OCTOBER 21, 2015

EXAMINING LAW ENFORCEMENT USE OF CELL PHONE TRACKING DEVICES

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

Rep. Will Hurd (R-TX) *[no pdf available, see 1:16:35 of webcast]*
Chairman, Subcommittee on Information Technology

Rep. Ted Lieu (D-CA) *[view pdf]*
Ranking Member, Subcommittee on Information Technology

WITNESSES:

Ms. Elana Tyrangiel *[view pdf]*
Principal Deputy Assistant Attorney General, Office of Legal Policy
U.S. Department of Justice

Mr. Seth Stodder *[view pdf]*
Assistant Secretary, Threat Prevention and Security Policy
U.S. Department of Homeland Security

AVAILABLE WEBCAST(S):*

Full Hearing: *https://youtu.be/tgfmIH1x7ro?t=4595*

COMPILED FROM:

https://oversight.house.gov/hearing/examining-law-enforcement-use-of-cell-phone-tracking-devices/

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

OPENING STATEMENT BY RANKING MEMBER LIEU AT SUBCOMMITTEE ON INFORMATION TECH. HEARING ON LAW ENFORCEMENT CELL PHONE USE

October 21, 2015 | Press Release

FOR IMMEDIATE RELEASE

Opening Statement:
Ranking Member Ted Lieu (CA-33)
Subcommittee on Information Technology
Hearing on Examining Law Enforcement Use of Cell Phone Tracking Devices

"Thank you Mr. Chairman for holding today's hearing on federal law enforcement policies regarding the use of cell-site simulators in criminal investigations.

"In September of this year, the Department of Justice (DOJ) announced its new policy on cell-site simulators, commonly known as Stingrays, aimed at enhancing privacy protections and establishing a consistent legal standard for obtaining authority to use a simulator. Federal law enforcement will now be required to obtain a search warrant supported by probable cause, consistent with the protections in the Fourth Amendment.

"Earlier this week, the Department of Homeland Security (DHS) announced its department-wide policy, which similarly establishes a higher and more consistent legal standard of a search warrant requirement.

"At the time of the DOJ announcement, I released a statement calling the policy change a welcome first step and suggested we needed hearings in this committee on the matter. As new technologies empower law enforcement with unique capabilities, stringent rules are needed to safeguard against abuse of our civil liberties.

"The search warrant requirement establishes a consistent legal standard for federal authorities and will allow increased oversight of the use of cell-site simulators. Even in those limited circumstances when a warrant is not required for use of a cell-site simulator, there are controls in place to help ensure that the exceptions are not abused. I look forward to the witnesses today providing more details on those exceptions and the safeguards put in place.

"These federal policies are needed to safeguard against abuse of individuals' privacy and civil liberties. The data collection and retention practices in the new policy are intended to enhance privacy protections—and they do so without undermining a law enforcement tool.

"I believe that these policy changes by DOJ and DHS, while a good step forward, could and should go further. As the ACLU has noted, the policy guidance contains significant gaps—including overbroad exceptions to the warrant requirement, lack of notice to individuals impacted by Stingrays, and lack of transparency in reporting. Most notably, these agency policy changes do not meaningfully restrict state and local officials who use Stingrays in the majority of U.S. states that do not regulate them.

"I hope that state and local law enforcement agencies follow the lead of these federal policies and implement stringent privacy protections and legal standards.

"In my home state of California, Governor Jerry Brown recently signed into law the California Electronic Communications Privacy Act, joining nine other states with laws that require state law enforcement to get a warrant before using cell-site simulators during criminal investigations. The California law also requires a warrant before law enforcement can search meta-data or other electronic communications.

"Finally, I note that the federal policy changes are reversible and they do not apply to all federal agencies. As we have seen in the past, not all administrations or agencies have had respect for our civil liberties. We should follow the lead of multiple states, including my own state, and enshrine these policies into law across all agencies to make clear that the Fourth Amendment needs to be respected and persons have the right to be free from unreasonable search and seizure by the government.

