Department of Legislative Services

Maryland General Assembly 2017 Session

FISCAL AND POLICY NOTE First Reader

House Bill 37 Judiciary (Delegate Conaway)

Public Safety - Local Law Enforcement Surveillance Programs and Equipment - Reporting

This bill requires a "local law enforcement agency" to send written notification of the operation of electronic surveillance equipment, within 30 days after initiating the operation, to the local governing body of the county or municipal corporation in which the local law enforcement agency is located. By January 31, annually, each local law enforcement agency that operates electronic surveillance equipment must submit a comprehensive report to the local governing body of the county or municipal corporation in which the local law enforcement agency is located regarding the operation of all electronic surveillance programs and equipment by the local law enforcement agency in the previous calendar year.

The bill takes effect January 1, 2018.

Fiscal Summary

State Effect: None.

Local Effect: Minimal. The bill's notification and reporting requirements can generally be handled with existing budgeted resources of local law enforcement agencies. Revenues are not affected.

Small Business Effect: None.

Analysis

Bill Summary: "Local law enforcement agency" means an agency of a county or municipal corporation in the state that performs police protection functions.

Current Law: While State law authorizes a court to issue an order authorizing or directing a law enforcement officer to obtain "location information" from an "electronic device," there is no requirement for law enforcement to provide notification to the local governing body of the county or municipal corporation in which the law enforcement agency is located.

"Location information" means real-time or present information concerning the geographic location of an electronic device that is generated by or derived from the operation of that device. In general, the period of time during which location information may be obtained under a location information order may not exceed 30 days. Within 10 calendar days after an order is issued, law enforcement must begin to obtain location information or, if applicable, deliver the order to the service provider. If neither of these two events occurs within 10 calendar days after the issuance of the order, the order is void.

Notice of the location information order must be delivered to the user and, if known and if the owner is a person or an entity other than the user, the subscriber of the applicable electronic device. Notice must be delivered within 10 calendar days after the expiration of the order. However, a court, on a finding of good cause, may order that the application, affidavit, and order be sealed and that the required notification be delayed for a period of 30 calendar days. A finding of good cause may be established by evidence that (1) the criminal investigation to which the affidavit is related is of a continuing nature and likely to yield further information that could be of use in prosecuting alleged criminal activities and (2) failure to maintain confidentiality of the investigation would jeopardize the use of information already obtained in the investigation, impair the continuation of the investigation, or jeopardize the safety of an information source.

A court may order that notification be delayed beyond 30 calendar days if a law enforcement officer provides continued evidence of good cause and the court makes a finding of good cause based on evidence that notice should be further delayed to preserve the continuation of the investigation.

A law enforcement officer may obtain location information without an order for up to 48 hours in exigent circumstances or with the express consent of the user/owner of the electronic device.

Background: The Fourth Amendment to the U.S. Constitution protects individuals from unreasonable searches and seizures by the government and has been interpreted to create a HB 37/ Page 2

right of privacy. The reasonableness of a governmental search often depends on the reasonableness of the expectation of privacy on the part of the person subject to the search, the location of the search, and the breadth of information gathered.

Generally, U.S. Supreme Court decisions have held a warrantless search of an individual's home to be unreasonable, with certain clearly delineated exceptions. However, courts have also held that the Fourth Amendment does not protect individuals from searches that take place in "open fields" because it is unreasonable for a person to have an expectation of privacy over activities that take place in such areas. Technological advances have made traditional legal standards that were often location based difficult to apply, and courts and lawmakers have increasingly had to grapple with the threshold question of whether information gathered through emerging technology constitutes a search at all.

Recently, discussion has focused on (1) law enforcement's use of cell site simulators that effectively turn cell phones into real-time tracking devices and (2) video monitoring of large geographic areas by air over long periods of time. Much of the controversy regarding such technologies has centered on (1) the scope of information gathered and the legal requirements for use of the technologies as they relate to an individual's Fourth Amendment right to privacy and (2) the lack of transparency in acquiring and deploying the technologies.

On August 26, 2016, Bloomberg Businessweek revealed that the Baltimore City Police Department, with funding from a private donor, had authorized the firm Persistent Surveillance to conduct aerial surveillance of a large portion of Baltimore City. Public concern over the program and the lack of notice provided to the public has been compounded by revelations that the Baltimore City Council, Mayor Stephanie Rawlings-Blake, and many other city and State leaders were not made aware of the department's activity until many months after the program began. A main concern regarding the technology is the breadth of what is captured. Rather than just focusing on suspects, the outdoor activity of every citizen in a 30-mile radius is recorded and stored.

Persistent Surveillance and other proponents of the technology claim that, as currently designed, very little detail is captured by the cameras. Individuals appear as little more than a pixel and cannot be personally identified because of the low quality of the images. Opponents and privacy experts indicate that, in a competitive market, it may only be a matter of time until highly detailed, high resolution, real-time aerial surveillance becomes a reality. What information may be stored and for how long also remains an open question.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Baltimore City; Montgomery and Talbot counties; Maryland Association of Counties; City of Frederick; Maryland Municipal League; Department of Legislative Services

Fiscal Note History: First Reader - January 26, 2017

lc/lgc

Analysis by: Shirleen M. E. Pilgrim Direct Inquiries to:

(410) 946-5510 (301) 970-5510