Department of Legislative Services

Maryland General Assembly
2014 Session

FISCAL AND POLICY NOTE
Revised

Senate Bill 698 (Senator Shank, *et al.*)
Judicial Proceedings Judiciary

Criminal Procedure - Electronic Device Location Information - Order

This bill authorizes a court to issue an order authorizing or directing a law enforcement officer to obtain "location information" from an "electronic device." "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. The bill (1) establishes requirements for an application for a location information order and (2) requires disclosure of specified information to a user/owner.

A person may not be held civilly liable for complying with the bill's provisions by providing location information.

Fiscal Summary

State Effect: Minimal increase in general fund expenditures for AOC to comply with the bill's requirements.

Local Effect: Minimal increase in local expenditures for local law enforcement units and circuit courts to comply with the bill's requirements.

Small Business Effect: None.

Analysis

Bill Summary:

Issuance of Order: A court may issue an order by application on a determination that there is probable cause to believe that (1) a misdemeanor or felony has been, is being, or

will be committed by the user/owner of the electronic device or the individual about whom electronic location information is being sought and (2) the location information being sought is evidence of, or will lead to evidence of, the misdemeanor or felony being investigated or will lead to the apprehension of an individual for whom an arrest warrant has previously been issued.

Application for Order: An application for an order must be in writing, signed and sworn to by the applicant, and accompanied by an affidavit that sets forth the basis for the probable cause and contains facts within the personal knowledge of the affiant. The order must (1) contain specified information; (2) authorize the executing law enforcement officer to obtain the location information without giving notice to the user/owner of the electronic device or to the individual about whom the location information is being sought for the duration of the order; (3) specify the period of time for which the disclosure of information is authorized; and (4) if applicable, order the service provider to disclose to the executing law enforcement officer the location information associated with the electronic device for the period of time for which disclosure is authorized and refrain from notifying the user/owner of the electronic device or any other person of the disclosure of location information for as long as the notice is authorized to be delayed.

Duration of Order: 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.

A location information order may be extended beyond 30 calendar days on a finding of continuing probable cause. An extension may not exceed an additional 30 calendar days unless the court finds continuing probable cause and determines that good cause exists for a longer extension.

Notice of Order to Owner or User of Electronic Device: 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. The notice must state the general nature of the law enforcement inquiry and inform the user/owner (1) if applicable, that location information maintained by the service provider was supplied to a law enforcement officer; (2) if applicable, the identifying number associated with the electronic device; (3) the dates for which the location information was supplied; (4) whether notification was delayed; and (5) which court authorized the order.

The 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.

Exceptions to Order Requirement: 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.

Current Law:

Stored Wireless and Electronic Communications and Transactions Access Act: The Stored Wired and Electronic Communications and Transactions Access Act statute describes the procedures investigative or law enforcement officers must follow to obtain specified electronic communication information. The statute can be divided into two components – requests for contents of wire or electronic communications and requests for records or other noncontent information.

With respect to records or other noncontent information, law enforcement officers seeking disclosure of the "records or other information" pertaining to a subscriber or customer may obtain the information through a subpoena, court order, warrant, or consent.

"Record or other information" includes names, addresses, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service, including any credit card or bank account number. "Record or other information" does not include the content information subject to warrant requirements or other procedural requirements under the Act.

A provider of electronic communications service or remote computing service may disclose a "record or other information" pertaining to a subscriber to or a customer of the service to any person other than an investigative or law enforcement officer.

However, a provider of an electronic communication service or a remote computing service must disclose a record or other information pertaining to a subscriber to or a customer of the service to an investigative or law enforcement officer only if the officer:

- uses a subpoena issued by a court of competent jurisdiction, a State grand jury subpoena, or a subpoena authorized under § 15-108 of the Criminal Procedure Article (subpoena issued by a State's Attorney);
- obtains a warrant from a court of competent jurisdiction;
- obtains a court order requiring the disclosure; or
- has the consent of the subscriber or customer to the disclosure.

An investigative or law enforcement officer who receives records or information is not required to provide notice to a subscriber or customer.

A court of competent jurisdiction may issue an order requiring disclosure only if the investigative or law enforcement officer shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry.

A court issuing an order may quash or modify the order, on a motion made promptly by the service provider, if the information or records requested are unusually voluminous in nature or if compliance with the order otherwise would cause an undue burden on the provider.

Court Order for Pen Register or Trap and Trace Device: In addition to the statute discussed above, law enforcement is using the pen register/trap and trace statute to obtain cell phone-related information.

With the exception of certain functions of a wire or electronic communication service provider, a person is prohibited from installing or using a pen register or a trap and trace device without first obtaining a court order. Violators are subject to maximum penalties of imprisonment for one year and/or a $5,000 fine. A "pen register" is a device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted. It does not include a device used by a provider or customer of a wire or electronic communication service for specified billing-related functions. A "trap and trace device" means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication. Neither a pen register nor a trap and trace device include a device or process used to obtain the content of a communication.

