Answering the Call: The Latest News on Tracking Individuals via Their Cellular Phones

By Alison Healey

There are 233 million cell phone owners in the United States, no fewer than 69% of the country's population.[1] Apple sold 270,000 iPhones during the product's first two days on the market.[2] Society is increasingly dependent upon cell phones, making it easier for law enforcement to locate and follow suspects and uncover criminal activity. In order to use this technology effectively, officers need to know the case law regarding when, where, and how cell phone users legally can be tracked.

Cellular Phone Technology

When turned on, a cell phone registers its location with the nearest cellular tower approximately every seven seconds. When an individual moves, the signal moves too, continually switching to the closest tower. Accordingly, one can get a very general sense of a person's location by learning with which tower a phone is registering. The greater the number of cell towers in the area, the greater the accuracy. For example, in urban areas, there usually are many towers, so one can gather more specific location information than in rural areas, where towers may be miles apart. One can obtain more precise detail by using triangulation, which measures the time delay or angle of arrival of the signal from a cell phone to the three nearest cellular towers. Global positioning satellite (GPS) chips in newer cell phones allow for even greater accuracy. Satellites broadcast signals from space that are picked up by GPS receivers, including GPS chips in cell phones. Each receiver then provides three-dimensional location information (latitude, longitude, and altitude) plus the time.[3] Although GPS is not as useful when the direct line to a satellite is broken, the system is being enhanced.[4] Approximately 90% of cell phones currently have built-in GPS capabilities, with the potential to be pinpointed within 50 feet.[5] Due to the prevalence of cell phones in the United States and the rapid advances in technology, courts are increasingly making decisions regarding the tracking of individuals by law enforcement. People often carry their phones with them at all times, and, inevitably, statutory and constitutional issues are emerging.

Obtaining the Location of Individual Cell Phone Users

So, what ***are*** the legal requirements for tracking an individual via his or her cell phone? The short answer is: it depends. It depends on the location of the court—and possibly the location of the targeted individual—as well as the type of information sought. Generally speaking, probable cause is required.

Neither the United States Supreme Court nor Congress has explicitly addressed the issue of tracking individuals via their cell phones. However, since 2005, at least fifteen federal district courts have ruled on government applications for acquiring "real-time" or "prospective" cell site location information. "Real-time" cell site information allows officers to locate a phone while it is on and a call is in progress. It is a subset of "prospective" cell site information, which refers to all cell site information generated after officers have received court permission to acquire it.[6] Thus far, federal court decisions have pertained to cellular tower and triangulation data; tracking

individuals using cell phone GPS has only been referenced in dicta. The majority of courts have held that probable cause is necessary to obtain real-time information about a cell phone user's current location.[7] A few have authorized the Government, on a showing of relevance and materiality, to access real-time single cellular tower data and/or information transmitted at the beginning and end of calls.[8] Under the minority view, a combination of three statutes—the Pen Register and Trap and Trace Device Statute,[9] the Stored Communications Act,[10] and the Communications Assistance for Law Enforcement Act[11]—lowers the threshold required to obtain certain cell phone location data. To date, no published federal decision has allowed the Government, absent probable cause, to employ a cell phone as an exact tracking device. In other words, officers have not been permitted to gather detailed location information while a phone is on but not in use.

Is a Cell Phone a "Tracking Device?"

A mobile tracking device is defined by statute as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[12] The statute also discusses governmental "installation" of such devices.[13] An individual can be located by cell phone using GPS or triangulation without the installation of any equipment. Thus, "a cell phone is not a tracking device as that term is commonly understood."[14] Some courts presume that they are equivalent,[15] meaning that, as with other tracking devices, if a cell phone remains in a public place where visual surveillance is available, the Fourth Amendment is not implicated and no warrant is needed. Yet cell phones remain distinct in certain ways. Unlike other devices, the Government initially needs some sort of court order to compel a wireless service provider to furnish the cell site information.[16] Moreover, many people have cell phones with them virtually twenty four hours a day, seven days a week. The portability of phones enables them to travel into both public and private places, raising the possibility that their location can reveal intimate details of people's lives.[17] When the phone is used to reveal detailed location information, such as triangulation and GPS data, the Fourth Amendment must be considered. Accordingly, the majority of courts have ruled that a Rule 41 search warrant based on probable cause is the appropriate mechanism to obtain such information.[18]

The Minority View: the Relevance and Materiality Standard

Most courts have labeled a cell phone as a tracking device and required the Government to demonstrate probable cause in order to track a cell phone user in real time. However, a few judges, upon a showing of relevance and materiality, have allowed law enforcement officers to acquire single cellular tower data as well as information transmitted at the beginning and ending of a person's calls. This theory relies upon three statutes to form a hybrid authority that lowers the necessary threshold. The basic premise is that cell phones are akin to pen registers, and cell location data qualifies as "signaling information" under the Pen Register and Trap and Trace Device Statute ("Pen/Trap Statute").[19] Pen/Trap information can be obtained upon a showing of relevance. However, another statute, the Communications Assistance for Law Enforcement Act ("CALEA"), prohibits the Government from gathering information that may disclose the physical location of a subscriber if the information would be acquired solely pursuant to the Pen/Trap Statute. A third statute, the Stored Communications Act (SCA), is used to eliminate the "solely" problem. Courts have held that cell phone location data constitutes "other information" under the SCA, which, like Pen/Trap information, can be obtained upon a showing

of relevance and materiality.[20] Judges endorsing this approach do not disregard the importance of the Fourth Amendment; rather, they simply seem to feel that if any invasions of privacy occur, they can be dealt with through motions to suppress later on.[21]

Support for the Hybrid Theory is Weak

Approximately half a dozen courts have accepted the hybrid authority, though it is doubtful that the three laws were intended to be applied in this manner. The statutes were passed fifteen years apart, and none of them explicitly references the others. In 1994, when CALEA was debated, then-FBI Director Freeh testified that the Act would not be used to learn about the physical location of a mobile phone. Furthermore, Congress appears to have recognized a privacy interest in cellular phone location information. In 1999, lawmakers enacted a bill permitting the disclosure of location information of cell phone users only in an emergency situation or upon consent by the customer.[22] Congress also contemplated amending the SCA to state that physical location information generated by a wireless service provider may only be released to the Government pursuant to a court order based upon probable cause; so far, no such law has been passed.

