November 9, 2026

The Honorable Nily Rozic
Chair, Assembly Standing Committee on Consumer Affairs and Protection

The Honorable John McDonald
Chair, Assembly Standing Committee on Governmental Operations

The Honorable Michaelle Solages
Chair, Assembly Standing Committee on Local Governments
New York State Assembly

New York Assembly
Legislative Office Building
Albany, NY 12248

Dear Chair Rozic, Chair McDonald and Chair Solages:

Thank you for the opportunity to present testimony on how Motorola Solutions responsibly deploys Automated License Plate Recognition (ALPR) technology in New York. At Motorola Solutions, our primary mission is to engineer safety and security tools that protect law enforcement officers and the communities they serve. We appreciate this opportunity to outline how our technologies support community safety while maintaining rigorous safeguards for individual privacy.

Our law enforcement partners routinely leverage our tools to achieve vital, life-saving outcomes—including rescuing abducted children, locating endangered seniors, identifying and stopping violent offenders, and dismantling organized auto-theft syndicates.

ALPR is a tool engineered specifically to help law enforcement solve crimes, locate missing individuals, and disrupt dangerous illegal activity. Within New York, our technology is already delivering tangible safety benefits such as:

- Assisting law enforcement in an East End Long Island community to solve a string of smash-and-grab thefts. By using ALPR, officers were immediately notified when the suspect vehicle reentered town, leading to an arrest that cleared open cases across multiple jurisdictions.

- Following a security breach where three individuals infiltrated underground infrastructure near accommodations for visiting foreign dignitaries, automated license plate readers (ALPR) were deployed to analyze real-time and historical vehicle patterns. The system successfully identified and tracked the fleeing suspects' getaway vehicle, enabling law enforcement to rapidly locate, arrest, and charge them.

Motorola Solutions engineers its ALPR technology exclusively to identify vehicles in public spaces using optical character recognition and non-personal, vehicle-related attributes, such as vehicle make, model, and color. The technology's hardware and algorithms are purpose-built for license plate capture and do not support facial recognition or human biometric tracking.

To help ensure these tools are operated responsibly, Motorola Solutions integrates the following rigorous data privacy controls, strict security standards, and regulatory compliance mechanisms directly into our platform architecture:

- **Default Zero Data Sharing:** Agency customers own and control their data. Company policy and contractual terms strictly prohibit Motorola Solutions employees from accessing customer data, with the sole exception of explicit, customer-supervised access granted for technical support.
- **Centralized Sharing Dashboards:** Our sharing dashboard enables administrators to maintain complete visibility over active data-sharing connections, allowing for quick modifications or bulk revocations at any time.
- **Automated Audit Logging:** Every system query is logged automatically. Administrators can generate and configure comprehensive reports detailing user identities, timestamps, and search justifications.
- **Responsible Data Retention:** Motorola Solutions' law enforcement customers set their own data retention schedules to comply with local and state laws, department standards, and Criminal Justice Information Services ("CJIS") requirements. We configure all new ALPR law enforcement products with a default data retention period of seven days.
- **Robust Security Systems:** Law enforcement customer accounts are managed independently by agency administrators under CJIS standards. Our platform requires, at a minimum, that users provide a case number, authorized purpose, and authorized reason to initiate a search.

We look forward to engaging with lawmakers as they work to develop legislation in this area to support responsible technology that protects both public safety with civil liberties. Motorola Solutions aligns with a national coalition of law enforcement officials—including but not limited to the International Association of Chiefs of Police ("IACP"), Major County Sheriffs of America ("MCSA") and the National District Attorneys Association ("NDAA")—in recommending an ALPR policy framework structured around three foundational pillars:

1. Data Ownership

- **Ownership:** Law enforcement agencies must retain 100% ownership and control over their ALPR data. Vendors must never pool, access, or share agency records.
- **Zero-Trust Default:** Data should only be shared with other law enforcement agencies for public safety purposes. For Motorola Solutions, the default for data sharing in our ALPR system is "off."
- **Hardware & Storage Integrity:** Deployments must use CJIS-compliant environments with hardware-level encryption to maintain the chain of custody. Motorola Solutions aligns with industry standards including ISO and NIST, and requires multi-factor authentication for access by all users.

2. Operational Safeguards

- **Investigative Leads Only:** An ALPR hit is a starting point, not proof of guilt. Officers must independently verify the license plate, state, and warrant status before taking enforcement action.
- **Civil Liberties Protections:** ALPR systems should be tied to documented public safety purposes. Usage targeting individuals engaged in lawful political, religious, or constitutionally protected activity must be strictly prohibited.
- **Retention Limits:** Data should be retained only as long as legally permitted and necessary for legitimate law enforcement investigative needs under local policy, then automatically purged.

3. Accountability

- **Audit Controls:** Systems should automatically log user activity including law enforcement searches and justifications. For example, every action in Motorola Solution's system is auditable and subject to routine supervisory audits.
- **Training and Limited Access:** Only trained and authorized individuals should have access to ALPR systems and data, and the number of individuals permitted to access these systems and data should be limited to only those who are necessary.
- **Transparency:** ALPR practices should be shared publicly with communities to build trust in the use of the technology.

Conclusion

Motorola Solutions remains deeply committed to ethical innovation, transparency, and accountability. Our Responsible Technology Blueprint serves as an operational framework to ensure our innovation aligns with strict ethical standards. This is further supported by our internal Technology Advisory Committee and our industry-leading AI Labels, which clearly disclose product technology types, intended uses, data ownership rules, and human oversight controls.

Motorola Solutions commends New York lawmakers for addressing the proper framework for ALPR deployment within the State. We welcome the opportunity to share operational best

practices and stand ready to partner with the Legislature to establish clear standards that enhance public safety while steadfastly protecting the civil liberties of all New Yorkers.

Thank you,



John Emling
Vice-President, Global Government Affairs & Public Policy

www.motorolasolutions.com

500 W. Monroe St
Chicago IL 60661