EXAMINING LAW ENFORCEMENT USE OF CELL PHONE TRACKING DEVICES

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

OCTOBER 21, 2015

Serial No. 114–69

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

21–433 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
TROY D. STOCK, *IT Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

EXAMINING LAW ENFORCEMENT USE OF CELL PHONE TRACKING DEVICES

Wednesday, October 21, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:52 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Walker, Blum, Chaffetz, Connolly, and Lieu.

Mr. HURD. The Subcommittee on Information Technology will come to order. Without objection, the chair is authorized to declare a recess at any time.

Today's hearing has a narrow but very important focus, Federal law enforcement agencies' use of cell site simulator devices, otherwise known as IMSI-catchers or stingrays.

Today's hearing also touches on fundamental questions of privacy that we have grappled with since the founding of this country. When and how, can or should the government use technology to locate people? What notice or information, if any, must people be given about the technology used to locate them? To what extent must the government take into account the rights of innocent people who may be swept into a law enforcement dragnet? And how can we protect our civil liberties and defend the homeland at the same time? These are essential questions.

Today's hearing won't give us a definitive answer to all these questions, but I hope that representatives from DHS, and DOJ, will be able to shed light on some of them and that this conversation will begin to reveal answers on others.

Tracking a person's movements for an extended period of time can reveal almost anything and everything about them. What establishments they frequent, whether or not they are church goers, who their friends are, and their day-to-day hobbies. Geolocation is more than a record of where you are or were, it's a window into who we are.

The Founders considered the ability of average citizens to keep things private from the government of such importance, that they built it into the Constitution. Thanks to the Fourth Amendment, we have the right to be secure in our persons, houses, papers, and effects against unreasonable searches and seizures. Simply put, unless, and until law enforcement can convince a judge to issue a probable cause warrant, they don't get to disrupt that security.

Cell site simulator devices work by impersonating a cell phone tower and forcing all mobile phones within range into connecting with the device. Once a stingray connects with a cellular phone, it is able to identify that cell phone's unique identifying number and to identify the approximate location of the phone.

There are also collateral consequences for the owners of non-targeted phones in the area. While searching for the target phone, the device will also make contact with other non-target cell phones that happen to be within range of the simulator device, even if those phones' owners are not suspected of criminal wrongdoing.

After considerable congressional, public, and media interest, both DOJ and DHS decided to create agency-wide policies governing the use of these devices. While there may be some lingering concerns about the substance of the policies, which we will discuss here today, in balance the policies are a big step forward for DOJ and DHS, and a win for transparency and privacy advocates everywhere, as well as this is a win for the American people. What does worry me, however, is that it took the extra scrutiny to convince DOJ and DHS to make these changes, and I remain troubled that Federal law enforcement is still not embracing transparency the way they need to in 2015.

I know, and I think, better than most, the need for the government to keep certain things secret from the public. Secrets in the wrong hands get people killed, but secrecy is a double-edged sword. Right now only about one in four Americans trust the Federal Government. If you do not have the trust of the people you are fighting for and with, you have nothing.

I commend DOJ and DHS for their efforts here, but this can't be the exception. Law enforcement must continually strive to appropriately balance privacy and security issues in the digital age and they must continue to be transparent with Congress, and the public, about the choices and trade-offs we face.

I hope today's hearing is a small step in beginning to bridge the gulf that has developed between our Nation's policies and the citizens they are meant to protect.

Our witnesses today are Elana Tyrangiel, the Principal Deputy Assistant Attorney General for Office of Legal Policy at the U.S. Department of Justice, and Seth Stodder, the Assistant Secretary of Threat Prevention and Security Policy at the U.S. Department of Homeland Security. I thank the witnesses for being here today and look forward to their testimony.

And now it's a pleasure to recognize the gentleman from California, Mr. Lieu, for 5 minutes for your opening statement.

Mr. LIEU. Thank you, Chairman Hurd, for holding today's hearing to examine law enforcement's use of cell phone tracking devices.

In September of this year, the Department of Justice 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. Most Federal law enforcement will now be required to obtain a search warrant supported by probably cause, consistent with the protections of the Fourth Amendment.

Earlier this week the Department of Homeland Security 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 need committee hearings on this issue, and I am pleased Chairman Hurd is holding this hearing today.

As new technology empowered 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 those limited circumstances when a warrant is not required for use of such a cell site simulator, there are controls in place that help ensure that the exceptions are not abused. I look forward to the witnesses today providing more details on what those exceptions are and the safeguards that are put in place.

These further policies are needed to guard against abuse of individuals' privacy and civil liberties. Their data collection retention practices, and new policy are intended to enhance privacy protections, and hopefully 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 warrant requirement, lack of notice to individuals impacted by stingrays, and lack of transparency reporting. These agency policy changes also do not meaningfully restrict State and local officials who use stingrays and 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, for example, 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. The California law also requires a warrant before law enforcement can search metadata or other electronic communications.

I also note that the Federal policy changes discussed today here 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 the Fourth Amendment or our civil liberties. We should follow the lead of multiple States, including my own, 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 Chair Hurd, and Ranking Member Kelly, for the 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 policies surrounding cell site simula-

tors, which increased the committee's visibility into the policies governing the use of this law enforcement tool.

I also want to thank the agencies appearing today for taking the time to testify about these important policy changes, and thank the witnesses especially for being here.

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 being employed consistently and with respect for privacy and civil liberties.

And I yield back.

Mr. HURD. Thank you, Congressman Lieu.

Mr. HURD. And thank you and Ranking Member Kelly.

Mr. LIEU. Sure.

Mr. HURD. I yield back.

Mr. LIEU. One more thing before I conclude. I would like to enter the ACLU letter for the record, if that's okay.

Mr. HURD. So moved.

Mr. LIEU. Great. Thank you.

Mr. HURD. I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

Mr. HURD. And now we will recognize our panel of witnesses. I'm pleased to welcome Ms. Elana Tyrangiel, Principal Deputy Assistant Attorney General at the Office of Legal Policy at the Department of Justice. Thanks for being here. And, again, Mr. Seth Stodder, Assistant Secretary of Threat Prevention and Security Policy at the U.S. Department of Homeland Security. Welcome to you both.

And pursuant to committee rules, all witnesses will be sworn in before they testify. So please rise and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Please be seated.

Let the record reflect that the witnesses answered in the affirmative.

In order to allow time for discussion, please limit you all's testimony for 5 minutes, and your entire written statement will be made part of the record.

Ms. Tyrangiel, we will start with you. You are recognized now for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF ELANA TYRANGIEL

Ms. TYRANGIEL. Chairman Hurd, Ranking Member Lieu, and members of the subcommittee, thank you for inviting me to testify on behalf of the Department of Justice regarding the Department's policy guidance on the use of cell site simulator technology. We appreciate the opportunity to engage with the subcommittee on this important topic.

Cell site simulators are critical tools that play an essential role in the Department's law enforcement and public safety missions. The Department has deployed this technology, for example, in efforts to locate and recover kidnapping victims, in operations to apprehend dangerous and violent fugitives, and in complex drug trafficking investigations. The Department uses cell site simulators only in the fraction of cases in which the tool is the most effective means of achieving a particular public safety objective, and as with any law enforcement capability, Department personnel must use cell site simulators consistent with constitutional and statutory requirements.

