AMERICAN CIVIL LIBERTIES UNION of MARYLAND

3600 Clipper Mill Road, Suite 350 Baltimore MD 21211
410-889-8555 • Fax 410-366-7838 • Email - ACLU@ACLU-MD.ORG

Testimony for the House Judiciary Committee
February 5, 2013

HB 377– Criminal Procedure – Court Order – Location of Mobile Communications Device

OPPOSE

The American Civil Liberties Union of Maryland opposes HB 377. This bill would create a low standard that law enforcement would have to meet before obtaining cell phone location information. Because cell phone location tracking information reveals personal and often private information, law enforcement should obtain a warrant based upon probable cause before accessing this information.

Background

There are now over 300 million cell phone subscribers in the United States.[1] Eighty-eight percent of all adults have cell phones.[2] Cell phones follow us everywhere we go and allow us to be followed everywhere we go.

In order to provide service to cell phones, cell phone companies are constantly "pinging" the cell phone to determine its location[3]. Pinging occurs whenever a cell phone is on;

[1] http://www.infoplease.com/ipa/A0933563.html (as of 2010)
[2] http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012/Key-Findings.aspx
[3] Cellular telephone networks are divided into geographic coverage areas known as "cells," which range in diameter from many miles in suburban or rural areas to several hundred feet in urban areas. Each contains an antenna tower, one function of which is to receive signals from and transmit signals to cellular telephones.

Whenever a cellular telephone is on, regardless of whether it is making or receiving a voice or data call, it periodically transmits a unique identification number to register its presence and location in the network. That signal, as well as calls made from the cellular phone, are received by every antenna tower within range of the phone. When the signal is received by more than one tower, the network's switching capability temporarily "assigns" the phone to the tower that is receiving the strongest signal from it. As a cellular telephone moves about, the antenna tower receiving the strongest signal may change as, for example, often occurs when a cellular phone moves closer to a different antenna tower. At that point, the cellular telephone, including any call in progress, is assigned to the new antenna tower.

The location of the antenna tower receiving a signal from a given cellular telephone at any given moment inherently fixes the general location of the phone. Indeed, in some instances, depending upon the characteristics of the particular network and its equipment and software, it is possible to determine not only the tower receiving a signal from a particular phone at any given moment, but also in which of the

whether a customer knows it or not, whether the customer is using the phone or not. This data can be accessed in real-time and is also stored.

Law enforcement across the country seek this information at an enormous rate. In 2009 alone, cell phone companies shared 8 million pings with law enforcement.[4] In 2011, cell phone carriers responded to at least 1.3 million requests for subscriber information from law enforcement.[5]

The implications for privacy and opportunities for abuse are significant. Cell phone location information gives a very detailed picture of a person's behavior—whether you are in the hospital, in a bedroom, what stores or coffee shops you are visiting. As DC Circuit Judge Ginsburg wrote, one's location might reveal

> "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts."[6]

Legal Standards

The legal standard for when law enforcement may obtain cell phone tracking information is not settled. A recent Supreme Court case, *United States v. Jones*, 132 S.Ct. 945 (2012), indicates the Court, when presented with the question, likely would require a warrant to obtain cell phone location tracking. In *Jones*, the Court held that the government conducts a search under the Fourth Amendment, and thus must obtain a warrant first, when it attaches a GPS device to a car and tracks its movements. Though the case was decided on relatively narrow grounds, a majority of justices, in two concurrences, recognized that the long term monitoring of each and every single

---

three 120-degree arcs of the 360-degree circle surrounding the tower the particular phone is located. In some cases, however, the available information is even more precise.

Often, especially in urban and suburban areas, the signal transmitted by a cellular telephone is received by two or more antenna towers simultaneously. Knowledge of the locations of multiple towers receiving signals from a particular telephone at a given moment permits the determination, by simple mathematics, of the location of the telephone with a fair degree of precision through the long established process known as triangulation. Real time information concerning the location permits the geographic movements of the phone to be tracked as they occur.

