New technologies enable state and local law enforcement agencies to investigate crimes in ways once thought impossible or impractical. Across the nation, lawmakers are debating and enacting legislation that addresses how police can use these innovative tools to maximize public safety while complying with the Fourth Amendment’s prohibition against unlawful search and seizure. Unmanned aircraft systems (UAS) and cell phones are two technologies on which much recent legislative attention has focused.

**Police Use of Unmanned Aircraft Systems**

*Warrant Requirements for UAS Use* - Fourteen states have enacted laws that address police use of UAS, commonly called drones. Thirteen of those states enable police to use UAS pursuant to a warrant, while Virginia prohibits their use by law enforcement agencies until July 1, 2015. In Iowa, law prohibits UAS from being used to enforce traffic violations.

*Operational Standards for Police use of UAS* - Laws in at least five states require that agencies adopt standardized protocols for police use of UAS. Alaska’s law requires that law enforcement agencies adopt procedures that ensure: the appropriate Federal Aviation Administration authorization is obtained; UAS operators are trained and certified; a record of all flights is kept and there is an opportunity for community involvement in the development of the policy. Similar laws in Iowa, Texas and Virginia require state agencies to develop protocols for law enforcement’s use of UAS. In North Carolina, the law requires all state personnel that operate a UAS to complete a knowledge and skills test developed by the state Division of Aviation.

*UAS Reporting Requirements* - States are also implementing reporting requirements for UAS use by law enforcement. Utah’s law requires law enforcement agencies to report annually on their use of UAS. Among other requirements, the report must include: the number of times an unmanned aircraft was used; the number of criminal investigations that were aided; the manner in which criminal investigations were aided; the cost of acquiring, maintaining, repairing, and operating each unmanned aircraft; and the data that was collected on any person, structure, or area. Similar reporting laws have been enacted in Illinois and Texas.

Two states, Oregon and North Carolina, require government UAS to be registered with certain state offices. Oregon’s law requires all public entities using UAS to register them with their state Department of Aviation while North Carolina’s law requires any state entity acquiring a UAS to get approval from the state chief information officer.

*Data Collection and Retention Polices* – At least two states, Illinois and Utah, have created statutory standards for the retention and deletion of data obtained using UAS. Illinois’ law requires law enforcement agencies to destroy all information gathered by UAS within 30 days unless there is reasonable suspicion that the information shows evidence of criminal activity. Utah’s law prevents law enforcement agencies from using UAS collected data related to any person, structure, or area that was not the specified target of an investigation or is not directly displaying criminal activity.

*Third Party UAS Use and Data Sharing with Law Enforcement* - Laws in Illinois and Utah address how private citizens or companies can share with police information obtained by use of their own UAS. Illinois’ law requires police to follow warrant protocols to compel third parties to share information. If the information is voluntarily shared with police, authorities are required to follow the state’s law governing UAS data retention and disclosure. In Utah, the public can share UAS obtained information with law enforcement if the data captures the commission of a crime or imminent or ongoing danger.
Police Use of Cell Phone Surveillance Technology

Cell phones, the information they contain, and the location data they transmit can significantly aid police during investigations. State and federal decision-makers have weighed in on the appropriate police use of cellular information. On June 25, 2014, the United States Supreme Court ruled in Riley v. California that warrants are generally required before police can search the contents of an arrestee’s cell phone. In addition, at least 10 states have enacted warrant requirements for police before they are able to acquire location or stored data from cellular devices or telecommunication companies.

Under certain emergency situations law enforcement is able to collect information from cell phones, or obtain location data without first procuring a warrant. Under Indiana and Virginia law, if a police officer obtains location data based on exigent circumstances, they must obtain a court order within 72 of their initial use of the tracking device.

Reporting Requirements - Minnesota’s law requires that each request for a warrant for location data be reported to and tracked by the state court administrator. The information collected by the state court administrator must include whether the warrant application was accepted or denied, the time period of its authorization, the nature of the monitoring and the identity of the police officer or agency requesting the warrant. This information is required to be reported to the Legislature biannually.

Notification Requirements - Utah’s law requires police who obtain a warrant for location data to notify the owner of the targeted electronic device within 14 days of the conclusion of the operation. Law enforcement must notify the owner that a warrant was issued, of the time period for which data was collected and of the alleged offense.

Enhanced Protections for Journalists - In Indiana, when police request a warrant for location data for a member of the media, the journalist or news entity targeted must be given notice of the request and the ability to be heard in court concerning the issuance of the warrant. Police are not required to notify journalists if they are the target of a criminal investigation and notifying them would pose a risk to the integrity of the investigation.

References:
