Department of Justice

STATEMENT OF
ELANA TYRANGIEL
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

BEFORE THE
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U. S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"EXAMINING LAW ENFORCEMENT USE OF
CELL PHONE TRACKING DEVICES"

PRESENTED
OCTOBER 21, 2015

Statement of
Elana Tyrangiel
Principal Deputy Assistant Attorney General

Before the
Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives

At a Hearing Entitled
"Examining Law Enforcement Use of Cell Phone Tracking Devices"

October 21, 2015

Chairman Hurd, Ranking Member Kelly, and Members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Justice regarding the Department's Policy Guidance on the Use of Cell-Site Simulator Technology. This topic is important to the Department, as cell site simulators fulfill critical operational needs for all of the Department's law enforcement agencies. The technology has been used, for example, to help locate kidnapped children, to assist in apprehending dangerous and violent fugitives, and to aid in complicated investigations into drug trafficking.

As with all evolving technologies, the Department must continue to assess the use of cell-site simulators to ensure that its policies and practices enable law enforcement to carry out its public safety objectives while continuing to uphold the Department's commitments to individuals' privacy and civil liberties. We are pleased to engage with the Subcommittee in a discussion about the Department's policy.

Cell-site simulators are devices that can help law enforcement agents locate a known cellular device, or identify an unknown device used by a known suspect. The technology works by collecting limited signaling information from cellular devices in the simulator's vicinity, providing the relative signal strength and general direction of a subject cellular telephone. Cell-site simulators are one tool among many traditional law enforcement techniques, and the Department deploys them only in the fraction of cases in which the technology is best suited to achieve specific public safety objectives.

As you know, the Department recently issued a new policy governing its use of cell-site simulators in domestic criminal investigations. The policy is intended to enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections.

The policy provides Department components with standard guidance for the use of cell-site simulators and establishes management controls for the use of the technology. These include training and supervisory protocols, data handling requirements, and auditing and tracking measures. The Department intends these requirements to ensure that our use of this technology is well-managed, consistent across the Department, and respectful of individuals' privacy and civil liberties. We hope and believe the policy properly accomplishes these objectives, while addressing any confusion or misperception surrounding the Department's use of cell-site simulators.

* * *

The Department's policy covers all use of cell-site simulators by Department personnel in support of domestic criminal investigations, including when they are working in cooperation with state or local law enforcement agencies. Cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication.

The policy has four basic elements:

First, the policy establishes a variety of management controls and training requirements. Specifically, all operators of cell-site simulators must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert. Each agency will also identify training protocols. Those protocols must include training on privacy and civil liberties and must be developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

In addition, agencies must designate an executive-level point of contact responsible for implementing the policy in each jurisdiction. Before the technology is deployed, its use must be approved by an appropriate individual who has obtained the grade of a first-level supervisor. Emergency use must be approved by a second-level supervisor. And, to the extent these devices are occasionally used on an aircraft, that use must be approved by an executive-level supervisor or by a branch or unit chief at agency headquarters. These measures will help to ensure that only trained personnel use cell-site simulators and that the technology is used in accordance with the requirements of the policy.

Second, the policy adopts a consistent legal standard for the Department's use of cell-site simulators in domestic criminal investigations. While the Department has, in the past, obtained appropriate legal authorization to use cell-site simulators pursuant to orders under the Pen Register Statute, law enforcement agents now generally must obtain a search warrant supported by probable cause before using such a device. The policy recognizes two limited exceptions to the warrant requirement:

- When the Fourth Amendment does not require a warrant due to exigent circumstances, this policy does not require a warrant either. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement

are so compelling that they render a warrantless search objectively reasonable (e.g., the need to protect human life or the hot pursuit of a fleeing felon). Agents, however, still must comply with the provisions of the Pen Register Statute, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. When emergency pen register authority is sought, approval must be obtained from a Deputy Assistant Attorney General in the Department's Criminal Division.

- There also may be very limited circumstances in which the Fourth Amendment does not require a warrant (for example, because the cell-site simulator will be used in a place where there is no expectation of privacy) and circumstances on the ground make obtaining a warrant impracticable. To use this exception, an agent first would need to seek approval from executive-level personnel from his law enforcement agency, approval from the relevant U.S. Attorney, *and* approval from a Deputy Assistant Attorney General in the Criminal Division. We expect this exception to be used only in very limited cases. In those cases, an agent still would need to obtain a court order under the Pen Register Statute as described above. The Criminal Division will track the number of times the use of a cell-site simulator is approved under this provision, as well as the circumstances underlying each such use.

Third, the policy enhances transparency to courts. As always, candor to courts is of utmost importance. The policy requires law enforcement agents to consult with prosecutors, and to include sufficient information in their warrant applications to ensure that courts understand that a cell-site simulator may be used. Specifically, the policy requires that the application or supporting affidavit include a general description of the technique to be employed, a statement that the target cellular device and other devices in the area might experience a temporary disruption of service, and an explanation of how law enforcement will treat the data the cell-site simulator obtains.

Fourth, in order to ensure that individuals' privacy interests are protected, the policy establishes consistent requirements for handling the data obtained by cell-site simulators. As used by the Department – and as now required by the policy – the devices do not, as noted above, obtain the contents of any communication or any data from the phone itself, whether emails, texts, or contact lists. Nor do they obtain subscriber account information such as name, address, or telephone number. But even for the limited types of information simulators do collect, the policy establishes requirements for deletion.

When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. In instances when it is used to identify an unknown cellular device, all data must be deleted as soon as the target device is identified, and in any event no less than once every 30 days. Agencies will be required to implement an auditing program to ensure adherence to these deletion requirements.

* * *

In conclusion, I would like to reemphasize that cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives: this technology saves lives, enabling law enforcement to rescue endangered victims and apprehend dangerous criminals. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. Our policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

The Department of Justice stands ready to work with the Subcommittee as it addresses the use of these valuable technologies, and we appreciate the opportunity to discuss this issue with you.