The Cell Site Simulator Warrant Act of 2021

This bill protects Americans from unconstitutional surveillance of their phones by government agencies and other entities using cell site simulators (CSS), a surveillance technology commonly known as Stingrays.

Cell site simulators indiscriminately send tracking signals through walls and into homes, cars, pockets and purses to identify all phones in an area and track particular devices. CSS can also intercept calls, texts and even help hack into phones. While there are legitimate government uses for CSS, a confusing patchwork of state and federal policies has led to abuses and failed to protect Americans' constitutional rights against unfettered surveillance.

For years, federal, state and local law enforcement agencies hid their use of CSS from courts, legislators, defense lawyers and the general public. In 2015, the Justice and Homeland Security departments adopted a policy requiring probable cause warrants and other basic conditions for their use. However, this policy could be reversed at any time.

There are a number of outstanding problems with CSS use: current federal policies do not apply to the intelligence community or to state and local government agencies (which continue to use CSS without warrants), courts are still not being told that CSS can jam some 9-1-1 calls, federal law enforcement agencies can still use evidence obtained in violation of these policies and Congress and the public remain in the dark about how frequently CSS are being used.

This bill allows government agencies to continue using CSS when appropriate, with supervision by the courts, and provides clear rules and legal certainty for when and how CSS can be deployed. It also requires full transparency from government agencies to ensure the public and Congress understand the impact of this dragnet surveillance technology.

The Cell Site Simulator Warrant Act:

- Establishes a probable cause warrant requirement for federal, state & local law enforcement agencies to use a CSS. Like wiretaps, CSS must be a tool of last resort, used when other methods have or are likely to fail.
- Permits emergency use, enabling the government to get a court order after the fact.
- Requires that judges be informed about all potential side effects, including jamming 9-1-1 calls, as determined by an independent lab, and requires judges to weigh the government’s surveillance interests against the impact to the community & public safety.
- Requires that data collected using a CSS from bystanders’ devices be minimized.
- Creates similar rules for intelligence agencies’ use of CSS authorized by the Foreign Intelligence Surveillance Court, including targeting of Americans abroad.
- Provides for fines up to $250,000 for entities that illegally operate a CSS, but with an exception for use of a CSS by those engaged in good-faith research or teaching.
- Provides for a private right of action by individuals who were illegally surveilled.
- Requires annual Inspector General reports on federal agencies’ use of CSS.