

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1328989-0

Total Deleted Page(s) = 13

- Page 8 ~ b5; b7E;
- Page 9 ~ b5; b7E;
- Page 10 ~ b5; b7E;
- Page 11 ~ b5; b7E;
- Page 12 ~ b5; b7E;
- Page 13 ~ b5; b7E;
- Page 14 ~ b5; b7E;
- Page 15 ~ b5; b6; b7C; b7E;
- Page 16 ~ b5; b7E;
- Page 17 ~ b5; b7E;
- Page 18 ~ b5; b7E;
- Page 19 ~ b5; b7E;
- Page 20 ~ b5; b7E;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

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 ACCOUNTABILITY²

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 Division⁵ 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(e).

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 prosecutors⁶ 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., trademark, 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 retention⁸ 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.