As you know, in September the Department announced a new policy governing its use of cell site simulators. The policy applies Department-wide, establishing common principles for the use of cell site simulators in support of criminal investigations in the United States. It applies when Department personnel are working in cooperation with State and local law enforcement and it makes clear that cell site simulators may not be used to collect the content of any communication.

The policy seeks to accomplish four basic objectives: first, to improve training and supervision, second, to establish a higher and more consistent legal standard, third, to enhance transparency and accountability, and finally, to increase privacy protections. I'd like to briefly discuss each of these.

First, the policy sets forth a number of measures to ensure that law enforcement officers using cell site simulators are trained and supervised appropriately. Each law enforcement agency must establish training protocols, which must include training on privacy and civil liberties. Each agency must also name an executive level point of contact, who will be responsible for ensuring implementation of, and compliance with, the policy in each jurisdiction. Finally, any use of a cell site simulator must be approved in advance by appropriate personnel. The required level of seniority for the approval depends on the type of use involved.

Second, the policy generally requires law enforcement agents to obtain a search warrant supported by probable cause before using a cell site simulator. There are two limited exceptions to the warrant requirement. The first is an exigent circumstances, a well established exception under Fourth Amendment law, where the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. Even in these circumstances, agents still must comply with the Pen Register statute. The second limited exception is for cases in which the Fourth Amendment does not require a warrant, and circumstances make obtaining a search warrant impracticable. Again, in these circumstances agents still would need to comply with the Pen Register statute.

Third, the policy enhances transparency to courts by requiring law enforcement agents to make clear in their warrant applications that a cell site simulator may be used. Finally, the policy protects individuals' privacy interests by establishing consistent practices for handling the data obtained by these devices.

As I have noted, the policy prohibits the use of cell site simulators to obtain the contents of any communication, nor do the de-

vices obtain subscriber information. Even so, the policy establishes deletion requirements for the types of information that they do collect. Auditing programs in each agency will ensure that these requirements are followed.

In sum, cell site simulators offer critical support of the Department's public safety and law enforcement missions, but as with other capabilities, the Department is committed to using the technology in a manner that is consistent with the Constitution and all other legal authorities while respecting individuals' privacy and civil liberties. We hope and believe the policy properly accomplishes these objectives while clearing up any misperceptions.

The Department of Justice appreciates the opportunity to discuss our policy with the committee, and I look forward to your questions here today.

Mr. HURD. Thank you.

[Prepared statement of Ms. Tyrangiel follows:]

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.

Mr. HURD. Mr. Stodder, you are recognized for 5 minutes.

STATEMENT OF SETH STODDER

Mr. STODDER. Thank you. Chairman Hurd, Ranking Member Lieu, and distinguished members of the subcommittee, thank you for the opportunity to talk with you today about the Department of Homeland Security's policy for how our officers use cell site simulator technology in support of criminal investigations to protect the American public, and in some cases to locate and rescue victims of human trafficking, child exploitation, and kidnapping.

In fact, in one recent case, ICE officers used the technology to rescue a 6-year-old girl who was held hostage by human smugglers in Arizona. And this technology is also used by the Secret Service to protect the President and other dignitaries under the service's protective umbrella.

Needless to say, this is an important tool, but it's also a technology that must be used responsibly and consistent with our duty to protect the constitutional rights of the American people. In that spirit, DHS issued a new policy this week on the use of this technology by our officers. I believe the new DHS policy draws the right balance between enabling our officers to use this important tool and protecting the privacy and civil liberties of Americans.

Cell site simulators allow DHS officers to identify and generally locate the mobile devices of the subjects and victims of active criminal investigations. They work by collecting signals from cellular devices within the cell site simulator's vicinity, usually within under 1,000 feet, and providing the operator the relative signal strength in the general direction of a subject's cellular device. A cell site simulator, though, is not a GPS locator. It does not provide precise geolocation.

And a few other things worth highlighting here as well in terms of what cell site simulators can't do. They don't provide sending subscriber account information or any other personal information. And the cell site simulators used by DHS do not collect the content of any communications, no data, no emails, no text messages, no voice communications. No content.

The new policy issued this week supports the continued use of cell site simulators by our officers, but it also strengthens management controls over the use of this technology. Let me highlight a few provisions that are similar to the DOJ policy.

First, the new policy clarifies that before using cell site simulator technology, our officers generally must obtain a warrant from a court founded upon probable cause. There's no Supreme Court authority on this issue, but as a matter of DHS policy, we've concluded that requiring our officers to obtain a warrant, founded on probable cause, is the appropriate standard here. It draws the right balance between protecting the public and preserving the privacy and civil liberties of Americans. There are two narrow exceptions to this general rule.

First, exigent circumstances, as my compatriot here discussed, the well-established exception under the Fourth Amendment in emergency cases. And, again, as with the DOJ policy, we require

these circumstances, a showing of probable cause, but also the use of the Pen Register statute.

Second, under the DHS policy, there is an exception for exceptional circumstances. It's another very specific exception, and in practice, really only applies to the Secret Service's protective mission. The Secret Service's duty is to investigate potential threats to the President or other protected persons, and often this involves very limited information in immediate timeframes. And sometimes the information's cryptic, it may not meet the probable cause standard that is required under exigent circumstances.

But the threat is imminent, the President's nearby, the consequences of attack obviously are significant and high. In these circumstances, the Secret Service needs to locate an individual immediately in order to ensure the President's safety. This is a very limited and narrow exception to the general rule, and in these circumstances, DHS policy does not require probable cause or a warrant, but does require approval of both an executive within the Secret Service as well as the local U.S. attorney. The policy also requires a court order under the Pen Register statute or an emergency Pen Register.

The policy also establishes several other key management controls that we believe also draw the right balance between protecting the public and protecting civil liberties and privacy rights. First, the DHS policy requires that applications for search warrants must include an affidavit explaining to the court what a cell site simulator is, how it works, why it will be used in a particular case, and the minor impact it might have on cellular devices in the area; no hiding the ball from the court.

Second, the DHS policy draws a strong line on data retention. Bottom line, after a mission is done and the target is identified or located, the operator of a cell site simulator must delete all data from the device.

Third, the DHS policy requires components to train and supervise their officers using the cell site simulators.

In sum, we believe that the new DHS policy draws the right balance here between enabling our officers to use cell site simulator technology to keep dangerous criminals off the street and protect the public, and also making sure that we protect the civil liberties and privacy rights of the American people.

Chairman Hurd, Ranking Member Lieu, and distinguished members of the subcommittee, thank you again for the opportunity to testify today. Look forward to answering any questions you might have.

Mr. HURD. Thank you for your opening remarks.

[Prepared statement of Mr. Stodder follows:]

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.

Mr. HURD. And now it's a pleasure to recognize my friend and colleague from the great State of North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

Ms. Tyrangiel, Mr. Stodder, thank you for being here.

Mr. STODDER. Thank you.

Mr. WALKER. I commend both your Departments for requiring warrants for the use of these cell site simulators.

Ms. Tyrangiel, you mentioned that these are now only used on a fraction of cases. Numeric-wise, statistics, do you have any data, when you say fraction of cases, what percentage are we looking at?

Ms. TYRANGIEL. So as I mentioned, these are critical technologies that are deployed in things like kidnappings and complex narcotics investigations and fugitive apprehensions. Those things do occur every day. But, the fraction of those cases in which a cell site simulator is deployed is small. I don't have numbers for you today, but I'm happy to get back with you.

