



Trust Before Technology

Constitutional Stewardship in an
Age of Intelligent Policing

Prepared by: Deputy Chief Dana S. Coston, Cape Coral Police Department

Date: August, 2026

Introduction

Every generation of law enforcement inherits new tools that promise to make policing more effective. Telegraphs gave way to radios. Fingerprints were supplemented by DNA. Paper maps became GPS. Patrol cars gained computers, body-worn cameras, drones, and sophisticated analytics. Today, one of those tools is the Automated License Plate Reader (ALPR).

Like every significant advancement before it, ALPR technology has generated important public discussion. Some view it as an indispensable investigative resource. Others worry that it represents an expansion of government surveillance inconsistent with a free society. Those concerns deserve to be heard. They also deserve thoughtful answers, not slogans, marketing claims, or false choices, but constitutional principles. This discussion is not fundamentally about cameras, software, or a particular vendor. It is about something much more enduring:

How should a constitutional democracy govern powerful technology while preserving the liberties it exists to protect?

That question will remain long after today's technology has been replaced.

The Constitution Comes First

Every police officer takes an oath not to a person, a political party, or a piece of equipment, but to the Constitutions of the United States and the State of Florida. That oath establishes an important order of priorities:

Technology serves policing

Policing serves the law

The law serves constitutional liberty

When viewed in that order, technology is neither inherently good nor inherently bad. It is simply a tool. Like every tool available to government, its legitimacy depends upon whether it is used lawfully, responsibly, transparently, and with appropriate restraint.

The Fourth Amendment remains our constitutional compass. Courts continue to evaluate how long-established constitutional protections apply to rapidly evolving technologies, distinguishing between settled precedent and questions that continue to develop. Responsible police leaders should neither overstate what the law currently permits nor ignore emerging legal questions simply because definitive answers have not yet been reached. Constitutional policing requires more than legal compliance. It requires humility before the law.

Public Trust Is Our Greatest Asset

Police agencies often discuss budgets, staffing, equipment, and technology. All of those matter. None are as valuable as public trust.

Communities willingly grant law enforcement significant authority because they expect that authority to be exercised fairly, transparently, and within constitutional limits. Trust cannot be purchased. It cannot be mandated. It is earned through consistent conduct. Every decision involving new technology is therefore more than a technical decision. It is a trust decision.

Citizens should expect their police department to explain not only what technology is used, but why it is used, what safeguards exist, who is accountable for its operation, what information is collected, how that information is protected, and what limits are intentionally imposed. Transparency, public notice, and accountability are consistently identified as foundational elements of responsible law-enforcement technology governance (International Association of Chiefs of Police [IACP], 2014).

Transparency is not a burden placed upon public safety. It is one of the foundations of legitimate public safety.

Capability Must Serve the Mission

Technology should never be adopted simply because it exists. Nor should agencies pursue innovation merely to keep pace with others. Every investment should answer a simple question:

What legitimate public safety capability does this create?

For ALPR technology, the answers are practical and measurable:

- It helps locate stolen vehicles.
- It assists investigators following violent crimes.
- It supports the recovery of missing or endangered persons.
- It generates investigative leads that may otherwise be unavailable.

It enables officers and detectives to spend more time exercising professional judgment and less time searching for information that technology can responsibly provide. ALPR systems can improve the speed and efficiency with which agencies identify vehicles associated with stolen-vehicle reports, missing persons, criminal investigations, and other legitimate public-safety purposes (Cape Coral Police Department [CCPD], 2025; Roberts & Casanova, 2012). These capabilities do not replace police judgment; they strengthen it.

At the Cape Coral Police Department, this philosophy extends well beyond any single technology. Through our Intelligent Policing Initiative, we have intentionally focused on using technology to improve decision-making, investigative effectiveness, officer safety, emergency response, and service to the community, not to replace the experience, discretion, and constitutional judgment of the men and women entrusted with enforcing the law (Coston, 2026).

