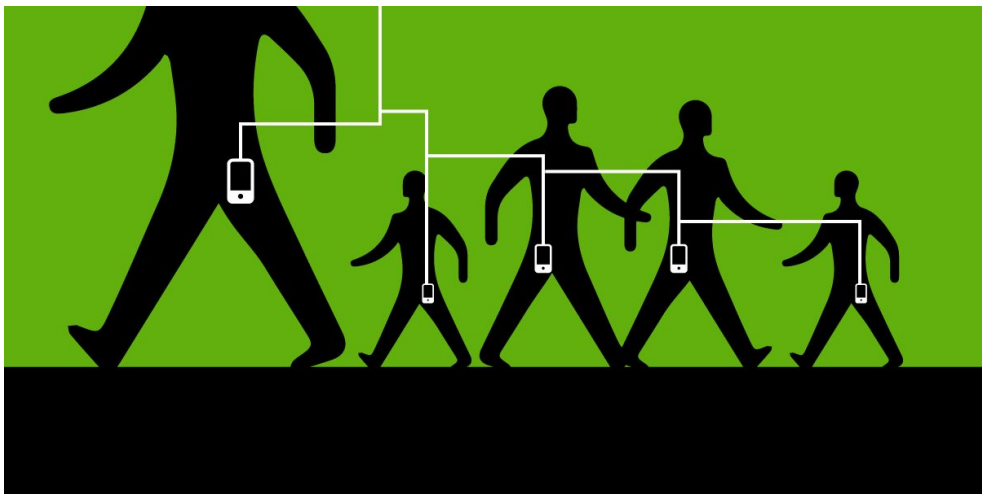
Cell Site Location Information

A Guide for Criminal Defense Attorneys



EFF One-Pager
Revised 3.28.19

Learn more:
eff.org/defense/CSLI

Support our work on CSLI:
eff.org/donate

What is it?

- A cell phone's location, whether stationary or moving, can be tracked through cell site location information (CSLI) or global positioning system (GPS) data. CSLI, which is also referred to as cell phone location tracking, refers to information cell phones convey to nearby cell towers.

How does it work?

- 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.
    - In addition to the data a cell phone regularly relays to cell towers, a cell phone may be "pinged" to force it to reveal its location to the carrier.
    - 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.
- GPS – the 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 database or Internet-connected computer using a cellular (GPRS or SMS), radio, or satellite modem embedded in the device.

Review cell-site location information cases (http://eff.org/CSLIcases)

- **Seminal 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.

What Do the Cops Do?

- Prior to the *Carpenter* decision, police routinely sought access to CSLI in criminal cases using either a 2703(d) order under the Stored Communications Act (18 USC 2701, et seq.) (a "D Order"), or a D Order in combination with 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. Expect that the government will try to rely on the *Leon* good faith exception to avoid suppression where they failed to obtain a warrant.

How to challenge the use of cell phone location data?

- File a discovery motion requesting the raw data and methodology of seizure.
- Where law enforcement fails to obtain a warrant for CSLI, file a motion to suppress citing *US v. Carpenter*, 585 U.S. _____, 138 S. Ct. 2206 (2018).
- Where there is a warrant, refer to our strategies for How to Challenge Digital Device Searches
- Look for potential grounds for support from 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. For example, California's CalECPA has specific particularity requirements for SWs seeking electronic location information.
- Challenge the foundation and authenticity of the proffered CSLI records.

How do I learn more?

- Visit: https://eff.org/defense/CSLI
- Read EFF's SCOTUS amicus brief: https://eff.org/CSLICarpenter
- Cell tracking issue web page: https://eff.org/celltracking
- State CSLI laws: https://eff.org/CSLIstatelaws

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