Mr. WALKER. If you would get those numbers to us, because a fraction, may be broad definitions there.

Mr. WALKER. Mr. Stodder, do you have anything to add to that?

Mr. STODDER. I have a similar response, in the sense that, I mean, they are a very important tool that's used by both Homeland Security investigations within ICE, as well as the Secret Service, and they are used in a very small fraction of cases, but I don't have the numbers with me here, but we can get those.

Mr. WALKER. Fair enough.

Mr. WALKER. Several of you mentioned—both of you mentioned as far as new policy, Mr. Stodder, and some things that changed September the 1st. Before that timeline, were you allowed to retain, or ascertain communication before the new policy was instituted? Ms. Tyrangiel?

Ms. TYRANGIEL. This policy makes clear that devices must be configured not to collect content.

Mr. WALKER. Before September 1, did you collect other content?

Ms. TYRANGIEL. I will have to get back to you about what the policy said, but—I'll have to take that back.

Mr. WALKER. Okay. Mr. Stodder?

Mr. STODDER. Well, this is the first overarching DHS policy on the use of cell site simulators, but the components before this policy certainly used cell site simulators but did not use them to collect content at all. I mean, literally the technology is not configured to collect content, at least the technology that DHS——

Mr. WALKER. Well, I'm glad to hear that we have new policies. I do have some trepidation about what we were collecting before then. I hope that we can get that information back as well.

Mr. STODDER. Sure.

Mr. WALKER. It leads me to the question, would it be better to enact legislation to make sure these policies are clear, because my concern is if you have new agency department heads, who makes the standard, who makes the rules there? Ms. Tyrangiel, would you like to comment on that?

Ms. TYRANGIEL. Sure. Because we have just implemented these policies and because we are about to see how they are implemented and how they work, we would recommend that we evaluate how

they are going in practice before anything is codified. On the other hand, anything you wish to work on, we would be happy to work on you with.

Mr. WALKER. Mr. Stodder, would you——

Mr. STODDER. I'd have a similar response, in the sense that, I mean, we obviously just issued our policy this week. We feel very good about the policy and strong about the policy. Our operating components definitely believe that the policy draws the right balance between enabling the use of these important technologies and privacy, but certainly if this committee were to walk down the road of considering legislation, we would obviously work with the committee on it.

Mr. WALKER. If the warrant requirements for these cell site catchers, if you will, both the DOJ created—the DOJ created an exception for circumstances, okay, where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Can you talk a little bit about what those impracticable circumstances—I mean, that's a kind of a broad definition. Would you mind expounding on that, Ms. Tyrangiel?

Ms. TYRANGIEL. Yeah. This exception is intended to be deployed very rarely, very rare circumstances. And, in fact, from the Department's perspective, this is more like a safety valve in the policy, in the event there are circumstances that we could not foresee when we went to a flat warrant requirement.

So in order to use that exception even now, there would need to be no problem under the Fourth Amendment, and it would need to be impracticable to get a warrant, and there would need to be a series of high level sign-offs in order to use that exception, including a high level agency official, the U.S. attorney in a jurisdiction, and a deputy attorney general in the criminal division.

And any exceptions that are granted under this provision will be tracked by the criminal division, so that if there is a set of circumstances that is emerging and the policy needs to be tweaked or adjusted, we can do that.

Mr. WALKER. Sure. So each one of those circumstances, you're telling me that there's a consistency there that all high levels sign off no matter what the situation might be?

Ms. TYRANGIEL. That's correct. In order to be able to use that exception, all of those people would need to sign off.

Mr. WALKER. I'm concerned about this exception and maybe the augmentation of it or the growth of it where—good intentions here, but I would assert if we are not able to put some teeth into this, that it could be a very broad definition.

Mr. Stodder, I've got about 15 seconds. Did you want to add anything to that?

Mr. STODDER. Well, I mean, the analogous exception of the DHS policy is the exceptional circumstances exception, which as I think I've discussed, it's—I mean, the main focus of that exception, at least within DHS, I mean, without putting any conceivable other option, is the Secret Service protective mission, in the sense of where it is an exceptional circumstance where probable cause may not necessarily make sense in that context, so the Pen Register applies.

Mr. WALKER. Okay. My time has expired. Thank you, Mr. Chairman. I yield back.

Mr. HURD. Thank you, Mr. Walker.

I'd now like to recognize Ranking Member Lieu for 5 minutes.

Mr. LIEU. Thank you.

I have a question about the capabilities of these stingrays, not how they can be configured. Just in terms of capability, can they collect content or they cannot?

Ms. TYRANGIEL. As I said, our policy requires that they be configured not to collect content. The kind of configuration we're talking about, and understanding that I am a lawyer, not a technologist, is the software configuration, not an on and off switch where someone could switch it on and off.

Mr. STODDER. I'm similarly hampered by being a lawyer, not a technologist, but, I will say the DHS—I mean, the cell site simulators that DHS agencies use, both HSI as well as Secret Service, are absolutely configured by the vendor not to collect content. I mean, I couldn't tell you one way or the other as to whether they could be, theoretically could be configured to collect content, but I know for a fact that the cell site simulators that DHS uses do not collect content and cannot collect content.

Mr. LIEU. Okay. If you could get an answer back as to whether they have the capability to——

Mr. STODDER. Sure.

Mr. LIEU. —not just——

Mr. STODDER. We can get back to you on that in terms of whether there are cell site simulators on the market that could, but DHS does not as a matter of policy.

Mr. LIEU. Okay. I share some of the same concerns of Mr. Walker regarding the exigent circumstances exception, but specifically I had one about the Secret Service.

Mr. STODDER. Yep.

Mr. LIEU. Is it a blanket exception for the entire Secret Service?

Mr. STODDER. Well, no. I mean, it's an exception within the DHS policy that—I mean, and the key exception that we can envision is the Secret Service's protective mission. So it's not an exception for the Secret Service, but in certain circumstances where you could have an immediate threat to the President and you have cryptic information. Our conclusion in terms of drawing the right balance between security and privacy here, is to err on the side here of protection.

Mr. LIEU. But why wouldn't they just fall under exigent circumstances?

Mr. STODDER. Well, because you could have a circumstance where—because the issue with the exigent circumstances exception is that the exigent circumstances exception still requires probable cause. And so you could have a circumstance with the Secret Service where—I mean, I'm trying to think of a fact situation where it could arise, but where you might have a cryptic email or something like that, or something that indicates there's a threat to the President or to a distinguished person within the Secret Service protective umbrella where the Secret Service would not have the capability, or the time, or enough information to determine whether

there's probable cause, but you need to locate that person before there's an attack on the President.

Mr. LIEU. I see. So let's say it's dealing with the Secret Service in a counterfeiting case. That exception would not apply?

Mr. STODDER. No, that would not apply. In a criminal investigative case, like a counterfeiting case, absolutely not, it would not apply. I mean, in a normal, I can't imagine a circumstance where this exception would apply in a counterfeiting case.

Mr. LIEU. Now, it looks like there's also an exception for the Foreign Intelligence Surveillance Court, is that correct, in the policy?