Technology must also demonstrate effectiveness. A capability should not be preserved merely because it was purchased or because it appears innovative. It should be evaluated against defined objectives, measurable outcomes, operational performance, legal requirements, and its effects on the community. Both law enforcement and local government guidance emphasize defining the problem to be solved, aligning technology with strategic objectives, establishing performance measures, and continuously evaluating whether the system produces its intended value (Desai et al., 2024; IACP, 2014).

Capability, not novelty, is the standard.

Stewardship Before Innovation

Public discussion about policing technology often presents a false choice. Either agencies are expected to embrace every emerging technology, or they are expected to reject innovation altogether. Responsible leadership requires neither. Innovation is not a virtue in itself. Restraint is not a virtue in itself.

The responsibility of executive leadership is to ensure that every innovation is governed in a manner consistent with constitutional principles, public accountability, operational necessity, and the trust placed in democratic institutions.

At CCPD, we have adopted a simple philosophy:

Governance should precede deployment.

Before implementing new technologies, we establish policies, define authorized and prohibited uses, identify legal authority, assign supervisory responsibility, evaluate privacy and security risks, determine training requirements, and build safeguards designed to protect both the public and the integrity of our officers. These steps reflect recognized professional guidance calling for written policies addressing purpose, authority, management, operations, data collection, access, use, retention, oversight, evaluation, auditing, and enforcement before or alongside technological implementation (IACP, 2014).

We also consider whether a technology aligns with the City's broader priorities, whether it addresses a clearly defined public-safety problem, whether the organization possesses the capacity to govern it responsibly, and how its value will be measured

after deployment. ICMA guidance similarly recommends that local governments align emerging technologies with community strategy, involve operational and technical stakeholders, assess ethical and organizational risks, define performance indicators, and establish ongoing feedback mechanisms (Desai et al., 2024).

Technology should never outrun governance.

No technology relieves public officials of personal responsibility for the decisions they make. Technology may inform professional judgment, but accountability remains with the human beings who exercise governmental authority. CCPD's artificial-intelligence policy expressly requires independent human review and provides that AI-generated alerts, predictions, identifications, or recommendations may not serve as the sole basis for reasonable suspicion, probable cause, or enforcement action (CCPD, 2026).

Liberty Requires Governance

The conversation about technology should never end with capability. Capability without governance invites misuse. Governance without transparency invites distrust.

Both are essential.

Responsible use of ALPR technology requires clearly defined authorized purposes, written policy, legal authority, supervisory oversight, auditing, user accountability, training, data-quality controls, retention practices, access restrictions, information-sharing rules, cybersecurity protections, and meaningful consequences for misuse. Established ALPR guidance specifically identifies program objectives, deployment, training, hot-list management, data quality, access, sharing, retention, security, auditing, and sanctions as essential components of responsible program governance (Roberts & Casanova, 2012).

It also requires attention to the accuracy and currency of information used to generate alerts. An automated notification should be treated as an investigative lead requiring appropriate confirmation, not as a substitute for independent observation, professional judgment, or the legal justification required for police action. ALPR guidance recommends that personnel verify the accuracy of the plate read, confirm the issuing jurisdiction, ensure that the underlying alert remains current, and recognize that a vehicle's registered owner may not be its driver before acting upon a system notification (Roberts & Casanova, 2012).

CCPD's policy follows that principle. It distinguishes an unverified alert from a tentative or confirmed hit and prohibits personnel from using an LPR alert as the sole basis for a traffic stop or other enforcement action until required verification has occurred (CCPD, 2025). These safeguards are not obstacles to effective policing. They are evidence of **disciplined** policing.

Our policies and procedures governing artificial intelligence and automated license plate readers reflect this philosophy. They emphasize human responsibility for decisions, documented oversight, transparency, accountability, auditing, information security, authorized use, training, and constitutional compliance. They also require controls over access, protected information, public records, vendor practices, and the use of automated outputs in police decision-making (CCPD, 2025, 2026).

