



# Use of Cell-Site Simulator Technology

Office of Privacy and Civil Liberties

[privacy@usdoj.gov](mailto:privacy@usdoj.gov)

2016



# Use of Cell-Site Simulator Technology

## Table of Contents

- I. DOJ Policy “Use of Cell-Site Simulator Technology”
- II. Other Laws & Policies
- III. Privacy Best Practices
- IV. DOJ Privacy Resources



# I. DOJ Policy

## Collection Limitations

Warrant & Order Required – Prior to using cell-site simulator technology, law enforcement agencies must obtain:

- (1) A search warrant supported by probable cause; AND
- (2) An order pursuant to the Pen Register Statute (18 U.S.C. § 3121, *et seq.*)

Exceptions:

- Exigent Circumstances under the Fourth Amendment; OR
- Exceptional Circumstances Where the Law Does Not Require a Warrant.



# I. DOJ Policy

## Collection Limitations cont.

Pen Register Configuration – Cell-site simulator technology 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).

The following collection categories are prohibited:

- GPS/location information from the device;
- Data contained on the phone itself (e.g., emails, texts, contact lists); AND
- Subscriber account information.





# I. DOJ Policy

## Notice & Transparency

Application for Use of Cell-Site Simulator Technology – Applications for the use of cell-site simulator technology must include sufficient information to ensure that courts are aware that the technology will be used and how it will be used.

Content of Application:

- The technique to be employed, in general terms;
- The location(s) and time(s) the device will be used;
- The possible, temporary disruption of service to target and surrounding devices; AND
- The deletion and prohibited use of data not associated with the target phone.



# I. DOJ Policy

## Use Limitations

Investigative Use Of Non-Target Data Is Prohibited – Agencies are prohibited from making affirmative investigative use of any non-target data.

Exception:

- By order of the court; OR
- To identify and distinguish the target device from other devices.

Limit Use Of Information As Stated in Application – Agencies must ensure that cell-site simulator technology is not otherwise used in a manner inconsistent with the filed application.



# I. DOJ Policy

## Retention Limitation & Disposal

Consistent with applicable laws and requirements, agencies must ensure that information collected using cell-site simulator technology is retained in accordance with the following practices:

Investigation	Deletion Policy
Used to locate a <u>known</u> cellular device	<ul style="list-style-type: none"><li>• All data deleted as soon as that device is located; BUT</li><li>• In any event, <u>no less than once daily</u>.</li></ul>
Used to identify an <u>unknown</u> cellular device	<ul style="list-style-type: none"><li>• All data deleted as soon as target cellular device is identified; BUT</li><li>• In any event, <u>no less than once every 30 days</u>.</li></ul>
Used as part of a new mission	<ul style="list-style-type: none"><li>• Must verify that equipment has been cleared of any previous operational data from any completed operation prior to new mission.</li></ul>





## II. Other Laws & Policies

### General Overview

- Cell-site data must also be collected, used, and retained consistent with applicable existing laws and requirements.
- It is important to note that other legal and policy requirements may apply in addition to, and distinct from, the DOJ Policy. For example:
  - Duty to Preserve Exculpatory Evidence;
  - Pen Register Statute (18 U.S.C. § 3121, *et seq.*); AND
  - **The Privacy Act of 1974 (5 U.S.C. § 552a).**





## II. Other Laws & Policies

### The Privacy Act of 1974

- The requirements of the Privacy Act generally apply to “records” maintained in a “system of records.”
  - “record” -- “any item, collection, or grouping of information about an individual that is maintained by an agency . . . that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual . . . .”
  - “system of records” -- “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”
    - NOTE: “Capability” to retrieve alone does not trigger the protections of the Privacy Act



## II. Other Laws & Policies

### The Privacy Act of 1974 cont.

- If information obtained through a cell-site simulator becomes part of a Privacy Act-protected record maintained in a system of records, agencies must ensure that a published System of Records Notice (SORN) exists.
- Example: “Investigative Reporting and Filing System” (JUSTICE/DEA-008) (77 FR 21808)
  - CATEGORIES OF RECORDS IN THE SYSTEM: “The system contains law enforcement intelligence and investigative information . . . compiled for the purpose of identifying criminal, civil, and regulatory offenders; reports of investigations”
  - PURPOSE(S): “The purpose of this system is to enforce the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, its implementing regulations, and related statutes.”



