ACLU
AMERICAN CIVIL LIBERTIES UNION of MARYLAND

SARA N. LOVE
PUBLIC POLICY
DIRECTOR

Testimony for the Senate Judicial Proceedings Committee
March 6, 2014

SB 698 – Criminal Procedure – Electronic Device Location Information – Warrant

SUPPORT

The American Civil Liberties Union of Maryland supports SB 698. This bill would require that a law enforcement officer obtain a search warrant before obtaining electronic device location information. Innovation in the field of communications has long outgrown the bounds of Maryland's statutes designed to protect us from unwarranted intrusion and this bill is necessary to re-calibrate the careful balance our society has always struck between technology and privacy.

As of December 2012, there were 326.4 million wireless subscriber accounts in the United States, responsible for 2.30 trillion annual minutes of calls and 2.19 trillion annual text messages.[1] The number of wireless accounts now exceeds the total population of the United States,[2] more than 83% of American adults own cell phones,[3] and one in three U.S. households has only wireless telephones.[4] Americans – and Marylanders – carry our cell phones with us everywhere we go, unaware that those same phones are transmitting our location – sometimes to a very precise degree – every few seconds.

AMERICAN CIVIL LIBERTIES UNION OF MARYLAND

MAIN OFFICE
& MAILING ADDRESS
3600 CLIPPER MILL ROAD
SUITE 350
BALTIMORE, MD 21211
T/410-889-8555
or 240-274-5295
F/410-366-7838

FIELD OFFICE
6930 CARROLL AVENUE
SUITE 610
TAKOMA PARK, MD 20912
T/240-274-5295

WWW.ACLU-MD.ORG

Background
In order to provide service to cell phones, cell phone companies maintain networks of radio base stations. These stations are no longer just big towers, but can be as small as conventional stereo speakers and mounted on stationary objects such as trees or flagpoles, or even in homes and offices. Each base station covers a geographic area (a "cell site").

Whenever a cellular telephone is on, regardless of whether it is making or receiving a call, text or email, it periodically and automatically transmits a unique identification number to register its presence and location in the network ("registration").
When a phone communicates with the network, the service provider automatically retains information about such communications.

Most cell sites consist of three directional antennas that divide the cell site into three 120-degree sectors. In addition to cell site and sector, some carriers also calculate and log the caller's distance from the cell site.[5]

The precision of determining a user's location depends upon the size of the sector. As more and more consumers buy cell phones and demand better coverage, more and more cell sites are needed, so the coverage of those cell sites and sectors become smaller and smaller. In addition to erecting conventional cell cites, providers also use low-powered, smaller cells, called "microcells," "picocells," or "femtocells," which provide service to

---

[1] *U.S. Wireless Quick Facts,* CTIA – The Wireless Association, http://www.ctia.org/advocacy/research/index.cfm/aid/10323.
[2] *Id.*
[3] Aaron Smith, Pew Research Ctr., *Americans and Text Messaging 2* (2011), http://pewinternet.org/~/media//files/Reports/2011/Americans%20and%20Text%20Messaging.pdf
[4] *U.S. Wireless Quick Facts, supra* note 1.
[5] *See Verizon Wireless Law Enforcement Resource Team (LERT) Guide 25* (2009), http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/ (providing sample records indicating caller's distance from cell site to within .1 of a mile).

areas as small as 10 meters.[6] As one court noted, "in urban areas and other environments that use microcells, this area can be small enough to identify individual floors and rooms within buildings."[7]

Real-time vs. Historical Location Tracking

Tracking someone in real-time or "pinging" means using their cell phone to determine their location. Telecommunications providers either give law enforcement the data that the phone automatically creates when it registers with a tower, [8] or they "ping" the phone by calling it and disconnecting immediately, without the user ever knowing the phone was called. This also pinpoints the phone's location. Real time information concerning the location permits the geographic movements of the phone to be tracked as they occur.

In addition, law enforcement use historical cell phone information for tracking purposes – that is, tracking where someone was at a given point in time or over a period of time. Historical records include the location information from each call or text message to or from a cell phone. As described above, depending on where that phone is, the location information may be very precise or less precise, and that will vary during the day as the user moves about in his or her daily life from areas with denser cell sites to areas with more sparse cell sites. Based upon the number average number of calls and texts, a Court noted in 2010 that historical cell site data for the typical adult user would reveal between 20-55 data points a day.[9] That number has likely gone up significantly in the last 4 years. In addition, some carriers' historical records include latitude and longitude along with the sector identification data, and some carriers store not only the location information when calls or texts are sent or received, but also location information as the device moves around the network.[10]

Law enforcement will argue that the data they obtain from historical information is less precise than the data they obtain from real-time tracking. In some cases that is true, depending on the density of the cell sites and the number of calls/texts/connections the user makes. But in other cases, the carrier will retain extremely precise information, as described above.