Ms. TYRANGIEL. The Department's policy applies to the use of cell site simulators in furtherance of criminal investigations inside the United States. There is a note, a footnote in the policy that discusses national security investigations that says, when working under FISA, the Department will make probable cause-based showings and make appropriate disclosures to the court in a manner that is consistent with the policy.

Mr. LIEU. Okay. What does that mean in terms of——

Ms. TYRANGIEL. Well, of course FISA and national security authorities are different than criminal authorities, but the policy does indicate via footnote that attorneys will make probable cause-based showings to the court and that they will make appropriate disclosures. And, of course, there is a whole section in the policy about transparency and the importance of transparency and letting the court know of the technology to be used. But because those authorities are different, different protocols, different structure, and statutes, they are not further defined.

Mr. LIEU. Could the Department just apply it the same way with the FISA court? Why would it have to be applied differently?

Ms. TYRANGIEL. That is a function of a different court and a different procedural setup based on FISA and that authority particularly, and so it's not the same system or the same authorities, and therefore, they're just slightly differently oriented.

Mr. LIEU. Okay. In non-FISA courts if there's a case that is brought, the ACLU letter references information where prosecutors will not disclose a stingray was used, in fact, they will say it was a confidential source. Do you have any thoughts on that or can your policy say that ought to be disclosed rather than using the, quote-unquote, confidential source phrase?

Ms. TYRANGIEL. I'm not familiar with the ACLU letter. I can tell you that the policy has a detailed section on transparency that the prosecutor must let the court know about the technology to be used, how it will be used, the disruption it might cause, to ensure that—should the court have questions or that the court knows in advance about this technology.

Mr. LIEU. So I've entered the ACLU letter in the record. I'll also send it to you. If you don't mind, if you could respond to the issues they raised, that would be terrific.

And then if I could take one more question. In terms of how you think this is going to be applied, how are you training your folks on this?

Ms. TYRANGIEL. Implementation is ongoing and the components are actively working on ensuring that all the pieces of this are falling into place.

Mr. LIEU. And what about local and State law enforcement? Do you do any guidance, any training?

Ms. TYRANGIEL. So I can tell you that a couple of—anecdotally, that a couple of State and local agencies have asked about this policy. We are hopeful that it will serve as a model. Beyond that at this time, that's all the information that I have.

Mr. LIEU. Great. Thank you. I yield back.

Mr. HURD. Thank you. I'll recognize myself for 5 minutes.

Let's pick up on Congressman Lieu's line. So when local law enforcement, they can attain these devices without DOJ's permission? Is that correct?

Ms. TYRANGIEL. They can buy and operate this equipment on their own, yes.

Mr. HURD. Is DOJ planning to require State and local law enforcement agencies to adhere to DOJ's policy or have similar policies of their own?

Ms. TYRANGIEL. So this policy, the Department's policy, will apply to State and locals when we are working together and when we are assisting State and locals. It is complicated and difficult beyond that for us to oversee the State and locals, but as I said, we are really hopeful that this will serve as a model for State and locals as they think about their own policies.

Mr. HURD. Does DOJ provide any of these stingrays to local law enforcement?

Ms. TYRANGIEL. Not that I'm aware of, but I would want to double-check and get back to you.

Mr. HURD. Yeah. My question there is, if DOJ is providing the equipment to local law enforcement, then can they be bound by the rules of DOJ in the operation of this? That would be my question.

Ms. TYRANGIEL. I'd be happy to take it back.

Mr. HURD. Great.

Mr. HURD. And, Mr. Stodder, can people apply for this within DHS?

Mr. STODDER. Well, I mean, you're asking in terms of the State and locals. I mean, similarly the DHS policy says that if DHS officers are working on a case with State and local governments, I mean, certainly the DHS policy applies in that circumstance to the DHS officers in that task force sort of environment.

DHS does not actually give or loan this equipment to State and local law enforcement. DHS does not do that. And the State and local governments can purchase this equipment on their own using their State funds, and consistent with their own State laws and the Federal Constitution, under their own police powers under the Constitution.

The issue here I think you're getting at perhaps is certainly State and local governments can apply for Federal grant funds from FEMA. And the Federal Government under FEMA, and I believe the Justice Department as well, I mean, we give grant monies to the States, and then the States, and then subgrantees to local governments can purchase equipment that is on an authorized equipment list, and certainly some States could conceivably purchase cell site simulator technology.

And our position on that essentially is—I mean, our standard terms and conditions in grant funding to the States and local gov-

ernments is essentially to—you know, they have to apply—they have to use the technologies that they buy consistent with the law and consistent with the Constitution, but we haven't imposed essentially our internal DHS policies in that context or other contexts on the State and local governments with regard to the grant dollar—with regard to the equipment that they buy using Federal grant dollars.

Mr. HURD. So, just so I'm clear, I'm a local law enforcement, let's say I'm a county sheriff——

Mr. STODDER. Yep.

Mr. HURD. —I apply for Stonegarden funds, I get them, I buy an IMSI-catcher, and I would not be bound by DHS policy on the use of said IMSI-catchers?

Mr. STODDER. Yeah, correct. You would not be bound by DHS policy with regard to the use of cell site simulators yourself. And essentially, that's correct.

Mr. HURD. So is there any effort on the way to have folks using Federal funds, using DHS funds or DOJ funds, to adhere to the rules and regulations? Because aren't there some significant nondisclosure agreements that are signed by local law enforcement? Is it with you all or with the companies when it comes to this issue?

Mr. STODDER. Not with the Department of Homeland Security. We do not require those kinds of nondisclosure agreements when the State and local governments, say, were to use something like that. And the question of whether the Department of Homeland Security would essentially require the use—essentially State and local governments using of Federal funds to, you know, the City of Bakersfield or whatever else, to apply internal DHS policies, we have not sort of determined that that would be the right approach, for any number of reasons from federalism.

But also from the perspective of you're talking about a $1.5 billion grant program with 56 grantees and thousands of subgrantees, and the ability to track the use of all these subgrantees of all this equipment, I mean, I think that would be—it would be a significant, you know, consideration to think about.

Mr. HURD. Thank you.

Yes, ma'am.

Ms. TYRANGIEL. I'm sorry.

Mr. HURD. Yeah. The same question. I believe some local law enforcement in terms of NDAs with the FBI on some of the use of this technology. Is that correct, and how does that work?

Ms. TYRANGIEL. Yeah. So the nondisclosure agreements that you're referring to are agreements between the FBI and State and local law enforcement. Those agreements are intended to protect particularly sensitive information about the operations, the operation of the technology, the capabilities of the technology. They're not meant actually to preclude more transparency in terms of disclosing that they've been used in any particular case, and actually FBI is revising those agreements now. But as to the question about how they intersect with State and local use, traditionally they're not a means to oversee the actual use of the equipment, rather they're an agreement about the sensitivity of the information involved.

Mr. HURD. Okay. Thank you.

I'm going to now recognize Mr. Lieu for an additional 5 minutes.

Mr. LIEU. Thank you.

Let me follow up on Chairman Hurd's questions about the FBI. So I have a letter from April 13, 2015, written from the Federal Communications Commission to Senator Bill Nelson. My understanding, according to this letter, is that for these devices to be used by law enforcement, they have to be certified by the FCC, and the commission places two conditions on them: one is that these devices will be used in fact by law enforcement, and second, that State and local law enforcement agencies must coordinate in advance with the FBI the acquisition and use of the equipment.

