Cellphone Tracking Powers on Request
Secret Warrants Granted Without Probable Cause

By Ellen Nakashima
Washington Post Staff Writer
Friday, November 23, 2007; A01

Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers.

In some cases, judges have granted the requests without requiring the government to demonstrate that there is probable cause to believe that a crime is taking place or that the inquiry will yield evidence of a crime. Privacy advocates fear such a practice may expose average Americans to a new level of government scrutiny of their daily lives.

Such requests run counter to the Justice Department's internal recommendation that federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas. The requests and orders are sealed at the government's request, so it is difficult to know how often the orders are issued or denied.

The issue is taking on greater relevance as wireless carriers are racing to offer sleek services that allow cellphone users to know with the touch of a button where their friends or families are. The companies are hoping to recoup investments they have made to meet a federal mandate to provide enhanced 911 (E911) location tracking. Sprint Nextel, for instance, boasts that its "loopt" service even sends an alert when a friend is near, "putting an end to missed connections in the mall, at the movies or around town."

With Verizon's Chaperone service, parents can set up a "geofence" around, say, a few city blocks and receive an automatic text message if their child, holding the cellphone, travels outside that area.

"Most people don't realize it, but they're carrying a tracking device in their pocket," said Kevin Bankston of the privacy advocacy group Electronic Frontier Foundation. "Cellphones can reveal very precise information about your location, and yet legal protections are very much up in the air."

In a stinging opinion this month, a federal judge in Texas denied a request by a Drug Enforcement Administration agent for data that would identify a drug trafficker's phone location by using the carrier's E911 tracking capability. E911 tracking systems read signals sent to satellites from a phone's Global Positioning System (GPS) chip or triangulated radio signals sent from phones to cell towers. Magistrate Judge Brian L. Owsley, of the Corpus Christi division of the Southern District of Texas, said the agent's affidavit failed to focus on "specifics necessary to establish probable cause, such as relevant dates, names and places."

Owsley decided to publish his opinion, which explained that the agent failed to provide "sufficient specific
information to support the assertion" that the phone was being used in "criminal" activity. Instead, Owsley wrote, the agent simply alleged that the subject trafficked in narcotics and used the phone to do so. The agent stated that the DEA had "identified' or 'determined' certain matters," Owsley wrote, but "these identifications, determinations or revelations are not facts, but simply conclusions by the agency."

Instead of seeking warrants based on probable cause, some federal prosecutors are applying for orders based on a standard lower than probable cause derived from two statutes: the Stored Communications Act and the Pen Register Statute, according to judges and industry lawyers. The orders are typically issued by magistrate judges in U.S. district courts, who often handle applications for search warrants.

In one case last month in a southwestern state, an FBI agent obtained precise location data with a court order based on the lower standard, citing "specific and articulable facts" showing reasonable grounds to believe the data are "relevant to an ongoing criminal investigation," said Al Gidari, a partner at Perkins Coie in Seattle, who reviews data requests for carriers.

Another magistrate judge, who has denied about a dozen such requests in the past six months, said some agents attach affidavits to their applications that merely assert that the evidence offered is "consistent with the probable cause standard" of Rule 41 of the Federal Rules of Criminal Procedure. The judge spoke on condition of anonymity because of the sensitivity of the issue.

"Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target," wrote Christopher Guttman-McCabe, vice president of regulatory affairs for CTIA -- the Wireless Association, in a July comment to the Federal Communications Commission. He said the "lack of a consistent legal standard for tracking a user's location has made it difficult for carriers to comply" with law enforcement agencies' demands.

Gidari, who also represents CTIA, said he has never seen such a request that was based on probable cause.

Justice Department spokesman Dean Boyd said field attorneys should follow the department's policy. "We strongly recommend that prosecutors in the field obtain a warrant based on probable cause" to get location data "in a private area not accessible to the public," he said. "When we become aware of situations where this has not occurred, we contact the field office and discuss the matter."

The phone data can home in on a target to within about 30 feet, experts said.

Federal agents used exact real-time data in October 2006 to track a serial killer in Florida who was linked to at least six murders in four states, including that of a University of Virginia graduate student, whose body was found along the Blue Ridge Parkway. The killer died in a police shooting in Florida as he was attempting to flee.

"Law enforcement has absolutely no interest in tracking the locations of law-abiding citizens. None whatsoever," Boyd said. "What we're doing is going through the courts to lawfully obtain data that will help us locate criminal targets, sometimes in cases where lives are literally hanging in the balance, such as a child abduction or serial murderer on the loose."

In many cases, orders are being issued for cell-tower site data, which are less precise than the data derived from E911 signals. While the E911 technology could possibly tell officers what building a suspect was in,
cell-tower site data give an area that could range from about three to 300 square miles.

Since 2005, federal magistrate judges in at least 17 cases have denied federal requests for the less-precise cellphone tracking data absent a demonstration of probable cause that a crime is being committed. Some went out of their way to issue published opinions in these otherwise sealed cases.

"Permitting surreptitious conversion of a cellphone into a tracking device without probable cause raises serious Fourth Amendment concerns especially when the phone is in a house or other place where privacy is reasonably expected," said Judge Stephen William Smith of the Southern District of Texas, whose 2005 opinion on the matter was among the first published.

But judges in a majority of districts have ruled otherwise on this issue, Boyd said. Shortly after Smith issued his decision, a magistrate judge in the same district approved a federal request for cell-tower data without requiring probable cause. And in December 2005, Magistrate Judge Gabriel W. Gorenstein of the Southern District of New York, approving a request for cell-site data, wrote that because the government did not install the "tracking device" and the user chose to carry the phone and permit transmission of its information to a carrier, no warrant was needed.

These judges are issuing orders based on the lower standard, requiring a showing of "specific and articulable facts" showing reasonable grounds to believe the data will be "relevant and material" to a criminal investigation.

Boyd said the government believes this standard is sufficient for cell-site data. "This type of location information, which even in the best case only narrows a suspect's location to an area of several city blocks, is routinely generated, used and retained by wireless carriers in the normal course of business," he said.

The trend's secrecy is troubling, privacy advocates said. No government body tracks the number of cellphone location orders sought or obtained. Congressional oversight in this area is lacking, they said. And precise location data will be easier to get if the Federal Communication Commission adopts a Justice Department proposal to make the most detailed GPS data available automatically.

Often, Gidari said, federal agents tell a carrier they need real-time tracking data in an emergency but fail to follow up with the required court approval. Justice Department officials said to the best of their knowledge, agents are obtaining court approval unless the carriers provide the data voluntarily.

To guard against abuse, Congress should require comprehensive reporting to the court and to Congress about how and how often the emergency authority is used, said John Morris, senior counsel for the Center for Democracy and Technology.

Staff researcher Richard Drezen contributed to this report.