New federal requirements on cellphone surveillance

3 September 2015, byEric Tucker

This undated handout photo provided by the U.S. Patent and Trademark Office shows the StingRay II, manufactured by Harris Corporation, of Melbourne, Fla., a cellular site simulator used for surveillance purposes. Federal law enforcement officials will be routinely required to get a search warrant before using secretive and intrusive cellphone-tracking technology under a new Justice Department policy announced Sept. 3, 2015. The seven-page policy, the first of its kind, is designed to create a uniform legal standard for federal law enforcement agencies using equipment known as cell-site simulators. (AP Photo/U.S. Patent and Trademark Office)

Federal law enforcement officials will be routinely required to get a search warrant before using secretive and intrusive cellphone-tracking technology under a new Justice Department policy announced Thursday.

The policy represents the first effort to create a uniform legal standard for federal authorities using equipment known as cell-site simulators, which tracks cellphones used by suspects.

It comes amid concerns from privacy groups and lawmakers that the technology, which is now widely used by local police departments, is infringing on privacy rights and is being used without proper accountability.

"The policy is really designed to address our practices, and to really try to promote transparency and consistency and accountability—all while being mindful of the public's privacy interest," Deputy Attorney General Sally Yates told reporters in announcing the policy change.

The policy applies only to federal agencies within the Justice Department and not, as some privacy advocates had hoped, to state and local law enforcement whose use of the equipment has stirred particular concern and scrutiny from local judges.

The technology—also known as a Stingray, a suitcase-sized device—can sweep up basic cellphone data from a neighborhood by tricking phones in the area to believe that it's a cell tower, allowing it to identify unique subscriber numbers. The data is then transmitted to the police, helping them determine the location of a phone without the user even making a call or sending a text message.

The equipment used by the Justice Department does not collect the content of communications.

Even as federal law enforcement officials tout the technology as a vital tool to catch fugitives and kidnapping suspects, privacy groups have raised alarms about the secrecy surrounding its use and the collection of cellphone information of innocent bystanders who happen to be in a particular neighborhood or location.

In creating the new policy the Justice Department was mindful of those concerns and also sought to address inconsistent practices among different federal agencies and offices, Yates said.

"We understand that people have a concern about their private information, and particularly folks who are not the subjects or targets of investigations," Yates said.

The new policy requires a warrant in most cases, except for emergencies like an immediate national security threat, as well as unspecified "exceptional circumstances." The warrant applications are to set out how the technology will be used.

In addition, authorities will be required to delete data that's been collected once they have the information they need, and are expected to provide training to employees.

The policy could act as a blueprint for state and local law enforcement agencies in developing their own regulations. But it's unclear how broad an impact Thursday's announcement will have, since it does not directly affect local police agencies unless they're working alongside federal authorities on a case or relying on their assistance.

Use of the technology has spread widely among local police departments, who have been largely mum about their use of the technology and hesitant to disclose details—often withholding materials or heavily censoring documents that they do provide.

Local departments have faced scrutiny from judges about how they deploy the equipment, though agencies have often insisted that non-disclosure agreements with the FBI limit what they can say.

The FBI has said that while specific capabilities of the equipment are considered sensitive, it did not intend for the agreements to prevent the police from disclosing to a court that the equipment was used in a particular case. Yates said she expected the FBI to revise any such agreements to be more transparent.

The American Civil Liberties Union called the policy a good first step, but expressed disappointment that it did not cover federal agencies outside the Justice Department or local police who use federal funds to purchase the surveillance equipment. It called on the Justice Department to close remaining loopholes, such as the one allowing for warrantless surveillance under undefined "exceptional circumstances."

"After decades of secrecy in which the government hid this surveillance technology from courts, defense lawyers, and the American public, we are happy to see that the Justice Department is now willing to openly discuss its policies," ACLU lawyer Nathan Freed Wessler said in a statement.

Nate Cardozo, a staff attorney with the Electronic Frontier Foundation, a privacy group, praised the policy as an important step, though he said he suspected Justice Department attorneys saw "the writing on the wall" and recognized that judges would increasingly begin requiring warrants.

Though the policy does not require local police to follow the lead of federal agencies, "this is going to let the air out of state law enforcement's argument that a warrant shouldn't be required."

"We think that given the power of cell-site simulators and the sort of information that they can collect—not just from the target but from every innocent cellphone user in the area—a warrant based on probable cause is required by the Fourth Amendment," Cardozo said.