"I would like to commend Chairman Chaffetz, Ranking Member Cummings, Subcommittee on Information Technology Chairman Hurd and Ranking Member Kelly for their oversight work related to cell-site simulators. In April of this year, the Committee sent letters to DOJ and DHS requesting information and briefings on the policies surrounding cell-site simulators, which increased the Committee's visibility into the policies governing the use of this law enforcement tool.

"I would also like to thank the agencies appearing today for taking the time to testify about these important policy changes and their impacts on our civil liberties. As with other policies regulating government use of technology for law enforcement and surveillance purposes, it is vital that we closely examine the rules to ensure we fully understand what is permitted.

"I look forward to reviewing policies related to the collection of geolocation and other electronic data to ensure that law enforcement tools are deployed consistently and with respect for privacy and civil liberties."

Thank you, Mr. Chairman."

###

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.

Elana Tyrangiel Bio

Elana Tyrangiel is the Principal Deputy Assistant Attorney General and head of the Office of Legal Policy. She joined OLP in 2009, and has served in a number of roles since then, including Chief of Staff, Deputy Assistant Attorney General and Principal Deputy.

Immediately prior to joining OLP, Ms. Tyrangiel worked in the Office of the White House Counsel. From 2000-2009, she was an Assistant United States Attorney in the U.S. Attorney's Office for the District of Columbia, where she handled a broad range of matters and served as Deputy Chief of the Sex Offense and Domestic Violence section. Before joining the U.S. Attorney's Office, Ms. Tyrangiel served as a policy counsel at the National Partnership for Women and Families.

Ms. Tyrangiel holds an A.B. in political science, magna cum laude, from Brown University and a J.D., magna cum laude, from the University of Michigan Law School, where she served as Managing Editor of the Michigan Law Review. After graduation, she clerked for the Honorable M. Blane Michael on the U.S. Court of Appeals for the Fourth Circuit.

Seth M. Stodder

Assistant Secretary, Threat Prevention and Security Policy

Office of Policy

U.S. Department of Homeland Security

testifying before the

Committee on Oversight and Government Reform

Subcommittee on Information Technology

United States House

"Examining Law Enforcement Use of Cell Phone Tracking Devices"

on

Wednesday, October 21, 2015
2:00 p.m.
2154 House Office Building
Washington DC 20515

Prepared Testimony

Seth M. Stodder
Assistant Secretary for Threat Prevention and Security Policy
Office of Policy
U.S. Department of Homeland Security

United States House Committee on Oversight and Government Reform
Subcommittee on Information Technology

October 21, 2015

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee, thank you for the opportunity to be here today to talk with you about how the Department of Homeland Security ("DHS" or the "Department") uses cell-site simulator technology. I will discuss this important law enforcement tool in the context of how cell-site simulators work and how DHS uses cell-site simulators. I will also provide an overview of the new DHS policy on the use of cell-site simulator technology.

Cell-site simulators, also known as International Mobile Subscriber Identity or "IMSI" catchers, are invaluable law enforcement tools that enable law enforcement personnel to identify and generally locate the mobile devices of both the subjects of an active criminal investigation and their victims. Cell-site simulators work by collecting limited signaling information from cellular devices in the cell-site simulator's vicinity, providing the relative signal strength and general direction of a subject cellular device. It is a tool that, when used in conjunction with other investigative efforts such as physical surveillance, can and has directly led to law enforcement saving lives and removing dangerous criminals from the street.

Before I describe how DHS uses this technology, I would like to dispel some common misconceptions about this technology and what it can and cannot do. Cell-site simulation technology allows law enforcement personnel to emit signals similar to a cell phone tower, resulting in nearby mobile phones and other wireless communication devices connecting to the simulated tower instead of the phone carrier's established tower. The simulator is then able to register the mobile device's unique identification number and identify an approximate location of the device. This technology does not provide the subscriber's account information; meaning no personal information, such as the account holder's name, address, or telephone number, can be detected by this device. Additionally, cell-site simulators provide only the relative signal strength and general direction of a subject's cellular telephone; the technology does not function as a GPS locator and cannot collect GPS location information from mobile devices. Cell-site simulators used by DHS do not collect the contents of any communication, including data

contained on the phone itself, e.g., call content, transaction data, emails, text messages, contact lists, or images.