## II. Other Laws & Policies

General Takeaway: Depending on the collection, use, maintenance, and/or dissemination of information retrieved by cell-site simulator technology, **other legal requirements may apply.**

**Always work with your general counsel and OPCL when collecting information that may be personally identifiable.**





## III. Privacy Best Practices

1. Always insure that the proper court order has been obtained prior to the deployment of cell-site devices.
2. Adhere to the jurisdictional parameters authorized by the court order.
3. Minimize the footprint of the device by focusing on the individual cellular protocol used by the target, if known.
4. Coordinate with the case agents to narrow the number of times/locations cell-site simulator technology will be used in order to minimize the collection of non-target data.
5. Always protect data collected by cell-site devices to ensure that no affirmative investigative use will be made of non-target data, except to identify and distinguish the target device from other devices, or otherwise directed by court order.





## III. Privacy Best Practices

6. Limit the exposure of data collected by cell-site devices to only those who are required to determine the relevance of such information.
7. Make efforts to examine data collected as quickly as possible to determine what information is relevant.
8. Immediately delete all data once the objective of the collection is accomplished, (e.g., numbers relevant to identifying the target device(s) or otherwise believed to be relevant to the investigation have been determined).
9. Work with your prosecutor, general counsel, and OPCL attorneys to ensure that collection and use of information from cell-site simulator technology is conducted in accordance with all applicable laws and Department requirements.



## IV. Privacy Resources

### DOJ Order 0601 “Privacy & Civil Liberties” (2014)

- Sets forth roles and responsibilities of the DOJ’s Chief Privacy and Civil Liberties Officer (CPCLO), the Office of Privacy and Civil Liberties (OPCL), Heads of Components, and Senior Component Officials for Privacy (SCOPs) regarding privacy and civil liberties.

### DOJ Office of Privacy & Civil Liberties

Website: <http://www.justice.gov/opcl>

IntraNet: <http://dojnet.doj.gov/privacy/>

Resources: <http://www.justice.gov/opcl/resources>

Contact: [privacy@usdoj.gov](mailto:privacy@usdoj.gov)

For Component-level privacy questions, reach out to your  
Senior Component Official for Privacy



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

December 18, 2015

The Honorable Elijah E. Cummings  
Ranking Member  
Committee on Oversight and Government Reform  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Cummings:

This responds to your letter to the Attorney General dated April 24, 2015, concerning cell-site simulator technologies. This letter supplements briefings, document reviews, demonstrations, conference calls, and discussions with the Committee on Oversight and Government Reform (the Committee) staff on this topic, as well as a hearing in which the Department of Justice (Department) participated on October 21, 2015. We have appreciated the opportunity to work with the Committee on this important issue. We are sending identical responses to the other Members, who joined in your letter and apologize for our delay in responding.

As we have previously discussed with the Committee, cell-site simulator technology is a critical tool utilized by the Department's law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigations (FBI); and the United States Marshals Service (USMS). This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, we advised the Committee regarding the enclosed new Departmental policy (policy) for its use of cell-site simulators. The Department also provided a briefing of the new policy to Committee staff on September 18, 2015. This policy, which applies



The Honorable Elijah E. Cummings

Page Two

Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations and establishes new management controls for the use of the technology. The policy enhances transparency and accountability, improves training and supervision, establishes a higher and more consistent legal standard, and increases privacy protections in relation to law enforcement's use of this critical technology. Further, the policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties.

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

The Department has appreciated the opportunity to work with Committee staff to provide information in response to the enumerated questions in your April 24<sup>th</sup> letter. During the spring of 2015, ATF, DEA, FBI, and USMS each provided extensive law enforcement sensitive briefings to the Committee on this topic, as well as in-camera reviews of component-specific policies as requested. Additionally, in May and July, ATF provided demonstrations of cell-site technology to Committee staff. These briefings, document reviews, demonstrations, and discussions provided the Committee with the requested information about certain sensitive law enforcement tools and techniques while avoiding making public specific details about sensitive equipment and techniques that may be deployed in furtherance of law enforcement missions. In response to follow-up questions from Committee staff, ATF, DEA, FBI, and USMS, as well as this office, have provided additional responses and information in conference calls and written communications. Finally, as you are aware, on October 21, 2015, Elana Tyrangiel, Principal Deputy Assistant Attorney General for the Office of Legal Policy, testified before the Committee regarding cell-site simulator technologies and policies. We are in the process of responding to written hearing Questions for the Record, which will be submitted upon completion.



