

## General Rule - Warrants

- Warrantless searches & seizures generally are presumed to be unreasonable unless a reasonable exception applies  
Requirements: Probable Cause  
Particularity



## Warrants & Electronic Devices

- Scope  
Particularity  
Retention  
Time limits



## Exceptions to Warrants But PC Still Needed

- Arrest in a Public Place  
Plain View  
Lawful presence/access  
Probable cause to seize is immediately apparent  
Exigent Circumstances  
Mobile Conveyances



## Exceptions – Warrant & PC

- Protective Sweep  
Regulatory  
Stop/Frisk Inventory Administrative  
Search Incident to  
Arrest Consent Border Search



## Search Incident to Arrest

- Purpose: To prevent arrestee's access to weapons or destruction/concealment of evidence  
Scope: Exterior of arrestee's clothing; Objects carried by arrestee; Area within arrestee's immediate control; Strip Search – Reasonable Suspicion articles are concealed beneath clothing  
No cell phones



## *Riley v. California*

- *Wurie (First Circuit) Limited search of a flip phone Categorical rule against SIA*  
*Riley (California) Two searches of a smart phone Categorical rule for SIA of device found on person*  
*S.Ct. – Categorical rule against SIA of cell phones Qualitatively and quantitatively different Other exception may be ok, including border search*



## Consent

Voluntary from a Totality of the  
Circumstances Knowledge of rights, Written  
consent, Presence of witnesses Age and  
sophistication, Authority to consent  
Authority to Consent: Actual: Person with  
REP in thing/place to be searched Apparent:  
Person who appears to have REP



# ICE

# Consent and Electronic Devices

Ambiguity of authority  
Scope  
Revocation  
Answering calls



U.S. Immigration  
and Customs  
Enforcement



## Border Search Exception

- *General Rule: Searches & seizures must be conducted with a warrant supported by probable cause*  
*Exception: Border searches*  
*No warrant needed*  
*No probable cause needed*  
*NOT exempt from reasonableness requirement of the Fourth Amendment*



## Border Search

- Purpose Protect nation's bordersProtect revenueProhibit importation or exportation of merchandise contrary to lawScope MerchandiseEvidence related to merchandise



## Elements

- Customs Officer  
Searching for merchandise or evidence relating to merchandise  
At the Border includes Functional Equivalent of the Border (FEB) includes Extended Border (EB)



## Customs Officer

- ICE Special Agents  
CBP officers  
Coast Guard officers -commissioned,  
warrant, or petty officer  
Others formally designated by ICE or  
CBP (other Fed, State, local, or  
foreign LEOs who go through formal  
cross-designation training)



## Merchandise

- Goods, wares & chattels of every description, including:
  - Prohibited items - contraband
  - Monetary instruments
  - Intellectual property – trade secrets, copyrighted material
  - Merchandise or evidence relating to merchandise
- Merchandise is not:
  - General evidence of criminality
  - Intelligence
  - Exclusively correspondence



## At the Border

- What is “the Border”?  
Territorial Limits of the United States  
Land, Air, Marine  
Border  
Functional Equivalent of the Border  
Extended Border



## Functional Equivalent of the Border (FEB)

- Reasonable certainty of border nexus  
Crossing or contact with something or someone that has crossed/will cross  
Reasonable certainty of no material change – and  
First practicable detention point or... last practicable detention point (for outbound searches)



## Extended Border (EB)

- Reasonable certainty of border nexus  
Crossing or contact with something or someone that has crossed  
Reasonable certainty of no material change – and  
Reasonable suspicion of criminal activity





## Landmark Cases

- General – U.S. v. Ramsey, 1977  
People – U.S. v. Montoya de Hernandez, 1985  
Objects – U.S. v. Flores-Montano, 2004



## Landmark Cases - Electronic Devices

- *U.S. v. Ickes* (4th Cir. 2005) *U.S. v. Arnold* (9th Cir. 2008) *U.S. v. Cotterman* (9th Cir. 2013) *Riley v. California* (U.S. 2014) \*\* *U.S. v. Saboonchi* (D. Md. 2014) *U.S. v. Kim* (D.D.C. 2015)