In addition to having the location—either more or less precise—of the phone at any given point in time, the aggregate of those points paint a picture of a person's life. Knowing periodic information about which cell sites a phone connects to over time can be used to determined the path the phone user traveled. For example, in *U.S. v. Graham*, the government argued that the historical cell site data points showing Defendants' locations revealed trajectories that placed them at the stores that were robbed at the time of the robberies. The map attached to this testimony is one the government used in its case against *Graham*, using historical data points to locate Defendants' phones, and thus their culpability for the robberies.[11]

---

[6] Ctr. For Democracy & Tech, *Cell Phone Tracking: Trends in Cell Site Precision (2)* (2013).
[7] *In re Application of the United States of America for Historical Cell Site Data*, 747 F.Supp.2d 827, 833 (S.D. Tex. 2010), *rev'd* by 724 F.3d 600 (5th Cir. 2013).
[8] In addition, some law enforcement agencies – including Montgomery County – use their own technology, called "stingrays," to gather this information. *See http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/.*
[9] *In re Application, supra* note 7.
[10] *Id.* at 833-834.
[11] In that case the government used 13 out of 58,069 data points for their case. Imagine what the remaining 58,056 remaining data points would show about Graham's life. Amicus Brief of the ACLU in *United States v. Graham*, https://www.aclu.org/technology-and-liberty/us-v-graham-aclu-

A data point at the cell site closest to one's home late at night, and another data point early in the morning can imply that the user was home at night. Data points at those same times in a different location can imply the user was not at home at that time, and other information about the user can add to the picture of where the user spent that night. In *Graham*, the defendant's wife was pregnant. Twenty-nine calls during business hours began or ended in the sector where the OB/GYN's office was located, indicating that the defendant was with his wife at the doctor at those times.

Privacy Implications

As discussed, because people carry their cell phone with them at all times, and because that cell phone is constantly transmitting its location information, cell phone location information gives a very detailed picture of a person's behavior. It can show 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."[12]

Law enforcement is accessing this information at staggering rates. In response to a letter from Senator Markey, T-Mobile and AT&T responded that together they received nearly 600,000 requests for customer information in 2012. Requests to Verizon have doubled in the last five years. The volume of requests is so high that AT&T has to employ more than 100 full-time workers to process them.[13]

Without the proper standard, the implications for privacy and opportunities for abuse are significant. This is an issue that brings together diverse coalitions, as is evidenced by Digital Due Process, an organization that supports the warrant standard and has members such as the ACLU, ALEC, Apple, AOL, AT&T, Ebay, Google and IBM, to name a few.[14]

Legal Standards

The legal standard for whether law enforcement needs a warrant or a court order to obtain cell phone tracking information is not settled. *United States v. Jones*, 132 S.Ct. 945 (2012), indicates the Supreme 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 movement made by a person, no matter what technology is used, impinges on an individual's reasonable expectation of privacy.[15]

---

amicus-brief; *see also https*://www.aclu.org/blog/technology-and-liberty-national-security/fighting-striking-case-warrantless-cell-phone-tracking

[12] *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S.Ct. 945 (2012).

[13] Catherine Crump, Cellphone Companies Reveal How Often They Hand Your Data Over to Law Enforcement, FUTURE TENSE (Dec. 9, 2013), http://www.slate.com/blogs/future_tense/2013/12/09/ed_markey_letters_from_cellphone_companies_how_often_at_t_t_mobile_give.html

[14] *See* Digital Due Process Coalition, http://digitaldueprocess.org.

[15] 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,

Unlike a GPS tracker on a car, which tracks the driver only when he/she drives, location tracking 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[16]) cell phone tracking and are coming to different conclusions. Some have held that this is a Fourth Amendment search subject to a warrant[17]; 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.[18] 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 SB 698 does

SB 698 would require law enforcement to obtain a search warrant based upon probable cause prior to obtaining someone's electronic device location tracking information. Electronic devices includes cell phones, GPS devices, internal automobile GPS, iPads, social networking check-ins, as well as electronic devices that can be tracked but have not been invented yet. SB 698 also: provides an exception to the warrant requirement in exigent circumstances or with the owner's or user's consent; sets parameters for how long the tracking can proceed; provides notice to the user that he or she was tracked; and allows a court to delay that notice upon a showing of good cause.

AMERICAN CIVIL LIBERTIES UNION OF MARYLAND

Law Enforcement Should Get A Warrant – And Many Do

Both Maine and Montana have enacted laws requiring law enforcement to obtain a warrant before they track individuals using electronic devices.[19] In addition, 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. These law enforcement agencies are able to protect public safety and privacy by meeting the warrant and probable cause requirement, and so can Maryland.

For these reasons, we support SB 698.

---

351 (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*, *e.g., Bond v. United States,* 529 U.S. 334 (2000); *California v. Ciraolo,* 476 U.S. 207 (1986); *Smith v. Maryland,* 442 U.S. 735 (1979).

[16] *U.S. v. Graham*, No. 1:11-CR-00094-RDB (D. Md.) is currently pending before the Fourth Circuit; *U.S. v. Sereme*, No. 2:11-CR-97-FtM-29SPC (M.D. Fla.) is currently pending before the Eleventh Circuit.

[17] *See e.g., Commonwealth of Massachusetts v. Augustine*, No. SJC-11482 (Feb. 18, 2014), *State of New Jersey v. Earls*, 70 A.3d 630 (N.J. 2013); *United States v. Maynard*, 615 F.S3d 544 (D.C. Cir. 2010); *In re 2012 Tex. Application*, 2102 WL 4717778 (S.D. Tex. 2012); *In re 2010 S.D. Tex. Application*, 747 F. Supp.2d 827 (S.D. Tex. 2010); *In re 2010 E.D.N.Y Application*, 736 F.Supp.2d 578 (E.D.N.Y. 2010).

[18] *See e.g., In re: Application of the United States of America For Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)*; United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012); *In re: MD Application*, 402 F.Supp.2d 597 (D.Md. 2005).

[19] Leg.mt.gov/bills/2013/billhtml/HB0603.htm; Ryan Gallagher, *Maine Enacts Pioneering Law Prohibiting Warrantless Cellphone Tracking*, FUTURE TENSE (July 10, 2013), www.slate.com/blogs/future_tense/2013/07/10/new_maine_law_prohibits_warrantless_cellphone_tracking.html.