Is there any reason we couldn't, consistent with DOJ policy, ask the FBI to say, okay, if you're going to use this equipment, you need to use it consistent with our FBI standards, which are DOJ standards, which is you need to get a warrant before you use it?

Ms. TYRANGIEL. So as I was mentioning, these agreements that you referenced to are—with respect to the sensitivity of the information and agreements about how to manage that sensitivity, they may be more or less effective at managing and effecting oversight over the use of this technology, but it is something we're happy to look at.

Mr. LIEU. Thank you.

And then, Mr. Stodder, I forgot to ask you the first time.

Mr. STODDER. Yeah.

Mr. LIEU. We'll send you the ACLU letter as well——

Mr. STODDER. Thank you.

Mr. LIEU. —and if you could respond to some of the issues that they raised, that would be great as well.

Mr. STODDER. Be happy to do that.

Mr. LIEU. So I have a different line of questioning, which is, these policies don't apply to the NSA or CIA or other agencies other than your own, correct?

Mr. STODDER. Correct.

Mr. LIEU. What happens if the FBI is doing an operation with local law enforcement? Can they sort of say, hey, you local law enforcement, you go use the stingray and do what we can't do? Is there anything in policy that keeps them from doing that?

Ms. TYRANGIEL. If I'm understanding your question correctly, if the FBI is working with the locals and using a cell site simulator, this——

Mr. LIEU. Well, the FBI is not using it, but the local——

Ms. TYRANGIEL. Oh.

Mr. LIEU. —person is——

Ms. TYRANGIEL. As in—yeah, they get around this policy——

Mr. LIEU. Correct.

Ms. TYRANGIEL. That is not permitted.

Mr. LIEU. Okay. Thank you.

In terms of these other agencies, what law enforcement other than—we'll take out the intelligence agencies, but what other law enforcement would not be covered by the two policies here today?

Mr. STODDER. Well, it would be law enforcement that's not part of the Department of Homeland Security or the Department of Justice, so presumably the Park Police, or I'm informed of the—I guess the Government Printing Office potentially has a——

Mr. LIEU. Correct.

Mr. STODDER. Yeah. So are there other law enforcement agencies that would not be covered?

Ms. TYRANGIEL. I'm not aware of which other law enforcement agencies would even have this capability.

Mr. STODDER. Yeah.

Ms. TYRANGIEL. So——

Mr. LIEU. And then you had mentioned earlier there's going to be tracking of the number of times that these devices are used, or only when they're used without a warrant?

Ms. TYRANGIEL. No. The policy requires a tracking of numbers annually of how many times they're used and how many times they're used in emergency circumstances in addition to the requirement under the exceptional circumstances exception to track any and all exceptions under that provision of the policy.

Mr. LIEU. And that's both agencies?

Mr. STODDER. Correct.

Mr. LIEU. And who gets this information?

Ms. TYRANGIEL. The agencies are required to track and collect their use, and the criminal division tracks the number of exceptions granted.

Mr. LIEU. Would this committee get that information or could this committee get that information? Is it public?

Ms. TYRANGIEL. We'd be happy to work with you on any requests you have for that information.

Mr. LIEU. Okay. Great. Thank you.

Mr. STODDER. Similarly with the DHS.

Mr. LIEU. Thank you. I yield back.

Mr. HURD. I'd like to recognize the gentleman from Iowa, Mr. Blum, for 5 minutes.

Mr. BLUM. Thank you, Chairman Hurd.

And thank you, Ms. Tyrangiel, is it?

Ms. TYRANGIEL. Tyrangiel.

Mr. BLUM. Tyrangiel, and Mr. Stodder for appearing here today. Appreciate it very much. I've got about 5 questions to each one of you, so if you can be quasi brief, we can get through this in 5 minutes.

First question, does your agency take the position that it does not, does not need a warrant to use the device to track a known suspect, a known suspect, in public?

Ms. TYRANGIEL. Our agency has gone to a policy that requires a warrant with two narrow circumstances for exceptions. So, we are now using a warrant as a general matter except in two circumstances. And I——

Mr. BLUM. And those are?

Ms. TYRANGIEL. Exigent circumstances that would satisfy the Fourth Amendment warrant exception and exceptional circumstances where the Fourth Amendment is not implicated and getting a warrant is impracticable. So even if the Fourth Amendment isn't implicated, if it's not impracticable to get a warrant, agents must get a warrant.

And if there are exceptional circumstances, that we expect to occur very rarely, then there would need to be sign-off from a high level agency official, the U.S. attorney, and a deputy assistant at-

torney general from the criminal division. And even in such circumstances——

Mr. BLUM. To not get a warrant?

Ms. TYRANGIEL. Exactly.

Mr. BLUM. What were those three individuals, a high level——

Ms. TYRANGIEL. A high level agency official within the law enforcement agency, the U.S. attorney in the district, and the deputy assistant attorney general in the criminal division.

Mr. BLUM. Is it all three or any of those three?

Ms. TYRANGIEL. All three.

Mr. BLUM. All three to not get a warrant?

Ms. TYRANGIEL. That's right.

Mr. BLUM. Okay.

Mr. Stodder?

Mr. STODDER. As a matter of DHS policy, similarly to the DOJ policy, DHS policy, we have determined that before the use of cell site simulators, that we will require probable cause in a warrant in most cases, with two exceptions, similar exceptions to the Justice Department: one is exigent circumstances, so involving, you know, well-recognized Fourth Amendment exception if there's life and limb at issue, et cetera.

And the second is exceptional circumstances, which in the DHS context is—the main example here would be the Secret Service protective mission with regard to protection of the President, which is not a criminal investigative mission, but it's where probable cause may not necessarily be the right standard in that context.

And, again, we also have, you know, significant sign-off where the Secret Service believes that it needs to have a cell site simulator but does not have probable cause or won't get a warrant, but we would need sign-off from a senior level executive within the Secret Service as well as the local U.S. attorney. And even there, we would also apply the Pen Register statute essentially to obtain a court order to use the technology or in an emergency Pen Register under the Pen Register statute.

Mr. BLUM. So both of those signatures required or just one of the two?

Mr. STODDER. Both.

Mr. BLUM. Both. Well, what about when the suspect is the subject of an arrest warrant? Is there any change there?

Ms. TYRANGIEL. No. A search warrant is still required under the policy, again, barring exigent circumstances that would satisfy the Fourth Amendment's warrant exception or the exceptional circumstances provision that I described to you that requires all that sign-off and fitting in with particular circumstances.

Mr. STODDER. Same with DHS.

Mr. BLUM. Mr. Stodder. Tell me if this is correct or not. I believe I have it correct. Each agency's policy requires deletion of the data at least once every 30 days?

Ms. TYRANGIEL. So our policy——

Mr. BLUM. Is that correct?

Ms. TYRANGIEL. Yes. And it also requires deletion as soon as the mission is completed. So if it's before 30 days, in the circumstance where you're trying to identify an unknown phone, it gets deleted immediately. It doesn't wait until the 30 days.

Mr. STODDER. And the same is true under the DHS policy. It requires deletion immediately after the mission.

Mr. BLUM. Right after the mission?

Mr. STODDER. Yeah.

Mr. BLUM. Now, the government's great at making laws, setting rules and regulations. I'm from the private sector. Where we're weak is follow-through.