## *U.S. v. Ickes*

- Searching contents of a laptop at border is categorically a routine border search Specifically applied Flores-Montano to computer searches No level of suspicion needed



## *U.S. v. Arnold*

- D. Ct. - Non-routine border search & requires RS  
Implicates dignity & privacy interests  
Likened to inner most recesses of human mind  
Reversed by 9th Circuit panel  
Laptop is merchandise; requires no heightened level of suspicion for border search  
Followed Flores-Montano  
En Banc denied, Cert. denied.



## *U.S. v. Cotterman*

- D. Ariz. - Movement to ICE lab considered 2nd search requiring reasonable suspicion under EB doctrine  
Court of Appeals (Round 1) – Not an extended border search, no reasonable suspicion necessary and search itself was reasonable En Banc 2013 – Forensic searches require reasonable suspicion. Reasonable suspicion was present here.



## *Post-Cotterman Issues*

What is a forensic search? The “in the alternative” reasonable suspicion argument. The “stop and get a warrant” approach. Detention pretextual Eroding authority Probable cause vs. Cotterman reasonable suspicion



## *U.S. v. Saboonchi*

- IEEPA & ITSR charges  
Not an extended border search just because examined away from the border  
Forensic search requires reasonable suspicion  
Forensic search = creation of a bitstream copy + analysis by special software



## *Post-Riley Issues*

Cell phone  $\neq$  any other container  
What if traveler is arrested?

Expansion of Riley to other warrant exceptions





## *U.S. v. Kim*

- IIEPA & AECA & ITSR charges  
Search done entirely in Ninth Circuit  
Search limited to allocated space  
only  
Holding: Reasonable suspicion for past criminal activity is not sufficient  
Degree to which search intruded on privacy outweighed need for promotion of legitimate governmental interests (outbound v. inbound)  
Limited to “unique circumstances of this case”



## Injunctive Relief & the ACLU

- *Abidor v. Napolitano, E.D.N.Y. House v. Napolitano, D. Mass*



## DHS Policies

- Congressional Interest Timeframes
- Training Supervisory Review
- Reasonable Suspicion



## DHS Policies (cont.)

- 2009 Policies Privacy Impact Assessment Civil Rights and Civil Liberties Impact Assessment Coordination between CBP & ICE policies Publicly available



## Levels of Suspicion

- Search No suspicion necessary  
Assistance Technical Assistance  
Subject Matter Assistance



## Timeframes

- Reasonable Period of Time Assistance



# ICE

## Sharing

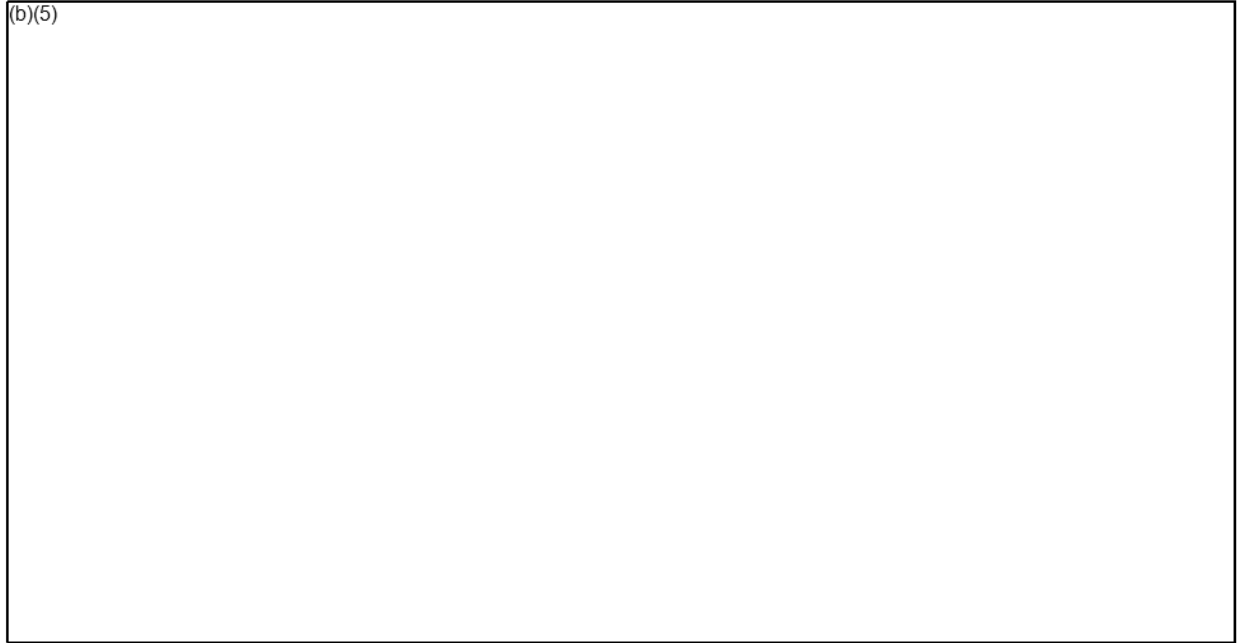
(b)(5)