The Honorable Elijah E. Cummings  
Page Three

In summary, we hope this information has been helpful and believe that the above noted efforts to provide information to the Committee respond fully to your April 24, 2015 letter. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik  
Assistant Attorney General

Enclosure

cc: The Honorable Harold Rogers  
Chairman  
Committee on Appropriations

The Honorable Nita M. Lowey  
Ranking Member  
Committee on Appropriations

The Honorable John Culberson  
Chairman  
Subcommittee on Commerce, Justice,  
Science, and Related Agencies  
Committee on Appropriations

The Honorable Mike Honda  
Ranking Member  
Subcommittee on Commerce, Justice,  
Science, and Related Agencies  
Committee on Appropriations



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

December 18, 2015

The Honorable Jason Chaffetz  
Chairman  
Committee on Oversight and Government Reform  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

This responds to your letter to the Attorney General dated April 24, 2015, concerning cell-site simulator technologies. This letter supplements briefings, document reviews, demonstrations, conference calls, and discussions with the Committee on Oversight and Government Reform (the Committee) staff on this topic, as well as a hearing in which the Department of Justice (Department) participated on October 21, 2015. We have appreciated the opportunity to work with the Committee on this important issue. We are sending identical responses to the other Members, who joined in your letter and apologize for our delay in responding.

As we have previously discussed with the Committee, cell-site simulator technology is a critical tool utilized by the Department's law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigations (FBI); and the United States Marshals Service (USMS). This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, we advised the Committee regarding the enclosed new Departmental policy (policy) for its use of cell-site simulators. The Department also provided a briefing of the new policy to Committee staff on September 18, 2015. This policy, which applies



Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations and establishes new management controls for the use of the technology. The policy enhances transparency and accountability, improves training and supervision, establishes a higher and more consistent legal standard, and increases privacy protections in relation to law enforcement's use of this critical technology. Further, the policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties.

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

The Department has appreciated the opportunity to work with Committee staff to provide information in response to the enumerated questions in your April 24<sup>th</sup> letter. During the spring of 2015, ATF, DEA, FBI, and USMS each provided extensive law enforcement sensitive briefings to the Committee on this topic, as well as in-camera reviews of component-specific policies as requested. Additionally, in May and July, ATF provided demonstrations of cell-site technology to Committee staff. These briefings, document reviews, demonstrations, and discussions provided the Committee with the requested information about certain sensitive law enforcement tools and techniques while avoiding making public specific details about sensitive equipment and techniques that may be deployed in furtherance of law enforcement missions. In response to follow-up questions from Committee staff, ATF, DEA, FBI, and USMS, as well as this office, have provided additional responses and information in conference calls and written communications. Finally, as you are aware, on October 21, 2015, Elana Tyrangiel, Principal Deputy Assistant Attorney General for the Office of Legal Policy, testified before the Committee regarding cell-site simulator technologies and policies. We are in the process of responding to written hearing Questions for the Record, which will be submitted upon completion.

The Honorable Jason Chaffetz  
Page Three

In summary, we hope this information has been helpful and believe that the above noted efforts to provide information to the Committee respond fully to your April 24, 2015 letter. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Peter J. Kadzik  
Assistant Attorney General

Enclosure

cc: The Honorable Harold Rogers  
Chairman  
Committee on Appropriations

The Honorable Nita M. Lowey  
Ranking Member  
Committee on Appropriations

The Honorable John Culberson  
Chairman  
Subcommittee on Commerce, Justice,  
Science, and Related Agencies  
Committee on Appropriations

The Honorable Mike Honda  
Ranking Member  
Subcommittee on Commerce, Justice,  
Science, and Related Agencies  
Committee on Appropriations





**U.S. Department of Justice**

**Office of Legislative Affairs**

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

October 6, 2015

The Honorable Jon Tester  
United States Senate  
Washington, DC 20510

Dear Senator Tester:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

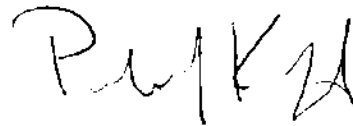
On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties.

