The Problem

The government is sidestepping the Fourth Amendment by engaging in warrantless location tracking of Americans using cell-site simulators, also known as “Stingrays.”

A Stingray (also called a cell-site simulator or an IMSI catcher) is an electronic surveillance device used by law enforcement officers to locate or identify potential criminal suspects by imitating cell towers, tricking nearby cell phones to connect to them. They collect critical personal data, including a phone’s GPS location, call history, and text messages. Stingrays can also intercept or block communications, including 911 calls, posing safety risks to local communities. Stingrays can collect this information — and are sometimes deployed without a warrant — from anybody carrying cell phones within their radius, regardless of whether they are suspected of a crime.

Law enforcement officers can use Stingrays to track the movement of individuals in real time across neighborhoods and even inside private homes. By moving the Stingray from place to place and gathering a wireless device’s signal from various locations, law enforcement can pinpoint a user’s location — sometimes to within six feet. There is currently no requirement to notify people when Stingrays access their phones. The only way for individuals to avoid Stingray tracking is to turn off their phones or not carry them.

Stingrays are especially dangerous because they collect sensitive location data on everyone in an area. By gathering this information en masse, Stingrays unavoidably cause collateral damage to privacy, scooping up location data of innocent bystanders as well as suspects. Deploying Stingrays in sensitive locations could expose intimate details of individuals’ lives, capturing information such as a full list of patients at a doctor’s office or rehab facility, participants at a protest or political rally, or worshipers at a religious ceremony.

Current federal, state, and local policies regulating Stingrays are confusing and inconsistent, opening the door to abuse and unconstrained, invasive surveillance by law enforcement. Congress must take action to end warrantless location tracking and uphold the constitutional prohibition on unlawful searches and seizures.

The Solution

The Cell-Site Simulator Warrant Act, introduced as S.2122 by Senators Ron Wyden (D-OR) and Steve Daines (R-MT) and as H.R. 4022 by Representatives Ted Lieu (D-CA) and Tom McClintock (R-CA), establishes a warrant requirement and creates clear legal standards for the use of cell-site simulators by any government agency.
What the bill does:

- **Establishes judicial review to guard against abuse:** The bill establishes a warrant requirement for federal, state, and local law enforcement agencies to use a cell-site simulator.
- **Supports less invasive methods whenever feasible:** The bill limits cell-site simulator use to situations when all other surveillance methods have or are likely to fail.
- **Ensures collateral damage to privacy is minimized:** The bill 1) mandates that data collected from bystanders’ cell phones be minimized, 2) requires that judges are informed of all potential negative consequences of cell-site simulators, including their ability to block emergency calls, and 3) compels judges to weigh government surveillance interests against risks to the community.
- **Sets penalties to prevent illegal monitoring:** The bill 1) institutes fines up to $250,000 for any agency that illegally operates a cell-site simulator, and 2) creates a private right of action for individuals who are illegally surveilled.
- **Supports emergency needs for rapid response:** The bill permits emergency use of cell-site simulators, allowing the government to get a court order after the fact.

Several states, including California, Washington, Virginia, Utah, and Illinois, have passed legislation requiring law enforcement agencies to obtain warrants before using Stingrays, and some state courts have held that warrantless use of these devices is unconstitutional.¹

This bill does not prohibit law enforcement from using Stingrays to find criminal suspects or otherwise protect the public’s safety. It simply requires that law enforcement obtain a warrant to use these devices and use them only as a tool of last resort, similar to existing wiretap rules.

*The Cell-Site Simulator Warrant Act has bipartisan support from lawmakers. A broad coalition of more than a dozen civil liberties groups have endorsed the bill, including Americans for Prosperity, Brennan Center for Justice, Center for Democracy and Technology, Demand Progress, Electronic Frontier Foundation, Electronic Privacy Information Center, FreedomWorks, Free Press Action, Project for Privacy and Surveillance Accountability, Project On Government Oversight, Public Citizen, Public Knowledge, and Restore the Fourth.*

The Cell-Site Simulator Warrant Act would protect Americans from unfettered surveillance by instituting common sense limitations on Stingray usage. Law enforcement should not be able to abuse Stingrays and track or collect personal information from innocent bystanders without constitutional safeguards in place.

For more information, please contact Jake Laperruque, Senior Policy Counsel of the Constitution Project at the Project On Government Oversight (POGO), at jlaperruque@pogo.org.