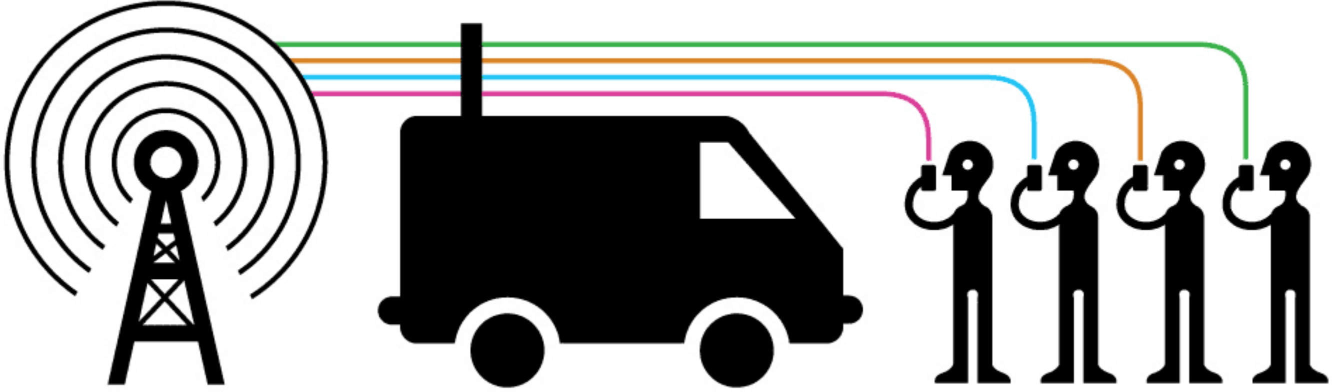
ELECTRONIC FRONTIER FOUNDATION

The leading nonprofit defending digital privacy, free speech, & innovation.

Cell Site Simulators

A Guide for Criminal Defense Attorneys

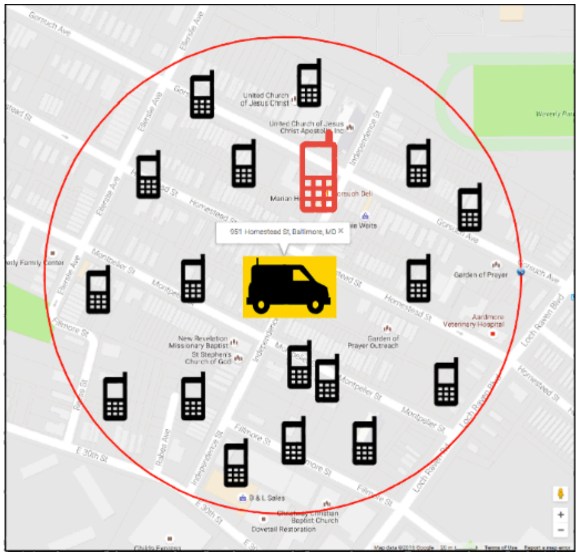


1. What are they and how do they work?

   a. Cell-site simulators ("CSS"), also commonly known as IMSI catchers or Stingrays, are devices that law enforcement uses to try to locate suspects. CSSs masquerade as legitimate cell phone towers, tricking all phones nearby into connecting to the device instead of the tower. They can log the IMSI numbers (a unique identifying number) of all mobile phones in a given area. 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 that comes from the phone company.

   b. Cell-site simulators work by taking advantage of a phone's preference for the strongest cell tower signal in the area. Because CSSs cause the phone to connect to the device rather than the cell tower, they actively interfere in communications between cell phones and towers.

   c. At this point, there is no way for a phone to be configured to avoid sharing its unique identifying number with a CSS. Also, in general, metadata like phone numbers dialed are not encrypted in transit so these may be revealed to a CSS.


951 Homestead St, Baltimore, MD
Gorsuch Ave
Homestead St
Montpelier St
Fillmore St
Independence St
Ellerslie Ave
E 30th St
Loch Raven Blvd
United Church of Jesus Christ
United Church of Jesus Christ Apostolic Inc
Garden of Prayer
Garden of Prayer Outreach
Aardmore Veterinary Hospital
New Revelation Missionary Baptist
St Stephen's Church of God
B & L Sales
Dovetail Restoration
Waverly Park

d. CSSs may also be configured to capture some content such as texts, calls, and unencrypted communications. However end-to-end encrypted apps should still provide some protection. It is very difficult to tell from the cell phone itself whether its information has been captured by an IMSI catcher, and there's no notification that encryption on the phone is no longer operating.

2. How do I know if law enforcement used a CSS in my case?
    a. Be on the lookout for search warrants referring to a "confidential informant" for a suspect's location or other obscure terms, including: digital analyzers, Triggerfish, Kingfish, Arrow-Head, Amberjack, Hailstorm, or WITT (FBI's "Wireless Intercept Tracking Team"). If police found your client at an unusual location, it may indicate CSS use. Also look for language that tracks the DOJ's model warrant application, which uses terms like: "target cell phone", "pen register" and "trap and trace."

3. How do I challenge them?
    a. File an MTS – most CSS use was without a warrant prior to the change in DOJ and DHS policy in September 2015: https://eff.org/CSSDOJ
    b. Review the scathing House Oversight Committee report here: https://eff.org/CSSHOGR
    c. Review the leading CSS cases:
        i. 7th Cir.: *US v. Damian Patrick* (842 F.3d 540 (2016)): Rejected MTS argument that CSS use required a warrant. Rehearing *en banc* denied. https://eff.org/CSSPatrick
        ii. SDNY: *US v. Raymond Lambis* (197 F.Supp.3d 606 (2016)): Granted MTS for warrantless use of CSS and rejected govt's attenuation and third party doctrine arguments. https://eff.org/CSSLambis
        iii. Court of Special Appeals of MD: *State of Maryland v. Kerron Andrews* (227 Md.App.350 (2015)): Granted MTS for warrantless CSS use, rejected TPD, and rejected pen register and trap & trace order as substitute for warrant. https://eff.org/CSSAndrews
        iv. ND IL: *Matter of the Application of the US* (2015): District Court order re: minimization of CSS use. https://eff.org/CSSNDIL

4. How do I learn more?
    a. Visit https://eff.org/CSSFAQ
    b. For more details on how CSS work, see the CSS manuals cited in the Intercept article: https://eff.org/CSSmanuals

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