JOANNA DIAMOND
ADVOCACY CONSULTANT

Testimony for the House Judiciary Committee
February 13, 2018

HB 510 – Criminal Procedure – Providing Electronic Device Location Information – Historical Data

SUPPORT

The ACLU of Maryland supports HB 510, which would require that a law enforcement officer obtain an order pursuant to Md. Crim. Proc. 1-203.1 before obtaining historical electronic device location information.

This legislation is necessary because of the extraordinary proliferation of physical devices and software services that automatically collect minutely detailed information about the location and movements of the huge numbers of people who possess them or use the services (such as every person with a cell phone), and transmit the information to companies that store the data (like our cellular service providers, or Google). Those vast troves of detailed location data have become a privacy nightmare, and an irresistible target for law enforcement data requests. The end result, absent this legislation, is that the devices and software that we depend on in ever increasing ways, are also turning those same devices and programs in personal tracking tools for the government, to be utilized without any meaningful privacy protections. HB 510 remedies this situation.

In 2014, the General Assembly passed, and the Governor signed, SB 698, requiring law enforcement to obtain a warrant[1] prior to tracking someone, in real-time, using their electronic device. Electronic devices include cell phones, GPS devices, internal automobile GPS units and iPads, as well as electronic devices that can be tracked but have not been invented yet. While that law was a huge leap forward for privacy, it left a significant gap by not setting rules governing access to the huge quantity of historical data that companies now collect about our movements, whether via hardware (like cell phones) or software (like Google Timeline, https://www.google.com/maps/timeline) Historical tracking should be added to our warrant statute to protect Marylanders' Fourth Amendment rights.

Ubiquity of location tracking

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. As of December 2014, there were 355.4 million wireless subscriber accounts in the United States.[2] Forty-seven percent of households are wireless only[3] and more than 90% of American adults own cell

[1] For clarity's sake, we will use the term "warrant." Md. Crim. Proc. §1-203.1 uses the term "order," but the statute requires the standards used to obtain a warrant, and §1-203 is the warrant statute.
[2] *U.S. Wireless Quick Facts,* CTIA – The Wireless Association, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey
[3] *Id.*

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

WWW.ACLU-MD.ORG

COLEMAN BAZELON
PRESIDENT

SUSAN GOERING
EXECUTIVE DIRECTOR

ANDREW FREEMAN
GENERAL COUNSEL

phones.[4] Forty-four percent of cell phone owners "have slept with their phone next to their bed because they wanted to make sure they didn't miss any calls, text messages, or other updates during the night." Twenty-nine percent of cell owners describe their cell phone as "something they can't imagine living without."[5]

Other common devices also create a location data trail. For example, the GPS units built in by car companies transmit location data (among other information) to manufactures who retain it in individually identifiable ways.[6] Increasingly popular fitness trackers often come equipped with GPS trackers that transmit location information to the manufacturer.

In addition, many smartphone apps transmit location information to the developer in order to function. For example, Google Timeline, built in to every Android smartphone, keeps finely detailed GPS data of the owner's movements for years at a time.[7]

The analysis below largely focuses on cell phone location tracking, because it is the most ubiquitous, given the pervasive ownership of cell phones.

Technical background of cell phone location tracking

Because cell phones are so widely distributed, it is important to understand how they function as location tracking devices. 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.[8]

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

---

[4] http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/
[5] *Id.*
[6] https://www2.onstar.com/web/portal/privacy?g=1
[7] https://theintercept.com/2015/11/06/how-law-enforcement-can-use-google-timeline-to-track-your-every-move/
[8] *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).

"femtocells," which provide service to areas as small as 10 meters.[9] 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."[10]

Real-time vs. historical location tracking

Tracking someone in real-time or "pinging" means using their cell phone to determine their location at that moment. Telecommunications providers either give law enforcement the data that the phone automatically creates when it registers with a tower,[11] 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. Law enforcement must get a warrant to obtain this information. Md.Crim.Proc. §1-203.1.

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.[12] That number has likely gone up significantly in the last 6 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.[13]

While government access to historical location data poses all of the same privacy concerns as does access to real-time data, historical data adds one unique feature. It acts as a virtual time machine, allowing law enforcement agents to go back in time to track a person's location long before the agents knew of the person or became interested in them. While it is easy to see the appeal of such data, it is equally important that the same protections that exist for real-time data should apply.

What HB 510 does

HB 510 would add "historical location" to the law requiring law enforcement to obtain a search warrant based upon probable cause prior to obtaining someone's electronic device location tracking information.

---

[9] Ctr. For Democracy & Tech, *Cell Phone Tracking: Trends in Cell Site Precision (2)* (2013).
[10] *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).
[11] In addition, many agencies use their own technology, called "stingrays," to gather this information. While these are covered by the 2014 law, they continued to be used in Maryland.
[12] *In re Application, supra* note 6.
[13] *Id.* at 833-834.

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. 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.

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.