So my question is what mechanism is there in place to ensure that what you just said actually happens?

Ms. TYRANGIEL. So there are a couple provisions in the policy that address this: one is there needs to be an auditing procedure put in place by each agency to make sure that the data is deleted consistent with the policy; and second, the policy requires each agency to designate an executive level point of contact in each jurisdiction to ensure that the policy's implemented and complied with.

Mr. BLUM. Mr. Stodder?

Mr. STODDER. The DHS policy is identical in that respect.

Mr. BLUM. So is this currently in place or is this——

Mr. STODDER. Yes.

Ms. TYRANGIEL. The policy is effective immediately and——

Mr. STODDER. In place.

Mr. BLUM. And out of curiosity, what will the punishment be if this policy is not followed? Because I've sat in on enough of these hearings and have people sit in your chairs where things, you know, weren't followed through on, things were messed up, they were against the rules, the IG says they need to change, and they don't change, and they receive bonuses instead of being terminated. So what happens if the rules are not followed?

Ms. TYRANGIEL. As with any technology procedure within an agency, if individuals violate their agency's orders, they are accountable to their agencies and subject to discipline.

Mr. BLUM. Mr. Stodder?

Mr. STODDER. And the same thing is true in DHS. I mean, each component will have a structure essentially to hold their employees accountable for not using technologies in a way that's authorized by DHS policy, and certainly DHS headquarters would have a similar sort of capability of management response.

Mr. BLUM. So you're saying it's the Department's policy?

Mr. STODDER. Yes.

Mr. BLUM. Yeah. I hope you will tell us today at this hearing that if someone doesn't follow these policies and somebody's privacy rights are in question, that you're going to take the appropriate actions——

Mr. STODDER. Yes.

Mr. HURD. —if it's——

Mr. STODDER. Department——

Mr. BLUM. Go ahead.

Mr. STODDER. At the Department of Homeland Security it certainly—you know, the component leaderships would take the—whatever appropriate action would make sense under the facts and circumstances of that case.

Ms. TYRANGIEL. Same here.

Mr. BLUM. Great. I think my time is up. I yield back, Mr. Chairman. Thank you very much.

Mr. HURD. I have a very basic question before we end. Is the private use of IMSI-catchers, is that illegal?

Ms. TYRANGIEL. I don't know the details of sort of how the manufacturers market themselves or to whom they can provide this, whether it is illegal. I can speak, you know, obviously to the government use and to these agreements between the State and locals and the FBIs, but not the private use.

Mr. STODDER. Yeah. I'm similarly hampered by lack of knowledge on that in this sense, but we are happy to get back to you on that.

Mr. HURD. Great. Thank you.

I apologize we started late today, but this is an important issue of being able to protect our civil liberties and ensure that law enforcement has the tools they need in order to do their jobs.

I think the plans have come a long way over these past few months. And we look forward to the additional information that we requested and having further conversations on this, and looking forward on how we can have some legislative fixes to this across the Federal Government.

I appreciate you all's time here today. And without—I thank you for taking your time to appear.

And if there's no further business, without objection, the subcommittee stands adjourned.

[Whereupon, at 3:43 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

HEARING BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED
"EXAMINING LAW ENFORCEMENT USE OF CELL PHONE TRACKING DEVICES"

OCTOBER 21, 2015

QUESTIONS FOR THE RECORD
FROM CHAIRMAN CHAFFETZ TO
ELANA TYRANGIEL, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

1. **Before the September 3, 2015, release of DOJ's policy governing IMSI catchers, had any DOJ component collected non-metadata using an IMSI catcher device (including, but not limited to, the content of calls, text messages, pictures, or messaging through apps) in domestic criminal investigations after January 1, 2010? If so, for each instance please list the component, the type of content collected, and the date of collection.**

RESPONSE: Between January 1, 2010 and September 2, 2015, the Federal Bureau of Investigation ("FBI"), the Drug Enforcement Administration ("DEA"), Alcohol, Tobacco, Firearms and Explosives ("ATF"), and the United States Marshals Service ("USMS") only used cell-site simulators to collect dialing, routing, signaling, and addressing information in domestic criminal investigations. Additionally, consistent with the limitations in the Pen Register Act, cell-site simulators were not used to collect the content of communications.

2. **Are DOJ's IMSI catchers capable of collecting content, including, but not limited to, the content of calls, text messages, pictures, or messaging through apps?**

RESPONSE: The Department of Justice's policy regarding the use of cell-site simulator technology ("Department's policy," enclosed) requires that Department cell-site simulators "must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone." (*See* Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology, at 2.) As a technical matter, some cell-site simulator models used by Department components, including FBI and DEA, would be capable of collecting content if they were configured to do so and had the necessary software installed. As noted above, the Department's policy does not permit such configuration and use.

3. **In criminal prosecutions, will DOJ treat the use of an IMSI catcher as a confidential source when making disclosures to the defendant?**

RESPONSE: As in any criminal prosecution, the Department will abide by the Federal Rules of Criminal Procedure, including Rule 16, as well as any pertinent authority governing disclosures to the defendant, including the assertion of the law enforcement sensitive qualified evidentiary privilege where appropriate to protect sensitive information about the operation of the device. The Department's policy emphasizes the need to comply with all legal disclosure requirements and for candor to the court in legal filings related to such devices.

4. **Are there IMSI catchers on the market and available to DOJ capable of collecting content, including but not limited to, the content of calls, text messages, or messaging though apps?**

RESPONSE: As noted in response to Question 3, the Department's policy regarding the use of cell-site simulator technology requires that Department cell-site simulators "must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone." (*See* Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology, at 2.) The Department is not familiar with the entire array of cell-site simulator devices that are available on the market, and can only comment regarding its own equipment. As noted in response to Question 2, as a technical matter some cell-site simulator models—including some used by Department law enforcement components—would be technologically capable of collecting content if so configured and with the necessary software installed. Such configuration and use, however, would violate the Department's policy.

5. **Will DOJ commit to requiring state and local law enforcement [*sic*] comply with DOJ's policy when DOJ provides either the IMSI catcher device or the funds for state and local law enforcement to obtain the devices?**

RESPONSE: The Department generally does not provide cell-site simulators to State and local law enforcement or fund their purchase. *See* Response to Question 7 below. With respect to funding, the Department is aware of only a handful of instances in which State or local law enforcement agencies have purchased cell-site simulators using formula-based Federal grant money. Nonetheless, the Department is open to considering whether Federal grant recipients should be required to comply with the Department's policy.

6. **Does DOJ have any knowledge of private—that is non-law enforcement and non-military—use of IMSI catchers? If so, please provide details of each report of misuse.**

RESPONSE: The Department is aware of media reports alleging that "hobbyists" may be building and testing cell-site simulators. In addition, the Department is aware of isolated incidents in which a cell-site simulator may have been used by a private entity. Any such use of a cell-site simulator could be inconsistent with Federal law. *See* 18 U.S.C. §§ 2512, 3121.

7. **Since January 1, 2010, has DOJ provided any IMSI catcher devices to state or local law enforcement outside of the context of a joint investigation? If so, please provide the name of the receiving agency, the device provided, and the month and year the device was provided.**

RESPONSE: Neither FBI, DEA, ATF, nor USMS generally do not provide cell-site simulators to State or local law enforcement. However, the Department is aware of one instance in which this did occur. In or about October 2010, the FBI's Charlotte field office requested and received from FBI headquarters a cell-site simulator for loan to the North Carolina Bureau of Investigation for an indeterminate period of time. Ultimately, the Charlotte field office retrieved the loaned cell-site simulator and returned it to FBI headquarters.