An investigative or law enforcement officer may make application for a court order authorizing or approving the installation and use of a pen register or a trap and trace device to a court of competent jurisdiction of this State. The application must include (1) the identities of the officer applying for the order and the law enforcement agency conducting the investigation and (2) a statement under oath by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

If the court finds that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation, the court must enter an *ex parte* order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court. The order must contain specific information and may only authorize the installation and use of a pen register or a trap and trace device for up to 60 days. An extension for no more than 60 days may be granted upon the filing of a new application and a new finding by the court.

Specified service providers and individuals relevant to the installation and use of the pen register or trap and trace device are required to provide, upon request of an authorized law enforcement officer, assistance in the installation of the devices and additional information and assistance relevant to the unobtrusively installing and using the devices and minimizing interference.

Unless otherwise ordered by the court, the results of the trap and trace device must be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

The requirements under the pen register and trap and trace device statute do not create a cause of action against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a pen register/trap and trace device court order. A good faith reliance on a court order, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under the pen register/trap and trace device statute.

Law enforcement and State's Attorneys in Maryland are currently applying for court orders under the statutes discussed above to obtain electronic location information and cell phone service providers are requiring these court orders before providing customer/subscriber information.

Background: In *United States v. Jones*, 132 S. Ct. 945 (2012), the U.S. Supreme Court ruled unanimously that law enforcement must obtain a search warrant before using global positioning system (GPS) technology to track criminal suspects. Police officers in the case obtained a warrant with a 10-day time limit to install a GPS device in the District of

Columbia on a car belonging to the wife of a local nightclub owner. However, police installed the device on the eleventh day and in Maryland. Officers tracked the nightclub owner's movements for 28 days and used the location information transmitted by the device to secure an indictment of Mr. Jones and others on drug trafficking charges. Mr. Jones was convicted and sentenced to life in prison. A federal court overturned his conviction after concluding that the evidence gathered from the warrantless installation of the GPS device violated protections against unreasonable searches and seizures under the Fourth Amendment to the U.S. Constitution. In January 2012, the Supreme Court affirmed the lower court's ruling and determined that officers encroached on a protected area when they physically attached the GPS to the vehicle and, by installing the device without a valid warrant, committed a trespass and illegal search.

In *United States v. Knotts*, 460 U.S. 276 (1983), the U.S. Supreme Court held that government agents did not violate the Fourth Amendment when they placed a beeper in a container of chloroform without obtaining a warrant to keep visual track of the vehicle transporting the chloroform. The court opined that the driver of the van did not have a legitimate expectation of privacy with respect to the visual movements of the van on public streets and highways, since anyone on the street would have been able to see the van.

While the Supreme Court cases have addressed the use of GPS devices and beepers, the use of cell phone location data by law enforcement is becoming an increasingly common practice. Cell phone signals bounce ("ping") off of cell phone towers in various locations, regardless of whether the phone is in use. Cell phone providers retain an extensive amount of historical location data as well as real-time data. As the number of cell phone towers grows, the precision of this location data also grows. Under the Electronic Communications Privacy Act of 1986 (ECPA), law enforcement can obtain cell phone records without a search warrant. While a search warrant requires a showing that there is probable cause linking a suspect to a particular crime, the requirement under ECPA only requires law enforcement to show that there are reasonable grounds to believe that the material sought is relevant to a crime. Also, while search warrants are usually delivered to the person whose property is being searched, the court orders obtained under ECPA are usually sealed from public view. A person whose cell phone data is obtained through one of these orders usually does not find out about it until he/she is charged with a crime and the evidence obtained is presented.

According to news reports, cell phone carriers responded to at least 1.3 million requests for subscriber information from law enforcement during 2011. Cell phone carriers have taken to charging fees for these services, since federal law allows for carriers to be reimbursed for reasonable expenses incurred in responding to law enforcement requests for information. AT&T reportedly collected $8.3 million in law enforcement reimbursements in 2011, compared with $2.8 million in 2007.

Given the growth in the number of cell phone tracking requests, the increase in the amount of data being requested, and the increased precision of cell phone location data, judges and courts are starting to take a second look at whether a warrant is required before law enforcement can obtain cell phone location data. In 2010, the U.S. Court of Appeals for the Third Circuit ruled that judges have statutory authority to require law enforcement to show probable cause in order to obtain cell phone location data. The court rejected an argument by the U.S. Department of Justice that a court must issue orders granting the government access to the data only on a showing that the location data is material and relevant to an ongoing investigation. However, the court also noted that courts should "sparingly" exercise their authority to demand probable cause warrants in these cases.

