HB 887

Department of Legislative Services

Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE

House Bill 887 (Delegates Waldstreicher and Rosenberg)
Judiciary

Criminal Procedure - Search Warrants - Location Privacy

This bill prohibits an agent of the State or a political subdivision of the State from obtaining "location information" without a search warrant. "Location information" means information concerning the 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 location information search warrants; (2) requires disclosure of specified information to a customer/subscriber; and (3) requires courts and the Administrative Office of the Courts (AOC) to submit specified information on an annual basis.

Except as proof of a violation of the bill's provisions, evidence obtained in violation of the bill's provisions is not admissible in a proceeding. Location information obtained in accordance with the bill's provisions and evidence derived from that location information may not be received in evidence or otherwise disclosed in a trial, a hearing, or any other proceeding in a federal or State court unless each party has been furnished with a copy of the relevant location information search warrant and the accompanying warrant application at least 10 days before the trial, hearing, or proceeding.

Fiscal Summary

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

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

Small Business Effect: None.

Analysis

Bill Summary:

Delayed Notification: An agent of the State or a political subdivision of the State ("an agent") may, as part of the application for the search warrant, request an order delaying notification to the customer/subscriber for a period of up to 90 days. An agent may also request an order directing a service provider to which the search warrant is directed not to notify any other person of the existence of the search warrant for a period of up to 90 days. The court must issue the order(s) if the court determines that there is reason to believe that the notification of the existence of the search warrant may have an adverse result. The court may grant one or more extensions for an additional 90-day period of a delayed notification order, on application of the agent of the State or political subdivision.

Disclosure of Search Warrant to Customer/Subscriber: An agent must serve on or deliver a copy of the search warrant and a notice containing specified information to the customer or subscriber within three days after receiving location information pursuant to a search warrant. Among other things, the notice must include information (1) on the nature of the law enforcement inquiry with reasonable specificity; (2) that the customer/subscriber's location information was supplied to or requested by the agent and the date on which the information was supplied or requested; and (3) on whether the court ordered delay of notification to the customer/subscriber.

Exceptions to Search Warrant Requirement: An agent may obtain location information without a search warrant (1) to respond to the user's call for emergency services; (2) with the express consent of the owner or user of the relevant electronic communications device; and (3) if the agent believes that an emergency involving immediate danger or death or serious physical injury to a person requires immediately obtaining information relating to the emergency and the request is narrowly tailored to address the emergency. The request must document the factual basis for believing that the emergency situation requires immediately obtaining the information relating to the emergency. Within 48 hours after the date on which the agent obtains access to these records, a governmental entity must file with the appropriate court a signed, sworn statement of a supervisory official setting forth the grounds for the emergency access.

Reporting Requirements: By January 31 of each year, a court issuing or denying a search warrant for location information during the preceding calendar year must report specified information on each warrant to AOC, including (1) the identity of the agency that applied for the search warrant; (2) the offense specified in the warrant application; (3) the expected number of devices about which location information was obtained; (4) whether the search warrant was granted as applied for, was modified, or was denied; (5) the

period of disclosures authorized; and (6) the number and duration of extensions of the search warrant.

Beginning in June 2014, AOC must submit an annual report to the General Assembly containing specified information, including full and complete information on the number of applications submitted for location information search warrants, the number of times access to location information was obtained, and the number of location information search warrants granted or denied during the preceding calendar year. Beginning in June 2014 and each year thereafter, a nonclassified summary of the AOC's annual report must be made available to the public on AOC's website.

Current Law:

Search Warrants: A circuit court or District Court judge may issue a search warrant whenever it is made to appear to the judge that there is probable cause to believe that (1) a misdemeanor or felony is being committed by a person or in a building, apartment, premises, place, or thing within the jurisdiction of the judge or (2) property subject to seizure is on the person or in or on the building, apartment, premises, place, or thing.

An application for a search warrant must be (1) in writing; (2) signed and sworn to by the applicant; and (3) accompanied by an affidavit that sets forth the basis for probable cause and contains facts within the personal knowledge of the affiant that there is probable cause.

Court Order for Pen Register or Trap and Trace Device: 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 pen register/trap and trace device statute 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*, 565 U.S. __ (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.

State Expenditures: General fund expenditures increase minimally for AOC to comply with the bill's reporting requirements. As previously noted, the bill requires AOC to compile an annual report on location information search warrants. It is unclear how the data for District Court warrants will be compiled and how AOC will compile information provided by the circuit courts. To the extent that AOC develops a computer program to track District Court warrants, computer reprogramming costs are incurred. To the extent

that the District Court and AOC use a manual process, administrative expenses are incurred.

Local Expenditures: Given the scope of information that must be provided on each location information search warrant and the number of search warrants that need to be included in the report, circuit courts incur additional administrative or personnel expenses to comply with the bill's reporting requirements.

Baltimore City advises that the bill's notification provision substantially increases administrative costs. The Montgomery County Police Department, Washington County, and Worcester County do not foresee a fiscal impact from the bill. Kent County advises that the bill's standard three-day notification requirement could be problematic for law enforcement absent an extension for delayed notification.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Baltimore City; Kent, Montgomery, Washington, and Worcester counties; Department of Natural Resources; Department of General Services; Judiciary (Administrative Office of the Courts); Maryland Department of Transportation; *New York Times; American Bar Association Journal; Bloomberg Businessweek; Harvard Journal of Law and Technology;* Center for Democracy and Technology; CNET; NBC News; Letter Dated May 23, 2012 from Sprint Nextel to U.S. Representative Edward J. Markey (Co-Chairman of the Congressional Bi-Partisan Privacy Caucus); GPS.gov; Department of Legislative Services

Fiscal Note History: First Reader - February 22, 2013
mc/kdm

Analysis by: Amy A. Devadas

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