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.