These policies also align with emerging CALEA guidance. CALEA's proposed artificial-intelligence standards call for written directives addressing authorized, restricted, and prohibited uses; human verification before law-enforcement action; documentation; training; accuracy and bias review; information security; annual audits; and mechanisms to disengage or deactivate systems that perform inconsistently with their intended purpose (Commission on Accreditation for Law Enforcement Agencies, Inc. [CALEA], 2026).

They also reflect an important principle: Governance is not complete when a policy is published. Systems must be reviewed. Performance must be measured. Access and searches must be auditable. Errors, bias, misuse, and security incidents must be identified and corrected.

Technologies that fail to perform consistently with their authorized purpose, legal requirements, or organizational values must be modified, restricted, or discontinued. Continuous evaluation, quality control, feedback, and the capacity to suspend deficient systems are recurring themes in contemporary law-enforcement accreditation and local-government governance guidance (CALEA, 2026; Desai et al., 2024).

Policies will undoubtedly evolve as technology, law, and public expectations evolve, but the principles behind them should remain constant.

The most important question is therefore not:

“Can this technology help solve crimes?”

The more important question is:

Can we demonstrate that its use consistently reflects our constitutional obligations and our commitment to public trust?

If that answer is not clearly yes, then governance, not technology, must improve.

Professional Standards and Public Accountability

CCPD does not develop its approach to emerging technology in isolation. Our governance philosophy reflects recognized principles across the law-enforcement and public-administration professions, including guidance from the International Association of Chiefs of Police, the Commission on Accreditation for Law Enforcement Agencies, the Police Executive Research Forum, and the International City/County Management Association.

Although those organizations approach technology from different perspectives, their guidance reflects several common expectations:

- Technology should serve clearly defined objectives.
- Policies should establish authorized, restricted, and prohibited uses.
- Privacy, civil rights, and civil liberties should be considered from the beginning, not after deployment.
- Information should be accurate, secure, appropriately limited, and retained only as authorized by law and policy.
- Personnel should be properly trained.
- Automated outputs should be independently reviewed before they influence consequential governmental action.
- Use should be documented and auditable.
- Performance should be evaluated against measurable outcomes.
- The public should receive meaningful information about how consequential technologies are used and governed.
- Community engagement should occur early enough to inform policy, not merely after decisions have already been made.

These principles are reflected across IACP's technology framework, CALEA's accreditation guidance, PERF's work on emerging police technologies and community engagement, and ICMA's local-government AI strategy framework (CALEA, 2026; Desai et al., 2024; IACP, 2014; Police Executive Research Forum [PERF], 2022).

These are not merely industry recommendations; they are the practical disciplines through which constitutional commitments become organizational conduct.

Constitutional Leadership in an Era of Change

Police executives today face a challenge that previous generations could scarcely imagine. Technological innovation now advances faster than legal precedent. Artificial intelligence, real-time crime centers, drones, biometric identification, predictive analytics, robotics, autonomous systems, and technologies yet to be imagined will continue to reshape policing.

This reality demands more than technical expertise. It demands constitutional leadership.

Leaders must resist two equally unhelpful impulses. The first is the assumption that every new technology should be adopted simply because it promises greater efficiency. The second is rejecting innovation simply because it introduces difficult questions. Neither approach reflects responsible stewardship.

The better course is deliberate evaluation grounded in constitutional principles, transparent governance, independent accountability, disciplined oversight, measurable performance, legal review, and ongoing public dialogue.

Engagement must also be meaningful. Public concerns should not be treated as barriers to overcome, but as information that can reveal risks, improve policy, strengthen safeguards, and help ensure that technology remains aligned with community expectations. PERF's guidance on emerging public-safety technologies emphasizes early communication, public education, stakeholder engagement, and opportunities for community input before and throughout implementation (PERF, 2022). Innovation and liberty are not opposing values. When properly governed, they reinforce one another.

