Talking points regarding the IACP Technology Policy Framework

The pace of technology development continues to expand.

- Technology continues to evolve at an exponential pace and it's playing an increasingly important role in supporting the daily work of officers in the field, making them safer, better informed, more efficient and effective.

The array of technologies available to law enforcement executives is extensive.

- In-car and body-worn video, public and private video surveillance systems, automated license plate recognition, facial recognition and other biometric technologies, GPS tracking devices, unmanned aerial systems (drones), gunshot detection systems—all of these technologies have the potential to enhance law enforcement operations, and improve public and officer safety.

Some agencies have implemented technologies without providing policy guidance governing its deployment, use, and how data are collected, used, shared, and retained.

- A 2009 survey of law enforcement agencies by IACP found that fewer than half of 40 agencies responding to a survey on ALPR use had policies in place governing the deployment and use of the systems (19 agencies, or 48%), though an additional 15% (6 agencies) were in the process of developing policies.
- Similarly, the Major Cities Chiefs Association (MCCA) reported in January 2013 that 40 percent of member agencies responding to a survey indicated that they had no policy regarding ALPR usage and 15 percent were developing a policy (n=27 agencies).
- The ACLU report, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, which was published in July 2013, raised important questions about ALPR data collection, use, retention, and sharing.
- Many communities around the nation have acted or are considering action to limit or reject the use of some technologies, including ALPR, UAS, red-light cameras, and video surveillance systems. Maine, Massachusetts, Wisconsin, Michigan, Iowa City (Iowa), etc.
- Failure to have and enforce policies can erode public confidence, promote widespread fears of privacy violations, and may provoke external limitations on the adoption or use of technologies.

Policies must be in place to assure the public that their privacy, civil rights, and civil liberties are recognized and protected.

- Creating and enforcing comprehensive agency policies governing deployment and use of these technologies, and the data they provide, is a critical step that agencies must take in assuring the public that their privacy, civil rights, and civil liberties are recognized and protected.
- Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Policies help to ensure uniformity in practice across the agency and to enforce accountability.
- Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

The IACP has created this Technology Policy Framework, in consultation with representatives of numerous IACP Divisions, Sections, Committees, our Policy Center, other professional law enforcement organizations, and our Federal Partners, to assist IACP Members and law enforcement executives in creating policies that will support responsible technology deployment and use.

The IACP has identified universal principles that agencies should use in developing their agency policies. These principles are widely recognized and reflect core values of our nation.

- Specification of Use: Define the purpose of the technology and the data captured
- Policies and Procedures: Policies should be developed and enforced surrounding the use of technologies and the data they provide
- Privacy and Data Quality: Respect the privacy interests of all persons and ensure the quality of data
- Data Minimization and Limitation: Only those technologies, and only those data that are strictly need to achieve specific objectives will be deployed, collected, and retained, and only as long as it demonstrates tangible value.
- Performance Evaluation: Agencies should regularly monitor and evaluate the performance and value of technologies in assessing whether continued use is warranted.
- Transparency and Notice: Agencies should employ open and public communication regarding the use of technologies
- Security: Agencies should implement security safeguards to prevent risks of loss, unauthorized access, destruction, modification, and disclosure.
- Data Retention, Access, and Use: Agency policies should clearly articulate data retention, access, and use practices, and these should be aligned with agency strategic plans and comport with applicable local, state, and federal laws and regulations.
- Auditing and Accountability: All deployment and use of these technologies, and the data they provide, should be audited to assure compliance with policy, and anyone with access should be held accountable.

The IACP has outlined core elements that should generally be addressed by agencies in developing their agency technology policies.

- The recommended elements are designed to ensure that agency policies are comprehensive and address both operational deployment factors and the universal principles identified in the document.

Like all resources and tools available to law enforcement, the use of new technologies must be carefully planned and managed. The development of agency policies is a proven way for executives to ensure they are implementing technologies that will provide the greatest public safety benefits, while protecting the privacy, civil rights, and civil liberties of citizens