Within DHS, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the U.S. Secret Service (USSS) use this technology in the furtherance of their ongoing criminal investigations. HSI personnel deploy the devices during critical stages of investigations of a wide range of criminal activity, such as narcotics trafficking, human trafficking, and kidnapping, and to rescue the underage victims of child exploitation and prostitution rings. USSS personnel use this technology in support of its protective and investigative missions, and in its joint law enforcement operations with state and local law enforcement. By helping to locate a cellular device known to be used by a particular subject or to determine what mobile device a subject is carrying, this technology can greatly advance an investigation by enabling law enforcement agents to locate and arrest subjects who are otherwise difficult to find.

The new DHS policy regarding the use of cell-site simulator technology ensures that management controls and accountability processes are in place; defines the legal requirements and procedures for using the technology; articulates what is to be included in an application to the court seeking authorization to use the technology; defines strict guidelines on data collection and disposal; and ensures training and oversight.

Management controls and accountability are cornerstones of compliance for any policy. The DHS-wide policy requires that each Component that uses cell-site simulators develop operational policy or procedures to govern the use of the technology that is consistent with the overarching DHS policy, and to do so in coordination with the DHS Office of the General Counsel, Office of Policy, Privacy Office, and Office for Civil Rights and Civil Liberties. The policy also requires that each Component designate an executive point of contact, at the Component's headquarters level, who will have overall responsibility for implementation of this policy, and for promoting compliance with its provisions. The policy articulates supervisory approval requirements for deployment of the technology. Additionally, the policy requires that cell-site simulators be operated only by trained personnel who have been authorized by their Component to use the technology and whose training has been administered by a qualified Component expert. This includes training on privacy and civil liberties protections.

The Department's cell-site simulator policy requires that DHS agents or operators, prior to using a cell-site simulator, generally obtain a search warrant supported by probable cause. The DHS policy does provide for two exceptions to the warrant requirement consistent with applicable law. The first exception is in the case of "exigent circumstances" in which law enforcement needs are so compelling that they render a warrantless search objectively reasonable under the Fourth Amendment. Under the exigent circumstances exception, agents must still comply with the Pen Register Statute and with the policy's requirement to obtain the approval of a supervisor. The second

exception is in cases of "exceptional circumstances" in which the law does not require a search warrant and obtaining a warrant would be impracticable. For example, in furtherance of protective duties, USSS may encounter exceptional circumstances that would make obtaining a search warrant impracticable. In these limited circumstances, USSS agents or operators must first obtain approval from executive-level personnel at USSS headquarters and the relevant U.S. Attorney, who will coordinate approval within the DOJ. DHS expects cases of exigent and exceptional circumstances to be limited.

When making any application to a court for the use of cell-site simulator technology, the Department's policy requires that DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. DHS law enforcement personnel must consult with prosecutors in advance of using a cell-site simulator, to include state and local prosecutors when DHS is engaged with state and local law enforcement for non-federal cases. DHS works in close partnership with state and local law enforcement, and the Department provides technological assistance under a variety of circumstances. The DHS policy applies to all instances in which Department Components use cell-site simulators in support of other Federal agencies and/or state and local law enforcement agencies.

The DHS policy also requires that applications for the use of cell-site simulators inform the court that cellular devices in the area of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. In the overwhelming majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. To dispel another misconception – law enforcement use of cell-site simulator technology will not disconnect end users from calls in progress.

