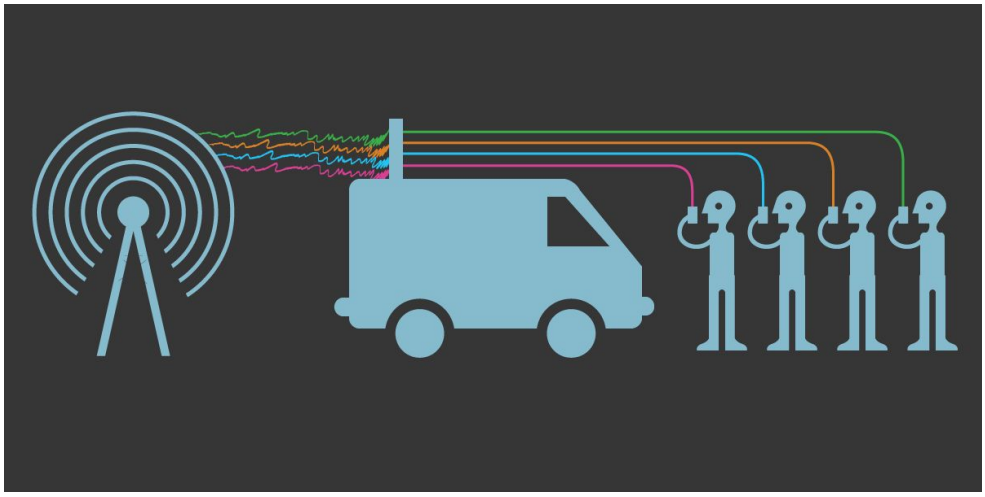
Cell-Site Simulators

A Guide for Criminal Defense Attorneys



EFF One-Pager
Revised 10.3.18

Support our work on Cell Site Simulators: eff.org/donate

What are they?

- A cell-site simulator ("CSS", also commonly referred to as an "IMSI catcher" or "Stingray") is a device that law enforcement uses to locate a suspect's cell phone. CSSs masquerade as legitimate cell phone towers, "tricking" all nearby cell phones into connecting to the device instead of to nearby cell towers. CSSs are not restricted to just suspect targets, but log the International Mobile Subscriber Identity ("IMSI") numbers of all cell phones within range of the device. They are useful to law enforcement because they can pinpoint a phone's location in real time with much greater precision than cell site location information stored and tracked by cell phone companies.

How do they work?

- Cell-site simulators work by taking advantage of a phone's preference for the strongest (or what appears to be the strongest) cell tower signal in the area.
- At this point, there is no way for a phone to be configured to avoid sharing its unique identifying number with a CSS.
- CSSs may also be configured to capture content such as texts, calls, and unencrypted communications. However, end-to-end encrypted apps, which encrypt messages between senders, should still provide some protection. It is very difficult to tell from the cell phone itself whether its information has been captured by a CSS, and there is no notification that encryption on the phone has been subverted or is no longer operating.

How Do I Know If Law Enforcement Used a CSS?

- Lookout for search warrants referring to a "confidential informant" used to identify a suspect's location or language that tracks the DOJ's model CSS warrant application, which uses terms like: "target cell phone", "pen register" and "trap and trace."
- Look for other CSS-related terms, like: IMSI catchers, digital analyzers, "WITT", the FBI's "Wireless Intercept Tracking Team", or Stingrays, Triggerfish, KingFish, ArrowHead, AmberJack, Blackfin, Stargazer and Hailstorm (which are models of CSSs)
- Review the DOJ's CSS policy

How to challenge them?

- File a motion to suppress. Prior to a September 2015 policy change for the DOJ, IRS, and the Department of Homeland Security, most CSS use was done without a warrant. Read the policy change here: https://eff.org/CSSDOJ
- Review the stern House Oversight Committee report: https://eff.org/CSSHOGR
- Review the leading locational privacy cases:
    - SCOTUS: *Carpenter v. U.S.*, 585 U.S. __, 138 S.Ct. 2066, 2217 (2018): law enforcement must get a warrant to search location data of 7 or more days. EFF *Carpenter* amicus: https://www.eff.org/document/amicus-brief-carpenter
    - 7th Cir.: *U.S. v. Damian Patrick*, 842 F.3d 540 (7th Cir. 2016) (cert denied, 138 S.Ct. 2706): Rejected MTS argument that CSS use required a warrant. EFF *Patrick* amicus: https://eff.org/CSSPatrick
    - Southern District of New York: *U.S. v. Raymond Lambis*, 197 F.Supp.3d 606 (S.D.N.Y. 2016): Granted MTS for warrantless CSS use and rejected the government's attenuation and third-party doctrine arguments. EFF *Lambis* amicus: https://eff.org/CSSLambis
    - Court of Special Appeals of Maryland: *State of Maryland v. Kerron Andrews*, 227 Md.App.350 (Md. App. 2015): Granted MTS for warrantless CSS use, rejected the third-party doctrine, and rejected pen register and trap & trace order as substitute for warrant. https://eff.org/CSSAndrews
    - Northern District of Illinois: *Matter of the Application of the US*, 2015 WL 6871289 (N.D. IL 2015): District Court order re: minimization of CSS use. https://eff.org/CSSNDIL

How do I learn more?

- Visit https://eff.org/defense, https://eff.org/CSSFAQ and https://www.eff.org/sls
- For more details on how CSSs work, see the CSS manuals cited in the following Intercept article: https://eff.org/CSSmanuals
- For details on the racial disparity of CSS deployment see: https://www.eff.org/CSSFCCBaltimore

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