U.S. Immigration  
and Customs  
Enforcement

## Remotely Stored Information

● (b)(5)





## Fifth Amendment & Electronic Devices

- (b)(5)



## Fifth Amendment & Electronic Devices (cont.)

- (b)(5)



## Electronic Communications Privacy Act

- Electronic Communications Privacy Act of 1986 (“ECPA”) is comprised of the Stored Communications Act, the Pen Register Statute, and amendments to the Wiretap Act. Controls the collection and disclosure of content and non-content information related to electronic communications, as well as content that has been stored remotely.



## Electronic Communications Privacy Act

- Title I of ECPA – Wiretap Act  
Title II of ECPA – Stored Communications Act  
Title III of ECPA – Pen register and trap and trace devices



## Title I – Wiretap Act

- Electronic Communications Act (ECA) approval: Any federal felony Wire or Oral Communications Act (WOCA) Attorney General approval: Predicate offenses (18 U.S.C. 2516)



## Title II – Stored Communications Act

- (b)(5)



## Title III – Pen Register and Trap and Trace Devices

(b)(5)

- 



## Cell Phone Location Data

- (b)(5)





## Title III – Penalties

- Suppression (18 USC § 2515) Criminal – fines & jail (18 USC § 2511(4) & (5)) Civil: Compensatory and punitive damages Attorneys fees Against individual or agency 18 USC § 2520



**From:**

(b)(6); (b)(7)(C)