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology

Cell-site simulator technology provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort, a complex narcotics investigation, or to locate or rescue a kidnapped child, cell-site simulators fulfill critical operational needs.

As with any law enforcement capability, the Department must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data.

As technology evolves, the Department must continue to assess its tools to ensure that practice and applicable policies reflect the Department's law enforcement and national security missions, as well as the Department's commitments to accord appropriate respect for individuals' privacy and civil liberties. This policy provides additional guidance and establishes common principles for the use of cell-site simulators across the Department.[1] The Department's individual law enforcement components may issue additional specific guidance consistent with this policy.

BACKGROUND

Cell-site simulators, on occasion, have been the subject of misperception and confusion. To avoid any confusion here, this section provides information about the use of the equipment and defines the capabilities that are the subject of this policy.

Basic Uses

Law enforcement agents can use cell-site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator user's vicinity. This technology is one tool among many traditional law enforcement techniques, and is deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

---

[1] This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. When acting pursuant to the Foreign Intelligence Surveillance Act, Department of Justice components will make a probable-cause based showing and appropriate disclosures to the court in a manner that is consistent with the guidance set forth in this policy.

How They Function

Cell-site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

What They Do and Do Not Obtain

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, 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, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

MANAGEMENT CONTROLS AND ACCOUNTABILITY[2]

Cell-site simulators require training and practice to operate correctly. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Department personnel 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.

[2] This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.

2. Within 30 days, agencies shall designate an executive-level point of contact at each division or district office responsible for the implementation of this policy, and for promoting compliance with its provisions, within his or her jurisdiction.

3. Prior to deployment of the technology, use of a cell-site simulator by the agency must be approved by an appropriate individual who has attained the grade of a first-level supervisor. Any emergency use of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction, as described in paragraph 2 of this section, or by a branch or unit chief at the agency's headquarters.

Each agency shall identify training protocols. These protocols must include training on privacy and civil liberties developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

LEGAL PROCESS AND COURT ORDERS

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent), except as provided below.

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 *and* the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell-Site Simulators").

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

1. Exigent Circumstances under the Fourth Amendment

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval in order to be lawfully deployed. 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. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, 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. In addition, in the subset of exigent situations where circumstances necessitate emergency pen register authority pursuant to 18 U.S.C. § 3125 (or the state equivalent), the emergency must be among those listed in Section 3125: immediate danger of death or serious bodily injury to any person; conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year. In addition, the operator must obtain the requisite internal approval to use a pen register before using a cell-site simulator. In order to comply with the terms of this policy and with 18 U.S.C. § 3125,[3] the operator must contact the duty AUSA in the local U.S. Attorney's Office, who will then call the DOJ Command Center to reach a supervisory attorney in the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations.[4] Assuming the parameters of the statute are met, the ESU attorney will contact a DAAG in the Criminal Division[5] and provide a short briefing. If the DAAG approves, the ESU attorney will relay the verbal authorization to the AUSA, who must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125. Under the provisions of the Pen Register Statute, use under emergency pen-trap authority must end when the information sought is obtained, an application for an order is denied, or 48 hours has passed, whichever comes first.

2. *Exceptional Circumstances Where the Law Does Not Require a Warrant*

There may also be other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. In such cases, which we expect to be very limited, agents must first obtain approval from executive-level personnel at the agency's headquarters and the relevant U.S. Attorney, and then from a Criminal Division DAAG. The Criminal Division shall keep track of the number of times the use of a cell-site simulator is approved under this subsection, as well as the circumstances underlying each such use.

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, 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. In addition,

[3] Knowing use of a pen register under emergency authorization without applying for a court order within 48 hours is a criminal violation of the Pen Register Statute, pursuant to 18 U.S.C. § 3125(c).

[4] In non-federal cases, the operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

[5] In requests for emergency pen authority, and for relief under the exceptional circumstances provision, the Criminal Division DAAG will consult as appropriate with a National Security Division DAAG on matters within the National Security Division's purview.

if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in section 1 directly above).

APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

When making any application to a court, the Department's lawyers and law enforcement officers must, as always, disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement agents must consult with prosecutors[6] in advance of using a cell-site simulator, and applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.[7]

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.

2. An application or supporting affidavit should inform the court that the target cellular device (*e.g.*, cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

3. An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

---

[6] While this provision typically will implicate notification to Assistant United States Attorneys, it also extends to state and local prosecutors, where such personnel are engaged in operations involving cell-site simulators.

[7] Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (*e.g.*, tradecraft, capabilities, limitations or specifications). Sample applications containing such technical information are available from the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division. To ensure courts receive appropriate and accurate information regarding the technical information described above, prior to filing an application that deviates from the sample filings, agents or prosecutors must contact CCIPS, which will coordinate with appropriate Department components.

DATA COLLECTION AND DISPOSAL

The Department is committed to ensuring that law enforcement practices concerning the collection or retention[8] of data are lawful, and appropriately respect the important privacy interests of individuals. As part of this commitment, the Department's law enforcement agencies operate in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of a cell-site simulator. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence,[9] the Department's use of cell-site simulators shall include the following practices:

1. 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.

2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.

3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

Agencies shall implement an auditing program to ensure that the data is deleted in the manner described above.

STATE AND LOCAL PARTNERS

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This 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.

TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Each law enforcement agency shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the

[8] In the context of this policy, the terms "collection" and "retention" are used to address only the unique technical process of identifying dialing, routing, addressing, or signaling information, as described by 18 U.S.C. § 3127(3), emitted by cellular devices. "Collection" means the process by which unique identifier signals are obtained; "retention" refers to the period during which the dialing, routing, addressing, or signaling information is utilized to locate or identify a target device, continuing until the point at which such information is deleted.

[9] It is not likely, given the limited type of data cell-site simulators collect (as discussed above), that exculpatory evidence would be obtained by a cell-site simulator in the course of criminal law enforcement investigations. As in other circumstances, however, to the extent investigators know or have reason to believe that information is exculpatory or impeaching they have a duty to memorialize that information.

responsibility of each agency with respect to the way the equipment is being used (*e.g.*, significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). We expect that agents will familiarize themselves with this policy and comply with all agency orders concerning the use of this technology.

Each division or district office shall report to its agency headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction; the number of deployments at the request of other agencies, including State or Local law enforcement; and the number of times the technology is deployed in emergency circumstances.

Similarly, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent. Model materials will be provided to all United States Attorneys' Offices and litigating components, each of which shall conduct training for their attorneys.

* * *

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. 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. This policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

Question#:	1
Topic:	Metadata Collected
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

2015-11-19 Hurd to Stoddard-DHS - QFRs 10-21 Stingray Hearing RESPONSE

Question: Before the October 20, 2015, release of the Department of Homeland Security's (DHS) policy governing IMSI catchers, had any DHS component collected non-metadata using an IMSI catcher device (including, but not limited to, the content of calls, text messages, pictures, or messaging through apps) in domestic criminal investigations after January 1, 2010? If so, for each instance please list the component, the type of content collected, and the date of collection.