Cellular telephone service providers record the identity and location of the antenna towers receiving signals from each phone at every point in time. As noted, some record also which 120-degree face or sector of the tower faces the phone. Some record also the identities and locations of all antenna towers receiving signals from each phone at every moment. Providers keep this information for anywhere from 12-24 months.

[4] Kim Zetter, "Feds "Pinged" Sprint GPS Data 8 Million Times Over a Year," Wired.com, *available at* http://www.wired.com/threatlevel/2009/12/gps-data/ (last visited March 1, 2010).
[5] http://www.popsci.com/technology/article/2012-07/wireless-carriers-reveal-how-often-theyre-asked-hand-over-user-data-not-how-often-they-do
[6] U.S. v. Maynard, 615 F.3d 544 (D.C. Cir. 2010)

movement made by a person, no matter what technology is used, impinges on an individual's reasonable expectation of privacy.[7]

Unlike a GPS tracker on a car, which tracks the driver only when he/she drives, pinging follows the cell phone wherever it goes, regardless of whether the holder is using it. Thus it would seem that after *Jones* courts would require a search warrant based upon probable cause before the government can obtain someone's cell phone tracking information. However, this is not the case. Lower courts have addressed (and continue to address) cell phone pinging and are coming to different conclusions. Some have held that this is a Fourth Amendment search subject to a warrant; others have held that under the Federal Electronic Communications Privacy Act (written in 1986 prior to the explosion of cell phone use and technology) the standard is lower. In fact, many of the courts have explicitly called on legislatures to clarify this issue. It is up to the state legislatures to lead the way and protect privacy while balancing the needs of law enforcement.

What HB 377 does

HB 377 would allow law enforcement to obtain someone's cell phone location tracking information based upon a showing that the information is "relevant to an ongoing criminal investigation." This is almost identical to the standard used for pen registers and trap/trace devices. Md. Cts. & Jud. Proc. § 10-4B-01. Despite the inclusion of the words "probable cause," this is not the search warrant standard; it is much lower. Under Maryland law, law enforcement may obtain a search warrant upon a showing that there is probable cause to believe that a criminal offense is being committed by the person or at the place for which the warrant is sought. Md. Crim. Pro. § 1-203.[8]

There is a substantive difference between the two sets of information, and thus a reason they should have different standards. Pen registers or trap/trace devices only record the numbers called or received from that particular phone. Contrast that with cell phone location tracking information, which shows everywhere you go and have gone. The pervasive nature of the surveillance with cell phone tracking is a search under the Fourth Amendment and thus a search warrant is required.

Law Enforcement Should Get A Warrant – And Many Do

A number of enforcement agencies across the country, in states as diverse as California, Colorado, Hawaii, Kansas, Kentucky, Nevada, New Jersey, North Carolina, and Wisconsin, obtain probable cause warrants in order to access cell phone location information.

---

[7] Earlier Supreme Court cases also lend credence to the view that a search warrant based upon probable cause would be required for cell phone tracking. *See Katz v.* ***United States****,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)(Court held that "the Fourth Amendment protects people, not places," and found a violation in attachment of an eavesdropping device to a public telephone booth); *see, also* See, *e.g., Bond v.* ***United States****,* 529 U.S. 334, 120 S.Ct. 1462, 146 L.Ed.2d 365 (2000); *California v. Ciraolo,* 476 U.S. 207, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986); *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979).

[8] Courts review probable cause challenges under a 'totality of the circumstances' test. That is, whether there is a fair probability that evidence of a crime will be found in a particular place. *See Illinois v. Gates*, 462 U.S. 213, 238; *Patterson v. State*, 401 Md. 76, 91-92 (Ct. App. 2007).

These law enforcement agencies are able to protect public safety and privacy by meeting the warrant and probable cause requirement, and so can Maryland.

Finally, in cases of emergency there is already a mechanism ("exigent circumstances" exception) by which law enforcement can bypass the warrant requirement, such that requiring a warrant in non-emergency situations would not hamper their ability to respond to an emergency.

For these reasons, we oppose HB 377.