IACP Statement on the Responsible Use of

Automated License Plate Recognition Technology

The International Association of Chiefs of Police (IACP) strongly supports the lawful, ethical, transparent, and accountable use of Automated License Plate Recognition (ALPR) technology when it advances legitimate public safety objectives, including preventing and solving crime, protecting community members and officers, locating missing, endangered, and vulnerable persons, and recovering stolen property.

When properly used, ALPR can locate vehicles connected to violent crimes and other serious offenses, generate investigative leads, improve officer safety, and direct limited public safety resources more effectively. These capabilities strengthen emergency response and criminal investigations.

IACP's support for ALPR technology is grounded in an equally strong commitment to constitutional policing, individual privacy, civil rights, civil liberties, and public trust. Because ALPR systems may create records containing a license plate image, a contextual vehicle image, and the date, time, and location, agencies must carefully manage how this data is collected, accessed, retained, analyzed, and shared. Strong safeguards protect individual rights and sustain public confidence, essential to effective policing.

Responsible ALPR programs should include these core safeguards:

- Use ALPR technology and data only for a documented, lawful public safety purpose.
- Limit access to trained, authorized personnel and prohibit personal, political, retaliatory, discriminatory, commercial, or other unauthorized use.
- Maintain a comprehensive written policy covering authorized uses, deployment, hot lists, training, accuracy, access, security, sharing, retention, complaints, audits, and consequences for misuse.

- Treat each ALPR alert as an investigative lead, not conclusive evidence. Confirm the plate, jurisdiction, record status, and connection to the driver before taking enforcement action.
- Maintain tamper-resistant audit records and conduct regular audits, supervisory reviews, and periodic evaluations to verify authorized use, data accuracy, retention compliance, and public safety value.
- Investigate suspected misuse promptly. Apply appropriate corrective or disciplinary action, including administrative, civil, or criminal accountability, when warranted, and use audit findings to improve policies, training, security, and system controls.
- Protect ALPR data with appropriate cybersecurity, authentication, access controls, and data-integrity measures. Retain data only as long as it serves an authorized purpose, then purge it promptly.
- Share ALPR information only with authorized entities for legitimate purposes under written agreements that preserve access limits, security, auditing, retention requirements, and restrictions on secondary use. Document each disclosure.

In addition, to help address questions and concerns regarding ALPR technology, the IACP has convened a diverse working group of law enforcement leaders, practitioners, subject matter experts, and key stakeholders to develop guidance, resources, and leading practices that support the responsible use of ALPR systems.

As part of this ongoing effort, the IACP has launched a new ALPR Resource Page that serves as a central hub for information, tools, and educational materials on the responsible use of ALPR technology. The page will be regularly updated with new resources, guidance, and leading practices developed through the working group's efforts, providing agencies with practical tools to navigate the evolving policy and operational landscape surrounding ALPR.

Access the resource page here: ALPR Resource Page