Conclusion

The legal requirements for real-time or prospective tracking of individuals by cell phone remain uncertain. There are no United States Supreme Court decisions or statutes directly on point. Lower court decisions are conflicting and do not specifically address the precision tracking of cell phone users with GPS. Questions remain as to whether a cell phone user has an expectation of privacy in his or her location, particularly because a person chooses whether or not to carry a cell phone and whether or not to turn the phone on. Cell phone subscribers also are aware that a third party—namely, a telecommunications provider—will be collecting information about their use and location. Arguably, this all may result in a diminished subjective expectation of privacy. Additionally, most members of society are eager to acquire the latest electronic devices and use technology such as GPS, which makes the objective expectation of privacy analysis more complicated. The answers to many of these issues are not yet known. However, one thing is certain: with the sales of the iPhone projected to possibly reach 10 million by the end of 2008,[23] the tremendous popularity of GPS, and the fact that cell phones have become a critical accessory, law enforcement officers will confront matters involving cell phone tracking with increasing frequency. Due to potential Fourth Amendment implications, it is advisable for the Government to proceed based on probable cause and equipped with a Rule 41 warrant, unless officers are certain that a cell phone will not be monitored in any place where a person has a reasonable expectation of privacy.

Alison Healey is interning in the FLETC's Legal and Computer & Financial Investigations Divisions during summer 2007. She is entering her final year at Harvard Law School and will graduate in June 2008. She earned a B.S. in Justice and Law Administration from Western Connecticut State University, graduating at the top of her business school class.

---

[1] According to the Cellular Telecommunications & Internet Association (CTIA), www.ctia.org.
[2] Jefferson Graham, *Apple Says IPhone Sales Hit 270,000 in First Two Days*, USA TODAY, July 26, 2007, at 1B.
[3] See http://www.gps.gov/.

[4] The signal between a phone and a satellite may be interrupted in urban areas or when the phone is indoors. The U.S. Government is modernizing GPS, working on adding second and third civilian GPS signals as well as Assisted GPS (A-GPS) technology to provide increased accuracy and reliability.

[5] Interestingly, iPhones do not have GPS chips.

[6] *See* In re the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register, 402 F. Supp. 2d. 597, 599 (D. Md. 2005). Records stored by a wireless service provider that detail the location of a cell phone in the past (i.e., prior to the entry of a court order authorizing government acquisition) are known as "historical" cell site information. Historical data is outside the scope of this article; it can be obtained using a subpoena or warrant, upon a demonstration of "reasonable grounds to believer" that the information is "relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. § 2703(d).

[7] Jurisdictions presently adhering to the probable cause standard include: the Southern District of Texas, the District of Maryland, the Western District of Louisiana, the Eastern and Western Districts of New York, the District of Columbia, and the Eastern District of Wisconsin. There is also an unreported decision from the Northern District of Indiana.

[8] Jurisdictions in which the minority view governs include: the Southern District of New York and the Southern District of West Virginia. A magistrate judge in the Eastern District of California has held that it is not necessary to obtain a warrant based on probable cause for cell site information, at least where the cell phone user being tracked is outside of a place where he or she has an expectation of privacy.

[9] 18 U.S.C. § 3121-3127. This statute is also known as Title III of the Electronic Communications Privacy Act of 1986 (ECPA).

[10] Specifically, 18. U.S.C. §2703. This statute is also known as the Title II of the ECPA.

[11] 47 U.S.C. § 1002.

[12] 18 U.S.C. § 3117(b).

[13] 18 U.S.C. § 3117(a).

[14] In re the Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing the Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678 (W.D.La. 2006); *see also* In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 (E.D.Cal. 2007) ("[T]he device contemplated [when the tracking device statute was passed in 1986] was only of the 'beeper' variety . . . No use of cell phones and cell towers for tracking was expressly contemplated, and perhaps was not even possible in 1986.").

[15] *See* In re Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005) ("While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data.").

[16] *See* In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register, 402 F. Supp. 2d 597 (D. Md. 2005); Cell Site Location Auth., 396 F. Supp. 2d 747.

[17] *See* In re Application of the United States of America, 402 F. Supp. 2d at n.10 ("[t]he Government cannot guarantee that [a] cell phone and its possessor will remain in a public place," which the court warns may result in an invasion of privacy).

[18] *See id*. at 605 ("When the Government seeks to acquire and use real time cell site information to identify the location and movement of a phone and its possessor in real time, the court will issue a warrant upon a sworn affidavit demonstrating probable cause to believe the information will yield evidence of a crime. The court will not enter an order authorizing disclosure of real time cell site information under authority other than Rule 41, nor upon a showing of less than probable cause."); *See also* Cell Site Location Auth., 396 F. Supp. 2d at 757 ("As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant.").

[19] 18 U.S.C. § 3121.

[20] 18 U.S.C. §§ 2703(c)(1) and 2703(d).

[21] *See* In re United States for Order for Prospective Cell Site Location Information, 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006).

[22] The Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)).

[23] Jefferson Graham, *Apple Says IPhone Sales Hit 270,000 in First Two Days*, USA TODAY, July 26, 2007, at 1B.