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik". The signature is written in a cursive, somewhat stylized font.

Peter J. Kadzik  
Assistant Attorney General

Enclosure



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

October 6, 2015

The Honorable Bernard Sanders  
United States Senate  
Washington, DC 20510

Dear Senator Sanders:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties



The Honorable Bernard Sanders  
Page Two

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik". The signature is written in a cursive, somewhat stylized font.

Peter J. Kadzik  
Assistant Attorney General

Enclosure



**U.S. Department of Justice**

**Office of Legislative Affairs**

Office of the Assistant Attorney General

*Washington, D.C. 20530*

October 6, 2015

The Honorable Tammy Baldwin  
United States Senate  
Washington, DC 20510

Dear Senator Baldwin:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik". The signature is fluid and cursive, with the first name "Peter" being the most prominent part.

Peter J. Kadzik  
Assistant Attorney General

Enclosure





U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 6, 2015

The Honorable John Walsh  
United States Senate  
Washington, DC 20510

Dear Senator Walsh:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties

The Honorable John Walsh  
Page Two

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Peter J. Kadzik', written in a cursive style.

Peter J. Kadzik  
Assistant Attorney General

Enclosure



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

October 6, 2015

The Honorable Tom Udall  
United States Senate  
Washington, DC 20510

Dear Senator Udall:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties

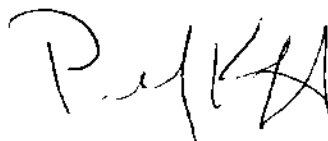


While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik". The signature is stylized and somewhat cursive.

Peter J. Kadzik  
Assistant Attorney General

Enclosure



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 6, 2015

The Honorable Christopher Coons  
United States Senate  
Washington, DC 20510

Dear Senator Coons:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.


Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,  


Peter J. Kadzik  
Assistant Attorney General

Enclosure





**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

October 6, 2015

The Honorable Jeff Merkley  
United States Senate  
Washington, DC 20510

Dear Senator Merkley:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties

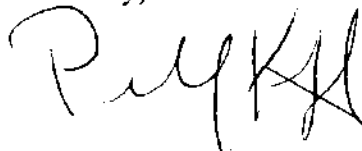
The Honorable Jeff Merkley  
Page Two

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter J. Kadzik". The signature is stylized and cursive.

Peter J. Kadzik  
Assistant Attorney General

Enclosure



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 6, 2015

The Honorable Martin Heinrich  
United States Senate  
Washington, DC 20510

Dear Senator Heinrich:

This responds to your letter to former Attorney General Eric H. Holder, Jr., and Department of Homeland Security Secretary Jeh Johnson, dated December 9, 2014, concerning the use of cell-site simulator technologies. We are sending identical responses to the other Senators, who joined in your letter, and apologize for our delay in responding. We understand the Department of Homeland Security responded to your letter under separate cover.

Cell-site simulator technology is a critical tool utilized by the Department of Justice's (the Department) law enforcement components: the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. This technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations, and complicated narcotics cases. The cell-site simulator devices are one tool among many traditional law enforcement techniques, and are only deployed in the fraction of cases in which the capability is best suited to achieve specific public safety objectives. Law enforcement agencies 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. Any potential service disruption to non-target devices would be temporary and all operations are conducted to ensure the minimal amount of interference to non-target devices.

On September 3, 2015, the Department announced a new policy (policy) for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this critical technology. A copy of the policy is enclosed with this letter. The policy, which applies Department-wide, provides Department components with standard guidance for the use of cell-site simulators in the Department's domestic criminal investigations, and establishes new management controls for the use of the technology. The policy ensures the Department's protocols for this technology are consistent, well-managed, and respectful of individuals' privacy and civil liberties.



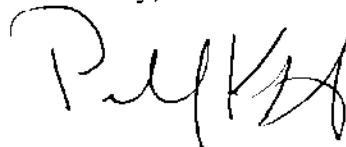
The Honorable Martin Heinrich  
Page Two

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, 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. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Peter J. Kadzik', written in a cursive style.

Peter J. Kadzik  
Assistant Attorney General

Enclosure