As previously stated, the scope of identification information collected when using cell-site simulator technology is limited to the phone manufacturer's or service provider's unique identifier (IMSI) for the device. Once these identifiers are obtained, law enforcement agents must undertake additional legal process (such as serving a subpoena on a service provider) to obtain subscriber information, or to initiate a wiretap pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in order to monitor a suspect's wire or electronic communications occurring over said device. Nevertheless, the DHS policy includes strict data collection and disposal standards to ensure that DHS law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals. Specifically, the Department's policy for the use of cell-site simulators requires that immediately following the completion of a mission, the operator of a cell-site simulator must delete all data collected. For example, when the equipment is used to locate a known cellular phone used by a suspect, data is deleted as soon as the target is located; when the equipment is used to identify a particular device used by a suspect, data is deleted as soon as the suspect device is identified, and no less than once every 30 days. To further safeguard

privacy, the policy also requires that prior to deploying equipment for another mission, the operator verifies that the equipment has been cleared of any previous operational data.

The Department's policy also requires that DHS Components implement an auditing program to ensure that the data is deleted in the manner described above. To the extent feasible, this auditing program includes hardware and software controls, for example through an equipment sign-in process that will include operator badge number and an affirmative acknowledgement by the operator that he or she is authorized by the Department to collect and view data.

DHS has been and remains committed to operating this equipment in a responsible manner. The recent implementation of this policy was meant to bring all DHS policies under a unified document and uniform DHS policy standard. The Department has always been committed to using cell-site simulators in a manner that is consistent with, and protects, the privacy rights of individuals.

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee, thank you for the opportunity to testify today. I look forward to answering your questions.

Seth M. M. Stodder

Assistant Secretary for Threat Prevention and Security Policy
Office of Policy
U.S. Department of Homeland Security

Seth Stodder was appointed by President Obama to serve as Assistant Secretary of Homeland Security for Threat Prevention and Security Policy, within the Office of Policy, in June 2015. Assistant Secretary Stodder leads a team advising Secretary Johnson and senior DHS leadership on a wide variety of issues relating to security threats to the U.S. homeland, and on how to address them while preserving the civil liberties and privacy rights we all cherish. Among other things, Assistant Secretary Stodder oversees DHS policy development on the screening of people moving through the global and domestic travel and transportation systems and across U.S. borders, visa policy, law enforcement policy, among many other issues.

A longtime expert in national and homeland security law and policy, Assistant Secretary Stodder also teaches Counterterrorism, Civil Liberties, and Privacy Law at the University of Southern California Law School. Prior to his appointment at DHS, Assistant Secretary Stodder was a partner in the law firm of Obagi & Stodder LLP, practicing civil and criminal trial and appellate litigation and immigration law, and also President of Palindrome Strategies, LLC., a consulting firm advising on a variety of issues relating to homeland security. He also served as a Senior Associate with the Center for Strategic and International Studies, a Senior Fellow at the George Washington University Homeland Security Policy Institute, and was closely involved in the development of the first Quadrennial Homeland Security Review and the National Strategy for Global Supply Chain Security. Earlier in his career, Assistant Secretary Stodder was a lawyer at Gibson Dunn & Crutcher LLP, as well as Akin Gump Strauss Hauer & Feld LLP, practicing appellate and constitutional law.

This is Assistant Secretary Stodder's second tour of duty at DHS. Earlier in his career, Assistant Secretary Stodder served in the Bush Administration as Director of Policy and Planning for U.S. Customs and Border Protection, and Counselor/Senior Policy Advisor for CBP Commissioner Robert C. Bonner. In that role, he was closely involved in the development and implementation of the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), and the pre-departure APIS/PNR and "24 Hour Rule" information collection requirements, among a variety of other initiatives focused not only on securing the borders of the United States, but also on facilitating the secure flow of lawful travel and trade across our borders and throughout the global economy.

Assistant Secretary Stodder is a member of the U.S. Supreme Court and California bars, has a J.D. from the University of Southern California Law School, and a B.A. from Haverford College. He is from Los Angeles, California.