**Sent:**

20 May 2016 18:38:43 +0000

**To:**

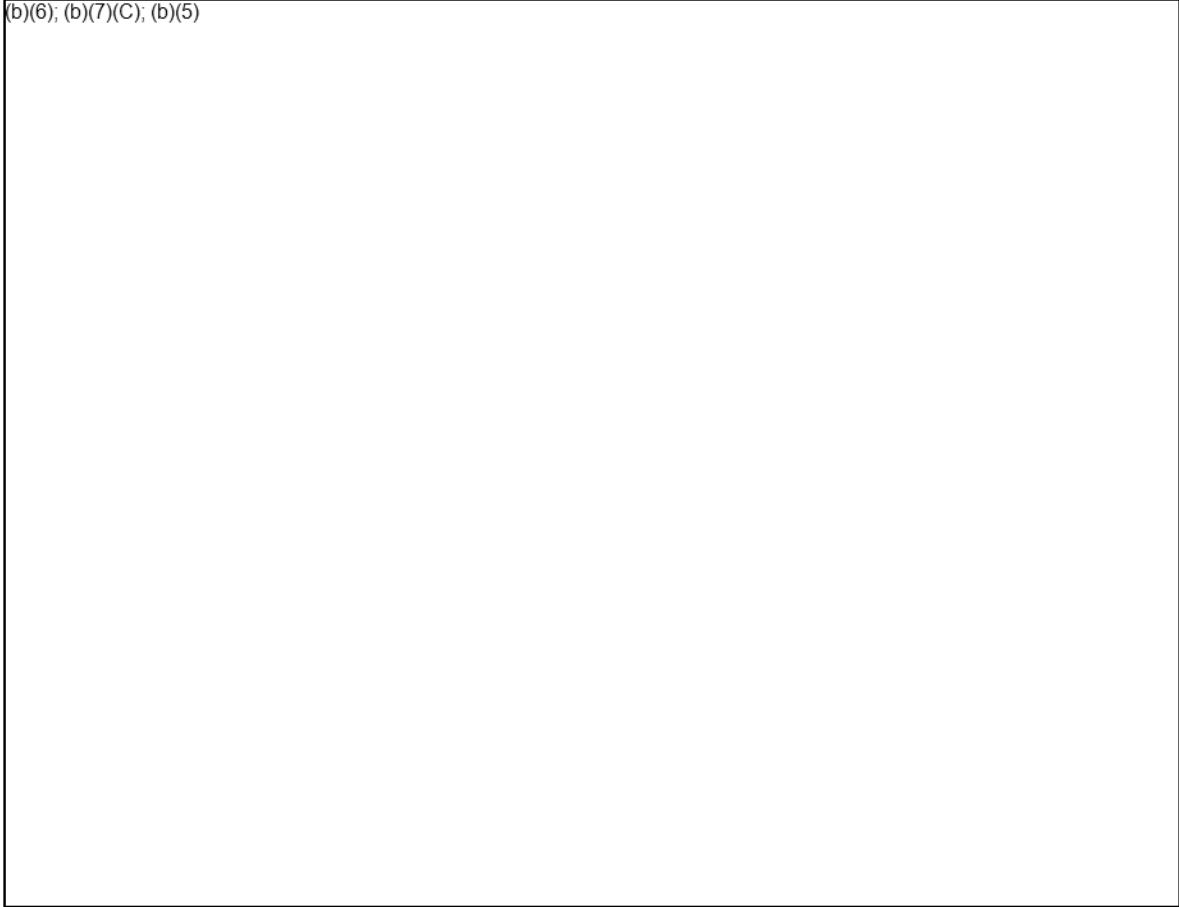
(b)(6); (b)(7)(C)

**Subject:**

Border Search suppression motions

Team,

(b)(6); (b)(7)(C); (b)(5)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 13 Aug 2016 10:16:29 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** (b)(6); (b)(7)(C) defense motions re search warrants

Good morning,

Judge Bredar denied the motion to suppress the border search on Thursday August 11, 2016. Not sure if he will issue an opinion.

(b)(6);  
(b)(7)(C)

Sent with Good (www.good.com)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:19:07 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Re: (b)(6); (b)(7)(C) defense motions re search warrants

Oh, got it. With other border search issues, DOJ's National Security Division has gotten involved. I wasn't sure if they were reviewing here as well. I'll get you our comments (with input from CBP OCC) by tomorrow morning. Sorry for the delay.

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk  
202-536-(b)(6); (b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:18 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6); (b)(7)(C)

(b)(5)

Thanks,

(b)(6);  
(b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, May 18, 2016 4:14 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6); (b)(7)(C)

(b)(5)

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732- (b)(6); (b)(7)(C) (Desk)  
202-536- (b)(6); (b)(7)(C) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 4:01 PM

**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6);  
(b)(7)(C)

I would appreciate the brief and holding in Kolsuz.