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."[14]

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.[15]

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.[16] In addition, in a recent survey about public perception, 82% of Americans believe that "details of your physical location over time" are sensitive, with fully half believing they are "very sensitive."[17]

Legal Standards

In order to obtain someone's real-time location information, law enforcement must obtain a warrant (an "order" under Maryland's language) that there is "probable cause to believe that:

> (i) a misdemeanor or felony has been, is being, or will be committed by

---

[14] *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).

[15] 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

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

[17] http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

the owner or user of the electronic device or by the individual about whom location information is being sought; and

(ii) the location information being sought:

1. is evidence of, or will lead to evidence of, the misdemeanor or felony being investigated; or

2. will lead to the apprehension of an individual for whom an arrest warrant has been previously issued."

Md.Crim.Proc. §1-203.1. This parallels Maryland's search warrant language. Md.Crim.Proc. §1-203.

However, to obtain historical location tracking information about a subscriber held by a company, Maryland law enforcement officers currently rely on a provision of the Maryland Stored Wire and Electronic Communications and Transactional Records Act that allows access to such information whenever they can show to a court "that there is reason to believe the records or other information sought are relevant to a legitimate law enforcement inquiry."[18] In other words, in order to access historical location data held by companies about their customers or subscribers, which can be just as, if not more, revealing of private facts as real time data, law enforcement agents need not establish that a crime has been committed, that the data will lead to evidence of the crime, or that subscriber whose data is sought is the suspect.

Whether these lesser statutory standards for access to stored location information comply with the Fourth Amendment's prohibition on unreasonable searches and seizures 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 historical cell cite location data. 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 a narrow trespass theory (that the installation of the GPS device on the car was a physical intrusion requiring a warrant), 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.

In the absence of a conclusive decision from the Supreme Court, lower courts have reached conflicting decisions on the appropriate legal standard governing government access to historical cell phone location information: some have held that this is a Fourth Amendment search subject to a warrant[19]; others have held that

[18] Md. Code, Cts. & Jud. Proc. § 10-4A-04(c)(1) (Maryland's standard mirrors the federal standard in the Stored Communications Act, 18 U.S.C. §2703(d)).

[19] *See e.g., Commonwealth of Massachusetts v. Augustine*, 4 N.E.3d 846 (Mass. 2014), *State of New Jersey v. Earls*, 70 A.3d 630, 642 (N.J. 2013)("[CSLI can reveal not just where people go – which doctors, religious services, and stores they visit – but also the people and groups they choose to affiliate with and when they actually do so"); *United States v. Maynard*, 615 F.S3d 544 (D.C. Cir. 2010); *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. Of a Specified Wireless Tel.*, 849 F.Supp.2d 526, 539 (D. Md. 2011)("reasonable expectation of privacy both in [subject's] location as revealed by real-time {CSLI} and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days");

the data can be obtained under the Stored Communications Act, where the standard is lower.[20] 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.

In August, 2015, the U.S. Court of Appeals for the Fourth Circuit (covering Maryland) decided *U.S. v. Graham*, 796 F.3d 332 (4th Cir. 2015). The Court in *Graham* held that the "government's warrantless procurement of the CSLI [cell site location information] was an unreasonable search in violation of Appellants' Fourth Amendment rights."[21] In that case, the government requested and obtained 221 days of historical cell site location data from Sprint/Nextel, resulting in 29,659 location data points for Graham, and 28,410 for Jordan, enough to provide a detailed account of their movements during the time period the data covered. As one example of how detailed the information was, 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.

The Fourth Amendment to the U.S. Constitution protects individuals from unreasonable searches and seizures. "A 'search' within the meaning of the Fourth Amendment occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable." *Id., at 344, citing Kyllo v. United States*, 533 U.S. 27, 33 (2001).

> We hold that the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI [cell site location information] for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information. Its inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies.

Graham, 793 F.3d at 344-345

Law Enforcement has argued that because a third party – the cell carrier – holds these records, there is no expectation of privacy, and thus no need for a warrant. This analysis only applies when an individual voluntarily turns that information over to third parties. *See United States v. Miller*, 425 U.S. 435 (1976), *Smith v. Maryland*, 442 U.S. 735 (1979). As the Court in *Graham* pointed out, individuals do not "convey" their location information to their service provider "at all –

In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809. F.Supp.2d 113, 120 (E.D.N.Y. 2011) ("reasonable expectation of privacy in long-term cell-site location records").

[20] *United States v. (Quartavious) Davis,* 785 F.2d 498, 516-18 (11th Cir. 2015) (en banc) *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).

[21] In October, 2015, the Fourth Circuit granted a motion to re-hear the case *en banc*.

voluntarily or otherwise – and therefore does not assume any risk of disclosure to law enforcement." *Graham*, 796 F.3d at 353.

Law enforcement should get a warrant for historical data – and many do. Seven states have laws requiring law enforcement to obtain warrants to access historical cell site location information.[22] Maryland should protect its citizen's Fourth Amendment rights as well.

For the foregoing reasons, the ACLU of Maryland supports HB 510.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

[22] https://www.aclu.org/map/cell-phone-location-tracking-laws-state.