Law Enforcement Principles for Responsible Use of Automated License Plate Recognition (ALPR) Technology

On behalf of the Association of State Criminal Investigative Agencies (ASCIA), International Association of Chiefs of Police (IACP), Major County Sheriffs of America (MCSA), National Association of Police Organizations (NAPO), National Alliance of State Drug Enforcement Agencies (NASDEA), National Association of Women Law Enforcement Executives (NAWLEE), National District Attorneys Association (NDAA), National Fusion Center Association (NFCA), National High Intensity Drug Trafficking Areas (HIDTA) Directors Association (NHDA), National Narcotic Officers' Associations' Coalition (NNOAC), National Real Time Crime Center Association (NRTCCA), National Sheriffs' Association (NSA), and Small and Rural Law Enforcement Executives Association (SRLEEA), we offer these model principles to support clear, enforceable policies governing law enforcement's use of automated license plate recognition (ALPR) technology.

For more than 20 years, ALPR technology and data have been critical tools for protecting the public. We recognize the recent concerns communities and policymakers have raised about law enforcement's use of this technology, and we believe those concerns deserve clear answers and strong safeguards. The principles below provide a framework for clear, enforceable policies with strong safeguards, transparency, meaningful accountability, and consequences for misuse. We are committed to working with policymakers and communities to protect against misuse while preserving a critical public safety capability that helps protect communities and save lives.

<u>How ALPR Works and Why Timely Access Matters</u>

ALPR technology captures still images - not continuous video - of vehicles and their publicly displayed license plates, along with the time and location of each image. ALPR systems can alert

law enforcement when a detected plate is associated with a stolen or wanted vehicle, a missing or endangered person, a person with an outstanding arrest warrant, or a vehicle connected to a crime. A single detection can narrow a search area, connect crimes across jurisdictions, rule out vehicles that are not involved, and help investigators focus limited resources on the right leads.

ALPR identifies a vehicle - not a person**.** It does not identify the driver or occupants of a vehicle. ALPR is not a surveillance tool and it is not used for traffic enforcement. A plate detection does not establish guilt and does not, by itself, provide probable cause for an arrest. ALPR provides an investigative lead that must be evaluated and appropriately verified before enforcement action is taken.

Immediate alerts are only part of ALPR's value. Serious crimes may not be reported immediately, investigations often develop over time, and missing people, victims, and dangerous offenders routinely cross jurisdictional boundaries. Preserving reasonable access to historical information and enabling responsible sharing among law enforcement agencies - with strong safeguards against misuse - can allow investigators to identify critical leads after a crime has occurred and act quickly when lives are at risk.

Principles We Support

A clear, enforceable framework for the responsible use of ALPR technology shall include the following principles:

- **Written policies.** Every law enforcement agency using ALPR systems must adopt and enforce clear written policies governing authorized uses, access, documented queries, verification, retention, sharing, data security, auditing, and accountability.
- **Permitted uses.** ALPR must be used by trained and authorized law enforcement personnel only for legitimate law enforcement and public safety purposes.
- **Authorized access.** System access must be subject to strong controls, routine auditing, and accountability for misuse—and promptly removed when an individual's duties no longer require it.
- **Auditing and accountability.** Agencies must maintain access logs, conduct routine audits, and investigate potential misuse. Policy violations shall result in meaningful discipline, up to and including termination, consistent with applicable due process requirements. Suspected criminal misuse must be referred to the appropriate authorities for investigation and potential prosecution under applicable law.
- **Required training.** Personnel with access to ALPR information shall receive initial and ongoing training on permitted uses, verification requirements, privacy and security protections, and the consequences of misuse.
- **Documented queries.** ALPR queries must be tied to an official case number or another documented law enforcement or public safety purpose, with query and access logs maintained for auditing and accountability.
- **Verification of plate matches.** ALPR information must be appropriately verified before enforcement action is taken. An alert alone does not identify the driver, establish guilt, or replace other investigative work.

- **Confidentiality.** ALPR data collected for law enforcement purposes must remain appropriately protected from public disclosure. Comparable protections must apply when a private company stores or manages the information on behalf of a government agency.
- **Meaningful retention.** Retention policies must preserve information needed for legitimate investigations while protecting privacy and security. The significance of a vehicle may not become apparent until weeks or months after a crime, particularly when a victim's report is delayed or an investigation develops over time. Strong access controls, documented queries, and auditing are more effective safeguards against misuse than destroying potentially important investigative information after an arbitrarily short time period.
- **Responsible data sharing.** Law enforcement must be able to responsibly share and query ALPR information across jurisdictions because missing people, victims, dangerous offenders, and criminal activity do not stop at jurisdictional boundaries. Sharing by agencies must be limited to legitimate law enforcement and public safety purposes and subject to appropriate controls and oversight. Government agencies must not sell access to ALPR data they collect.
- **Law enforcement access to non-governmental ALPR data.** The same restrictions, safeguards, and accountability requirements must apply to law enforcement's access to and use of ALPR data regardless of whether the data was collected by a government agency, a commercial provider, or another non-governmental entity.
- **Data security.** Law enforcement agencies, technology providers, and other entities that store or manage ALPR information must maintain strong security, access, and disclosure protections.

Working Together on a Responsible Framework

We are committed to working with policymakers and communities at the federal, state, and local levels to translate these principles into clear, workable, and enforceable policy. The goal is straightforward: **prevent misuse without preventing legitimate use.** Strong access controls, documented queries, auditing, training, and meaningful consequences can protect privacy and constitutional rights without sacrificing the capabilities investigators need to protect the public.