Thanks,

(b)(6);  
(b)(7)(C)

(b)(6); (b)(7)(C)

Assistant United States Attorney  
United States Attorney's Office, District of Maryland/36 S. Charles Street, Fourth Floor/Baltimore, MD 21201  
(desk) 410-209-4606/(cell) 410-908-6006 (fax) 410-962-3091  
[Ayn.Ducao@usdoj.gov](mailto:Ayn.Ducao@usdoj.gov)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 3:57 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(5)

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-6006 (b)(6); (b)(7)(C) Desk)  
202-536-6006 (b)(6); (b)(7)(C) Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE~~

ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 3:23 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6); (b)(7)(C); (b)(5)

(b)(6);  
(b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 1:55 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

Thank (b)(6); (b)(7)(C) - please let us know what we can do to help with the reply brief.

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (Desk)  
202-536-(b)(7)(C) (Cell)

\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 12:10 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(6);  
(b)(7)(C) just reached out to me on this, so I don't know if the AUSA has drafted her  
reply. (b)(6); (b)(7)(C) copied on this email and can fill us in.

Sent with Good ([www.good.com](http://www.good.com))

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 12:02:43 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

Thank (b)(6); (b)(7)(C) Did you already reach out to the AUSA? Can I contact (b)(6); (b)(7)(C) directly (or can you put me in touch with her) so that we can review the draft responses?

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) (Desk)  
202-536-(b)(6); (b)(7)(C) (Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, May 16, 2016 11:33 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: (b)(6); (b)(7)(C) defense motions re search warrants

(b)(5); (b)(7)(E)

Sent with Good ([www.good.com](http://www.good.com))

(b)(6); (b)(7)(C)  
**From:** [redacted]  
**Sent:** Monday, May 16, 2016 11:16:52 AM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: (b)(6); (b)(7)(C) defense motions re search warrants

Sorry I didn't send this early. I've been so unbelievably busy.

-----Original Message-----

From: (b)(6); (b)(7)(C)  
Sent: Monday, May 09, 2016 12:48 PM  
To: (b)(6); (b)(7)(C)  
Subject: (b)(6); (b)(7)(C) defense motions re search warrants  
(b)(6); (b)(7)(C)

Attached are the defense motions that we discussed this morning.

Thanks,


(b)(6); (b)(7)(C)



**ICE**  
Title III  
Training

**Electronic  
Surveillance**

(b)(6); (b)(7)(C)  
Criminal Law Section  
October 2018



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Introduction to  
Electronic Surveillance**

- (b)(5)



---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Introduction to  
Electronic Surveillance**

- (b)(5)
- 



---

---

---

---

---

---


---

---

**ICE**

Title III  
Training

TITLE III BACKGROUND AND  
STATUTORY AUTHORITY




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Statutory History of TIII**

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Wiretap Act”)
- Electronic Communications Privacy Act of 1986 (ECPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)




---

---

---

---

---

---

---


---

**ICE**

Title III  
Training

**Statutory Authority**

- Interception of Communications (Title III) – 18 U.S.C. §§ 2510-2522
- Stored Wire and Electronic Communications and Transactional Records Access – 18 U.S.C. §§ 2701-2711 (Part of the ECPA)
- Pen Registers and Trap and Trace Devices – 18 U.S.C. §§ 3121-3127




---

---

---

---

---

---

---


---

**ICE**  
 Title III  
 Training

**Title III –  
 18 U.S.C. §§ 2510-2522**

Live Communications

- 2510 – Definitions
- 2511 – Unlawful to Intercept & Disclose
- 2516 – Authorization for Interception
- 2517 – Authorization for Disclosure
- 2520 – Civil Action




---

---

---

---

---

---


---

---

**ICE**  
 Title III  
 Training

**Title III – 18 U.S.C. § 2516**

- Court authorization required for:
  - Interception, disclosure, or use
  - Of content
  - Of any wire, oral, or electronic communication




---

---

---

---

---

---


---

---

**ICE**  
 Title III  
 Training

**Title III – 18 U.S.C. § 2510**

- Intercept
- Device
- Wire Communication
- Oral Communication
- Electronic Communication




---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definitions – Intercept

A communication is 'intercepted' if a device is used by a third party to acquire any information concerning the substance, purport or meaning (i.e., the "content") of that communication.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definitions – Device