Response: No. Cell-site simulators used by DHS have not collected and do not collect non-metadata, (including, but not limited to, the content of calls, text messages, pictures, or messaging through apps).

Question#:	2
Topic:	IMSI Catchers Capabilities 1
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Are DHS's IMSI catchers capable of collecting content, including, but not limited to, the content of calls, text messages, pictures, or messaging through apps?

Response: No. Cell-site simulators used by DHS are not capable of collecting the contents of any communication, nor data contained on the phone itself, e.g., call content, , emails, text messages, contact lists, or images.

Question#:	3
Topic:	IMSI Catchers Capabilities 2
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Are there IMSI catchers on the market and available to DHS capable of collecting content, including, but not limited to, the content of calls, text messages, pictures, or messaging through apps?

Response: Although varying degrees of such technology are available, DHS does not currently possess or plan to acquire cell-site simulator devices that are capable of collecting content, including, but not limited to, the content of calls, text messages, pictures, or messaging through apps.

Question#:	4
Topic:	State and Local Law Enforcement Compliance
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Will DHS commit to requiring state and local law enforcement comply with DHS's policy when DHS provides either the IMSI catcher devices or the funds for state and local law enforcement to obtain the devices?

Response: DHS does not loan cell-site simulators to state and local law enforcement agencies, but does use such technology in support of state and local law enforcement agencies with appropriate court authorization. DHS's policy applies to instances in which Department Components are assisting state or local law enforcement agencies.

With respect to concerns regarding state and local law enforcement agencies that purchase cell-site simulator technology with DHS's financial assistance, DHS maintains a number of safeguards to ensure that, as a condition of their award, recipients of preparedness grant funds comply with all applicable federal laws, executive orders, and regulations governing the proper and lawful use of the technology. While not specific to cell-site simulators, the scope of these assurances guards individual rights and civil liberties by prohibiting conduct that violates protections under the Constitution, including the Fourth Amendment, and all other applicable federal laws.

Additional controls governing the use of cell-site simulator technology are embedded in Federal Emergency Management Agency (FEMA) policies governing the application for and the use of preparedness grant funds. For example, as part of the preparedness grant application process, FEMA requires that applicants proposing the acquisition of cell-site simulator technology provide documentation to prove that such equipment is necessary to address a specific preparedness capability shortfall. Supplemental policy governing the acquisition and use of cell-site simulator technology is also provided in the Authorized Equipment List, which applies to all equipment purchased with preparedness grant funds. The Authorized Equipment List policy specifically states that use of such technologies is subject to the requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §§ 2510-2522.

DHS acknowledges that policies for use and training for law enforcement personnel who seek to acquire cell-cite simulator technology through FEMA's preparedness grant programs could further safeguard privacy and civil liberties protections. DHS will further examine whether grantee adoption of baseline policy provisions, including training requirements, should be mandated as a condition of purchase through FEMA's preparedness grant programs, and if so, how any necessary training can most effectively be delivered.

Question#:	5
Topic:	Private Use
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Does DHS have any knowledge of private - that is, non-law enforcement and nonmilitary - use of IMSI catchers? If so, please provide details of each report of misuse.

Response: DHS has no knowledge of private use of IMSI catchers.

Question#:	6
Topic:	DHS Provided Devices
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Since January 1, 2010, has DHS provided any IMSI catcher device to state or local law enforcement outside of the context of a joint investigation? If so, please provide the name of the receiving agency, the device provided, and the month and year the device was provided.

Response: DHS does not loan cell-site simulators to state and local law enforcement agencies, but does use such technology in support of state and local law enforcement agencies with appropriate court authorization. DHS's policy applies to instances in which Department Components are assisting state or local law enforcement agencies.

Question#:	7
Topic:	Grant Compliance
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: According to testimony given during the hearing, DHS is responsible for administering a $1.5 billion dollar grant program with 56 grantees and thousands of sub grantees. With respect to IMSI catchers, what, if anything, does DHS do post-award to ensure that grant recipients comply with the terms of the grant?

Response: The Department does allow the purchase of cell site simulators through the preparedness grant programs that are administered by FEMA. Before allowing such purchase, FEMA requires the grant recipient to provide documentation to prove that the equipment is necessary to address a specific preparedness capability shortfall as identified through risk assessments and preparedness reports.

As noted earlier, additional controls relating to the purchase and use of cell site simulators are stipulated in FEMA policy and in the terms and conditions outlined in the grant award documents. DHS identifies categories of allowable equipment under FEMA Preparedness Grant programs in the Authorized Equipment List (AEL). Policy related to this type of equipment is provided in the AEL in the Grant Notes Section. The policy specifically states that use of such equipment is subject to the prohibitions contained in Title III of the Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. This is in addition to the assurances that all grant recipients execute a term and condition of their awards, including assured compliance with all applicable federal laws, executive orders, and regulations. While not specific to cell-site simulators, the scope of these assurances prohibits grantee conduct that violates the Fourth Amendment or any provision of the Constitution of the United States and all other applicable federal laws.

DHS acknowledges that policies for use and training for law enforcement personnel who seek to acquire cell-cite simulator technology through FEMA's preparedness grant programs could further safeguard privacy and civil liberties protections. DHS will further examine whether grantee adoption of baseline policy provisions, including training requirements, should be mandated as a condition of purchase through FEMA's preparedness grant programs, and if so, how any necessary training can most effectively be delivered.

Question#:	8
Topic:	Training
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: With respect to grants to state and local law enforcement relating to IMSI catchers, what, if anything, does DHS do to ensure that the grant recipients require that officers receive training on how to use the devices properly, whether technical, legal, or other training?

Response: FEMA policy and the terms and conditions outlined in the grant award documents stipulate controls relating to the purchase and use of cell site simulators. DHS identifies categories of allowable equipment under FEMA Preparedness Grant programs in the AEL. Policy related to this type of equipment is provided in the AEL in the Grant Notes Section. The policy specifically states that use of such equipment is subject to the prohibitions contained in Title III of the Omnibus Crime and Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. This is in addition to the assurances that all grant recipients execute a term and condition of their awards, including assured compliance with all applicable federal laws, executive orders, and regulations. While not specific to cell-site simulators, the scope of this assurance prohibits grantee conduct that violates the Fourth Amendment or any provision of the Constitution of the United States and all other applicable federal laws.

As noted above, DHS acknowledges that policies for use and training for law enforcement personnel who seek to acquire cell-cite simulator technology through FEMA's preparedness grant programs could further safeguard privacy and civil liberties protections. DHS will further examine whether grantee adoption of baseline policy provisions, including training requirements, should be mandated as a condition of purchase through FEMA's preparedness grant programs, and if so, how any necessary training can most effectively be delivered.

Question#:	9
Topic:	CBP Use
Hearing:	Examining Law Enforcement Use of Cell Phone Tracking Devices
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Does DHS' new policy governing IMSI catchers cover Customs and Border Protection's (CBP) use of the devices during each of CBP's missions along the U.S. borders? In other words, will CBP rely on the "border exception" to the Fourth Amendment?

Response: The DHS policy applies to all DHS Components. CBP does not currently use cell-site simulator technology. In the event that CBP does use cell-site simulator technology in the future, the DHS policy will apply to CBP's use of the technology.