Cell Site Simulators

Cell-site simulators ("CSS"), also commonly known as IMSI catchers or Stingrays, are devices that law enforcement uses to try to locate and identify suspects. CSSs take advantage of flaws in cellular communication technology (which are especially common in older technologies such as 2G) and masquerade as legitimate cell phone towers, potentially tricking all phones nearby into connecting to the device instead of the tower. These devices can log the unique identifying numbers of all mobile phones in a given area and pinpoint the location of a specific number in real time with much greater precision than cell site location information that comes from the phone company.

Areas of Concern:

- No transparency: US law enforcement, along with criminals and foreign spies, can quickly and easily deploy CSSs, with little risk of detection by the target. It is almost impossible to tell from the cell phone itself whether its information has been captured by an IMSI catcher. The same flaws in the cellular technologies — such as 2G and SS7 — that let law enforcement operate CSSs can also be used by foreign spies and criminals to spy on Americans with no chance of being detected.
- No consistent regulation/data protection/accountability: Very few states have laws on the books limiting law enforcement use of CSSs, allowing public access to the information collected and the period of storage, or mandating an account of CSS use.
- Interference Questions: Because CSSs can cause the target phone(s) to connect to the device rather than the cell tower, they can ***actively interfere*** in communications between targeted phones and towers, including 911 calls.
- Collateral Data Collection: Data logged by CSSs can reveal intensely personal information about *anyone* with a phone in the affected area, not just the target of the operation. There is no way for a phone to be configured to avoid connecting to a CSS. Also, some CSSs are reported to have the capability to intercept and log metadata, such as dialed phone numbers, as well as content, such as SMS messages and phone calls.

Past Congressional Action

- In December 2016, the House Oversight and Government Reform Committee investigated the use of CSSs and issued a bipartisan scathing report, criticizing the use of CSSs without uniform standards or policies.
- The FY2019 House Homeland Security Appropriations Report included a request for the Department to provide a briefing on the implementation and oversight of DHS Policy Directive 047-02, related to the use of cell-site simulators by the Department and its state and local partners.

Want more information? Please contact Legislative Analyst India McKinney at **india@eff.org**.