal judge in Oklahoma ruled that searching ALPR data without a warrant constituted a Fourth Amendment search.[4] The decision is indicative of the law's growing recognition of the magnitude of this technology's intrusion on privacy. Unfortunately, the law doesn't always move fast enough to

[1] https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/
[2] https://www.stopspying.org/content-input/stop-applauds-mamdani-canceling-cop-city-demands-mayor-go-further-to-dismantle-nypd-surveillance-n6yb5
[3] https://www.cbsnews.com/sanfrancisco/news/san-jose-police-officer-fired-alpr-data-improper-access-domestic-violence/
[4] https://www.404media.co/federal-judge-rules-a-flock-search-was-indiscriminate-mass-surveillance-and-unconstitutional/

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

1350 Ave of the Americas
Fl 2, Box 1089
New York, New York 10019
www.StopSpying.org | (212) 518-7573

stop these systems, meaning that vulnerable communities are still being targeted, tracked, and harmed by this technology.

In 2025, a Texas sheriff's office accessed a network of over 83,000 ALPRs to surveil a woman "...suspected of self-managing an abortion."[5] The search encroached into states like Washington and Illinois, where abortion access is legal, demonstrating how law enforcement exploits invasive surveillance technology across state lines.[6] Across New York, local police departments have conducted Flock searches on behalf of Immigration and Customs Enforcement (ICE) for civil immigration enforcement, placing immigrant communities in clear danger.[7] Sharing sensitive location data enables ICE to spy on immigrants during their routine activities, such as driving to work or taking their children to school.[8] During major demonstrations, such as the "Hands Off" and "No Kings" protests, "...more than 50 federal, state, and local agencies..." ran hundreds of warrantless searches through Flock's national ALPR database, where "...law enforcement specifically targeted known activist groups," underscoring how surveillance technology threatens our First Amendment freedoms.[9] [10]

The Need for Comprehensive Legislation

We need strict limitations on when ALPRs can be used, to dramatically reduce data retention periods, and to prohibit out-of-state sharing without explicit judicial oversight. A10808-A would enact robust and comprehensive protections characterized by the following:

- ALPRs can only be used for specific purposes: felony investigations, locating stolen vehicles or missing persons, parking and traffic enforcement, secured area access, and toll collection.
- Data must be deleted within 48 hours, unless the data is used as evidence in an investigation or pursuant to a warrant.
- No out-of-state sharing unless judicially authorized.

[5] https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down.
[6] https://www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down.
[7] https://www.stopspying.org/flock-favors
[8] "https://www.aclu-il.org/press-releases/ice-targeting-immigrants-based-automatic-license-plate-reader-alpr-data-supplied/.
[9] https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists.
[10] https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists.

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

1350 Ave of the Americas
Fl 2, Box 1089
New York, New York 10019
www.StopSpying.org | (212) 518-7573

- No commercial circumvention: Warrant requirement to access this information from data brokers.
- Mandatory audit logs of every query, including who, when, and why.
- Annual public reporting on camera locations, statistics, and privacy policies.
- Provides a private right of action: Individuals harmed by rogue ALPR use may sue for damages and attorney's fees.

A10808-A is not the only bill that has been introduced that seeks to regulate the use of ALPRs, however, it is the only one that would sufficiently protect New Yorkers. Several proposed pieces of legislation take the approach of trying to create "carve-outs" in ALPR use to protect communities such as abortion seekers. Unfortunately, not only do such bills fail to address the widespread harms posed by ALPRs, but they also leave the even the individuals they hope to protect vulnerable due to obfuscation by out-of-state law enforcement requesting information.

Conclusion

Unconstrained ALPR usage poses a definitive threat to New Yorkers by granting law enforcement an unprecedented and "Orwellian" capacity to monitor the public. These systems mainly target innocent drivers while proving largely ineffective at reducing actual crime. Moreover, the mass collection and retention of such sensitive data "just in case" undermines indispensable constitutional protections. By enacting this legislation, New York State will affirm its commitment to public safety, civil liberties, and the fundamental privacy rights enshrined in our Constitution.