Stewardship of Public Trust

The most important responsibility of a police executive is not acquiring advanced technology. It is ensuring that every capability entrusted to the organization is exercised in a manner worthy of the public's confidence.

That responsibility can be summarized in six enduring principles:

1. Technology should strengthen constitutional policing, not replace constitutional judgment.
2. Public safety and individual liberty are complementary responsibilities, not competing objectives.
3. Transparency strengthens legitimacy.
4. Governance determines trustworthiness.

5. Organizational capabilities should always expand within constitutional boundaries.
6. Every technological decision should withstand public explanation. If a police agency cannot confidently explain why a capability exists, how it is governed, what information it uses, how its effectiveness is evaluated, and what safeguards protect individual rights, then it has more work to do.

These principles apply equally to license plate readers, artificial intelligence, drones, facial recognition, robotics, autonomous systems, and technologies yet to be invented. The tools will change; the principles should not.

Looking Beyond Today's Debate

History suggests that many technologies initially viewed with skepticism eventually become accepted components of modern policing, while others evolve under new legal and policy safeguards as courts, legislatures, police agencies, and communities refine the balance between public safety and individual liberty.

What endures is not the technology itself. What endures is the manner in which public servants choose to govern it. Future generations will not judge today's police leaders simply by whether we adopted a particular technology. They will judge whether we exercised the wisdom to govern powerful capabilities without compromising the constitutional values that give those capabilities legitimacy.

Our legacy will not be measured by the sophistication of our tools. It will be measured by the fidelity with which we preserved public trust while using them. The question before us has never been whether technology will continue to evolve.

It will.

The enduring question is whether those entrusted with that technology will exercise their authority with wisdom, restraint, transparency, and unwavering fidelity to the Constitution.

For the Cape Coral Police Department, trust is not something technology creates. It is the standard against which every technology must ultimately be judged. Public trust is earned not by possessing sophisticated tools, but by demonstrating that every capability is governed by enduring principles. Constitutional policing is therefore defined not by the technologies we adopt, but by the values we refuse to abandon.

References

1. Cape Coral Police Department. (2025). *CPD-23: License plate readers* [Standard operating procedure].
2. Cape Coral Police Department. (2026). *A-7: Artificial intelligence* [General order].
3. Commission on Accreditation for Law Enforcement Agencies, Inc. (2026). *Standards for law enforcement agencies: Proposed artificial intelligence standards 80.2.1–80.2.4* [Proposed accreditation standards]. <https://www.calea.org/sites/default/files/2026-03/Law%20Enforcement%20to%20Post%2020260314.pdf>
4. Coston, D. S. (2026). *The evolution of the Tactical Information and Analytics Center: Building a real-time operational intelligence, analytics, and situational-awareness capability for the Cape Coral Police Department* [Internal white paper]. Cape Coral Police Department.
5. Desai, H., Fullerton, K., & Ingram, L. (2024). *Local government AI strategy workbook: A guide for municipalities to begin thinking about their community's AI strategy*. International City/County Management Association. <https://lgr.icma.org/wp-content/uploads/2024/04/Use-of-Artificial-Intelligence-in-Local-Government-Strategy-and-Tools-1.pdf>
6. International Association of Chiefs of Police. (2014). *IACP technology policy framework*. <https://www.theiacp.org/sites/default/files/Technology%20Policy%20Framework%20January%202014%20Final.pdf>
7. Police Executive Research Forum. (2022). *Community engagement strategies for state, local, tribal, and territorial law enforcement agencies considering the use of unmanned aircraft systems*. <https://www.policeforum.org/assets/DronesCommunityEngagement.pdf>
8. Roberts, D. J., & Casanova, M. (2012). *Automated license plate recognition use by law enforcement: Policy and operational guide, summary*. National Institute of Justice. <https://www.calea.org/sites/default/files/LPR%20Guidance.pdf>