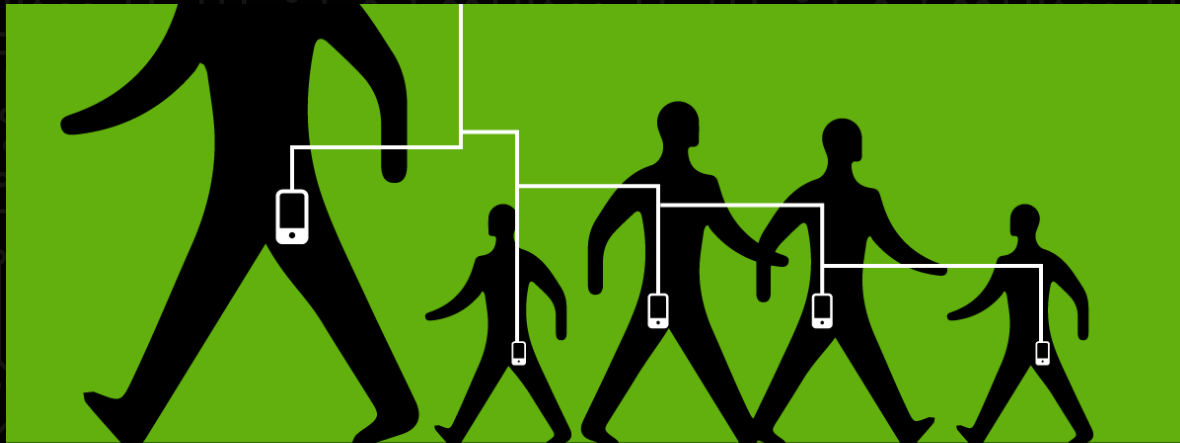


Cell Site Location Information



A cell phone's location, whether stationary or moving, can be tracked through cell site location information (CSLI) or global positioning system (GPS) data

Cell Site Location Information (“CSLI”)

- A cell phone is constantly searching for the cell tower with the strongest signal to connect it to the mobile network in order to provide the user with the fastest service. Each time a cell phone connects with a cell tower, the time and duration of that connection is recorded by the cell phone service provider.

NOV 9 2011 18:10:50



Types of CSLI:

- Cell phone companies store historical and prospective CSLI, along with prospective GPS data, which police may request.
 - Historical data can be used to track past movements.
 - Prospective data allows police to track a phone in real time.

Real-time "pinging":

- In addition to the data a cell phone regularly relays to cell towers, a cell phone may be "pinged" in an emergency to force it to reveal its location to the carrier.
- "Ping" is another word for "contact" or "connect."
- "Pinging" means to send a signal to a particular cell phone and have it respond with the requested data, typically revealing location data for the connected cell towers

Global Positioning System ("GPS")

- Tracks a device's movements using signals received from satellites at set intervals in order to determine a device's location.
- The recorded location data may be stored within the device itself, or it may be transmitted to a central location database, or Internet-connected computer, using a cellular (GPRS or SMS), radio, or satellite modem embedded in the device.

Seminal CSLI Case:

- *US v. Carpenter*, 585 U.S. ___, 138 S. Ct. 2206 (2018) - SCOTUS held seizure of 7 days or more of historical CSLI is a search requiring a probable cause search warrant and that the third-party doctrine (TPD) does not defeat an individual's reasonable expectation of privacy in CSLI.

How do cops get CSLI?

- Prior to Carpenter, police routinely sought access to CSLI in criminal cases using either
 - 2703(d) order under the Stored Communications Act (18 USC 2701, et seq.) (a “D Order”), or
 - D Order + a pen register/trap and trace order under the Pen Register and Trap and Trace Device Act (18 USC 3121, et seq.); rather than seeking a probable cause warrant.

How do cops get CSLI?

- Post Carpenter, cops must obtain a probable cause warrant for 7 days or more of historical CSLI.
- But expect that the government will try to rely on the *Leon* good faith exception to avoid suppression where they failed to obtain a warrant pre-*Carpenter*.
- A number of jurisdictions also require a PC SW for real-time CSLI.

What to look for?

- Seizure of your client's cell phone or other digital device with location tracking capabilities such as personal health trackers like Fitbits and Apple watches.
- Any mention of cell phone extraction software, like Cellebrite, Pen-Trace, Secureview, Oxygen, FTK Imager, Encase, MSAB XRY, or E-fense Helix3.

What to look for?

- Any subpoenas or search warrants addressed to cell phone service providers like AT&T, T-Mobile, Verizon, Sprint, Boost Mobile, MetroPCS, etc. that include location information.
- Any discovery referring to cell tower location information, GPS data, or cell phone extraction reports that include location information.
- Any subpoenas or search warrants seeking “accounts associated with the area near” a specified location.

How do I challenge CSLI evidence?

- File a discovery motion requesting the raw data and methodology of seizure.
- Where law enforcement fails to obtain a probable cause search warrant for CSLI, file a motion to suppress pursuant to *US v. Carpenter*, 585 U.S. ___, 138 S. Ct. 2206 (2018).

How do I challenge CSLI evidence?

- Where law enforcement *does* obtain a warrant for CSLI, refer to our strategies for [How to Challenge a Digital Device Search](https://www.eff.org/defense/DDS) ([eff.org/defense/DDS](https://www.eff.org/defense/DDS))
- Challenge the foundation and authenticity of the proffered CSLI record(s).

How do I challenge CSLI evidence?

- Rely on more privacy-protective state laws. Many states have enacted statutes requiring a warrant to get CSLI: California, Colorado, Maine, Minnesota, Montana, New Hampshire, New Mexico, and Utah.
- Other states like Illinois, Indiana, and Maryland, specifically protect real-time CSLI; while Iowa protects GPS location data. The standards for obtaining these types of warrants differs from state to state, along with what kind of CSLI is being sought.

How do I challenge CSLI evidence?

- California's CalECPA not only requires law enforcement to obtain a search warrant (CA Penal Code § § 1546.1) before obtaining CSLI, but also provides for a notice requirement (CA Penal Code section § § 1546.2) and a statutory suppression remedy (CA Penal Code § § 638.55, 1546.4) for violation of the state's warrant requirement.

How do I challenge CSLI evidence?

- You can learn more about CalECPA by going through this Prezi presentation. And for a peek at what California police are being told about CalECPA, take look at this CA Peace Officers' Association Fact Sheet on CalECPA.

How do I challenge CSLI evidence?

- The Florida and New Jersey State Supreme Courts require a warrant for real-time CSLI.
- A more comprehensive geo-location privacy protection bill was proposed in Illinois, but was vetoed by the Governor in September of 2017.

How do I challenge CSLI evidence?

- Refer to ACLU's chart (last updated 10/13/15) for the status of state legislation on locational privacy across the country.

Where do I learn more?

- Visit: <https://eff.org/defense/CSLI>
- Read EFF's *Carpenter* amicus brief: <https://eff.org/CSLICarpenter>
- Visit EFF's Cell tracking issue web page: <https://eff.org/celltracking>
- For a review of State CSLI laws: <https://eff.org/CSLIstatelaws>

Stephanie Lacambra
Criminal Defense
Staff Attorney
415-436-9333 x130
stephanie@eff.org