Department of Legislative Services

Maryland General Assembly
2013 Session

FISCAL AND POLICY NOTE

House Bill 377 (Delegates Cluster and McDermott)
Judiciary

Criminal Procedure - Court Order - Location of Mobile Communications Device

This bill prohibits a person from receiving real-time location information transmitted by a "mobile communications device" from a common communications carrier without first obtaining a court order. This requirement does not apply to the receipt of real-time location information transmitted for a single period of up to 48 hours in exigent circumstances or with the consent of the contract holder or lawful possessor of the mobile communications device. Violators are subject to imprisonment for up to one year and/or a fine of up to $5,000. A "mobile communications device" is a device capable of transmitting electronic communications to a communications common carrier.

The bill also authorizes an investigative or law enforcement officer to apply to a court of competent jurisdiction in the State for a court order or an extension of a court order to receive real-time location information transmitted by a mobile communications device from a common communications carrier. The bill also contains provisions governing the required content in an application for a court order, the issuance of a court order, the duration of a court order, and the confidentiality of a court order.

Fiscal Summary

State Effect: The bill's requirements can be met with existing State resources.

Local Effect: The bill's requirements can be met with existing local resources.

Small Business Effect: None.

Analysis

Bill Summary: The application must (1) be in writing; (2) be signed and sworn to by the applicant; (3) include the identity of the investigation or law enforcement officer making the application and the law enforcement agency conducting the investigation; and (4) include a statement accompanied by an affidavit setting forth the basis for probable cause.

If, after receipt of the application, the court finds that there is probable cause to believe that the real-time location information is relevant to an ongoing criminal investigation, the court must enter an *ex parte* order authorizing the receipt of real-time location information transmitted by a mobile communications device from a communications common carrier within the court's jurisdiction. The order must (1) specify the identity, if known, of the person to whom the mobile communications device is leased or listed; (2) specify the identity, if known, of the person who is the subject of the criminal investigation; (3) contain a description of the offense being investigated; and (4) direct, on the request of the applicant, the furnishing of information and technical assistance from the communications common carrier for the purpose of providing the real-time location information sought in the application.

A court order may last for up to 60 days. However, the court may order an extension of up to 60 days. The court may order a longer extension period for good cause shown. The bill's authorization for a court to order a longer extension period also applies to court orders for the installation and use of a pen register or a trap and trace device.

The order must direct that the order remain sealed until further order of the court. The order must also direct the person owning or leasing the line that is the subject of the order, or who is obligated by the order to provide assistance to the applicant, not to disclose the receipt of the real-time location information or the existence of the investigation to the subscriber or any other person unless otherwise ordered by the court.

Current Law: 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.

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.

Additional Information

Prior Introductions: HB 460 of 2012 received a hearing in the House Judiciary Committee. The bill was then withdrawn.

Cross File: None.

Information Source(s): Montgomery County, Department of Natural Resources, Department of General Services, Comptroller's Office, Judiciary (Administrative Office of the Courts), Department of Public Safety and Correctional Services, 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 1, 2013
mc/kdm

Analysis by: Amy A. Devadas

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