- A 'device' is anything that does the job of acquiring the content of any wire, oral, or electronic communication.
- Some devices are specifically excluded
  - Hearing Aids

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Wire Communication

- Any communication
- the human voice travels
- in whole or part
- by means of a wire, cable, or other like connection provided by a communications facility
- interstate or foreign commerce.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Oral Communication

- Any speaking
- other than a wire or electronic communication
- in which the speaker exhibits a reasonable expectation of privacy in that speaking.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Definition – Electronic Communication

- Any communication
- other than a wire or oral communication
- in which anything is transmitted
- in whole or in part
- by a wire, radio, electromagnetic, photo-electronic or photo-optical system
- affecting interstate or foreign commerce.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Authorization Rules

### Electronic

- AUSA may approve
- May be made in connection with any federal felony investigation

### Wire/Oral

- Requires AG approval
- May be made only in connection with investigations of certain predicate offenses

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Predicate Offenses**

- 18 USC § 115 (Retaliation Against a Federal Official)
- 18 USC § 659 (Theft from Interstate Shipment)
- 18 USC § 1963 (RICO)
- 18 USC §§ 2251-52 (Sexual Exploitation of Children)
- 18 USC § 201 (Bribery of a Public Official)
- 18 USC §§ 1956-57 (Money Laundering)
- 18 USC § 2332d (Financial Transactions with Certain Governments)
- 22 USC § 2778 (AECA)
- 31 USC 5322 (Monetary Instruments Reporting)
- Any Drug Importation
- Conspiracy to Violate any of these statutes

---

---

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Disclosure & Use by ICE**

Lawfully obtained – Disclosure by ICE (sharing)

- Communications & “other offense evidence” to other agents for criminal investigative purposes
- Communications during testimony / oath
- Foreign intelligence info to other LEOs for official purposes

Lawfully obtained – Use by ICE

- Contents for criminal investigative purposes
- “Other offense evidence”

---

---

---

---

---

---

---

---

---

---

**ICE**

**Title III Training**

U.S. Immigration and Customs Enforcement

**Title III – Penalties**

- Suppression (18 USC § 2515)
- Criminal – fines & jail (18 USC § 2511(4) & (5))
- Civil:
  - Compensatory and punitive damages
  - Attorneys fees
  - Against individual or agency
  - 18 USC § 2520

---

---

---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Stored Communications  
and Records –  
18 U.S.C. §§ 2701-2712**

- (b)(5); (b)(7)(E)
- 
- 
- 




---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Pen Registers / Trap and  
Trace –  
18 U.S.C. §§ 3121-3127**

- (b)(5); (b)(7)(E)
- 




---

---

---

---

---

---


---

---

**ICE**  
Title III  
Training

**Stingray/Trigger Fish  
Devices**

- Determines location of cellular telephone
- Assists in identifying user of cellular telephone
- Obtain search warrant




---

---

---

---

---

---


---

---

**ICE**

Title III Training

**TECHNICAL OPERATIONS' ROLE IN TITLE III PROCESS**




---

---

---

---

---

---

---


---

**ICE**

Title III Training

**Technical Operations**

- The mission of ICE Technical Operations is to provide the field agents (ICE-Wide) with the most innovative cutting edge electronic surveillance equipment and support in furtherance of ICE investigations and national security operations.
- Manages all technical surveillance national initiatives
- Research and development of emerging technologies
- Develop ICE technical surveillance policy and procedures
- Oversee the procurement of all ICE technical surveillance equipment




---

---

---

---

---

---

---


---

**ICE**

Title III Training

**Title III Program**

- Located within Operational Technology and Cyber, Technical Operations and Systems Development in Lorton, VA
- Technical Operations consists of HSI Special Agents, Technical Enforcement Officers, and Mission Support Specialists
- Annual budget of \$20+ million
  - Title III Monitor Contract
  - Telecommunications Intercept Fees