In November 2011, a federal District Court judge affirmed a magistrate judge's denial and declared that the ECPA's authorization of government procurement of cell phone records without a search warrant is unconstitutional. Several federal magistrate judges have denied government requests for records.

In August 2012, the U.S. Court of Appeals for the Sixth Circuit ruled that the Drug Enforcement Administration did not violate a drug trafficker's Fourth Amendment rights when it obtained a court order and not a search warrant to obtain real-time location data and "ping" information from the trafficker's pay-as-you-go cell phone. The court determined that the trafficker did not have a reasonable expectation of privacy in the data emitted by the cell phone he purchased voluntarily. The court stated that officers lawfully tracked the location information freely transmitted by the cell phone and that "[t]he law cannot be that a criminal is entitled to rely on the unexpected trackability of his tools." *U.S. v. Skinner*, 690 F.3d 772 (6th Cir. 2012). The court also noted that the trafficker traveled with his cell phone on public roads and stopped at a public rest stop – information that could have also been gathered through visual surveillance.

Legislation was introduced in Congress that would have required a warrant before the government can obtain cell phone data and would have required customer consent before cell phone providers can collect customer location data. The bills were referred to committees, but no further action was taken. The legislation was reintroduced on July 31, 2012, as a proposed amendment to the Cybersecurity Act of 2012, which later failed.

While cell phone records are usually obtained from a cell phone provider, technology is making it possible for law enforcement to bypass these companies altogether. Certain devices allow law enforcement to obtain location data by imitating a cell phone tower, getting a phone to connect with it, and measuring signals from the phone to pinpoint its location. The device, which is being used by the Federal Bureau of Investigation, the military, and local law enforcement, is known by several trade names, including StingRay, KingFish, and LoggerHead.

According to news reports, Montgomery County spent more than $180,000 in 2012 to upgrade and enhance its StingRay/KingFish system.

State Expenditures: General fund expenditures increase minimally for AOC to accommodate the bill's requirements.

AOC advises that the bill is likely to result in a significant increase in applications for court orders and requests for extensions submitted by law enforcement personnel to judges and additional judicial time necessary for the review and issuance of location information orders. However, the operational and fiscal impact of this effect is difficult to project because of uncertainty with respect to the number of additional filings the courts will receive. An order issued under the bill has a shorter duration than other available options and may require law enforcement to file for extensions more frequently.

The bill does not specify who is required to provide notice of the order to the owner or user of a relevant electronic device. According to AOC, if the court is required to provide such notice, then the bill requires system changes, the cost of which depends on the number of notifications required under the bill.

The Department of State Police advises that it can implement the bill with existing budgeted resources.

Local Expenditures: Expenditures increase minimally for local law enforcement units and circuit courts to comply with the bill's notice requirements. The extent of the fiscal impact depends on the volume of requests for applicable orders filed in the jurisdiction.

Baltimore City advises that it needs to employ two administrative employees at an estimated cost of $100,000 each year to accommodate the bill's notification requirements. The Baltimore City Police Department's (BCPD) Criminal Investigative Division submits 25 to 35 requests to the Circuit Court for Baltimore City for court orders each week for electronic geographical information data. Other units in BCPD submit approximately 20 requests per week. These figures do not include requests for stored information made through subpoenas. The information is used in the investigation of various crimes, including kidnapping, robbery, carjacking, other violent crimes, and narcotics offenses.

Baltimore County advises that the bill has an operational impact on the Baltimore County Police Department's ability to conduct investigations in a timely manner.

Frederick County and the cities of Frederick and Havre de Grace do not anticipate a fiscal impact from the bill. Charles County advises that as long as the bill does not apply to county-owned vehicles equipped with GPS, the bill does not have a fiscal impact.

Additional Information

Prior Introductions: HB 887 of 2013, a similar bill, received a hearing in the House Judiciary Committee, but no further action was taken.

Cross File: HB 1161 (Delegate Waldstreicher, *et al.*) - Judiciary.

Information Source(s): Baltimore City; Baltimore, Charles, Frederick, and Montgomery counties; cities of Frederick and Havre de Grace; Department of Natural Resources; Comptroller's Office; Judiciary (Administrative Office of the Courts); Department of State Police; Office of the Public Defender; Department of Public Safety and Correctional Services; Governor's Office of Crime Control and Prevention; State's Attorneys' Association, Maryland Department of Transportation; WUSA9.com; Department of Legislative Services

Fiscal Note History: First Reader - March 4, 2014
mc/kdm Revised - Senate Third Reader - April 1, 2014
Revised - Enrolled Bill/Clarification - May 15, 2014

Analysis by: Amy A. Devadas

Direct Inquiries to:
(410) 946-5510
(301) 970-5510