---

---

---

---

---

---

---

---



# ICE

Title III  
Training



## Title III Program

- Program established in 2002 creating a centralized point of contact
- Provide Support to Field Offices
  - Facilitate ELSUR Record Checks
  - Provide Go-Bys
  - Streamline the Title III Process
  - National Title III Monitor Contract

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Funding Requests

- Draft affidavit is submitted by HSI Special Agent to AUSA before the funding request is submitted.
- Funding request memo is submitted from SAC to the Executive Associate Director, HSI.
- The funding request is routed through HSI Domestic Operations to Technical Operations.
- The Technical Operations COTR requests a bid from ICE approved contract monitoring companies.
- Funding approval authority has been delegated to the Unit Chief, Technical Operations.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## OPLA TITLE III REVIEW PROCESS

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Affidavits

- SAC office sends affidavit to Technical Operations and DOJ Criminal Division, Office of Enforcement Operations (OEO) via the AUSA.
- Technical Operations sends affidavit to OPLA for legal sufficiency review as part of overall approval and funding process.
- OPLA reviews the affidavit for legal sufficiency and works directly with the HSI Special Agent to make necessary revisions.
- Once OPLA is satisfied that the affidavit is legally sufficient, the letter of legal sufficiency is sent to Technical Operations for processing.
- The HSI Special Agent ensures the final version of the affidavit is submitted to the court through the AUSA.

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Affidavit: Legal Sufficiency Review

- (b)(5); (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 

---

---

---

---

---

---

---

---

# ICE

Title III  
Training



## Title III Affidavit Review Probable Cause

- That "an individual is committing, has committed, or is about to commit a particular offense" AND
- That "particular communications concerning that offense will be obtained through such interception."

---

---

---

---

---

---

---


---

**ICE**  
Title III Training

**Title III Affidavit Review  
Probable Cause**

- Factors courts consider:
  - Type of crime
  - Length of criminal activity
  - Nature of object of search
  - Staleness

(b)(5); (b)(7)(E)




---

---

---

---

---

---


---

---

**ICE**  
Title III Training

**Title III Affidavit Review  
Necessity**

- Full and Complete Statement  
OR
- Minimum "other investigative procedures have been tried and failed; appear unlikely to succeed; or, are too dangerous"




---

---

---

---

---

---

---


---

**ICE**  
Title III Training

**California Wiretaps**

- Not Title III (CA statute)
- Less formal review process
- Less stringent probable cause requirement

(b)(5); (b)(7)(E)




---

---

---

---

---

---

---

---

**ICE**

Title III  
Training



### TIII – Emergency Interceptions

- Emergency situation
  - Purpose
  - Determination
- Process to obtain emergency TIII
  - Case agent/SAC
  - Coordination with AUSA and DOJ

---

---

---

---

---

---

---

---

**ICE**

Title III  
Training



### Resources

- What reference materials will I need?
- Submitting Affidavits to Tech Ops at HSI HQ
- Who are the CLS POCs?
  - [OPLA-CLS@ICE.DHS.GOV](mailto:OPLA-CLS@ICE.DHS.GOV)

---

---

---

---

---

---

---

---

**From:**

(b)(6); (b)(7)(C)

**Sent:**

2 Dec 2016 18:24:30 +0000

**To:**

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

**Cc:**

(b)(6); (b)(7)(C)

**Subject:**

7CTA case; U.S. v. Patrick

(b)(5)

[Redacted content]

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) (office)  
(202) 308- (C) (cell)

(b)(6); (b)(7)(C)



**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 18:45:41 +0000  
**To:** OPLA-CLS  
**Subject:** Accepted: Cell-Site Simulator Training to TechOps

**From:** (b)(6); (b)(7)(C)  
**Sent:** 26 Sep 2017 13:00:23 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** CSS doc  
**Attachments:** Cell-site simulator response - IMD TechOps IGP 092017.docx

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-733-(b)(6); (b)(7)(C) Desk)  
202-833-(b)(7)(C) Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~



~~LAW ENFORCEMENT SENSITIVE // FOR OFFICIAL USE ONLY~~

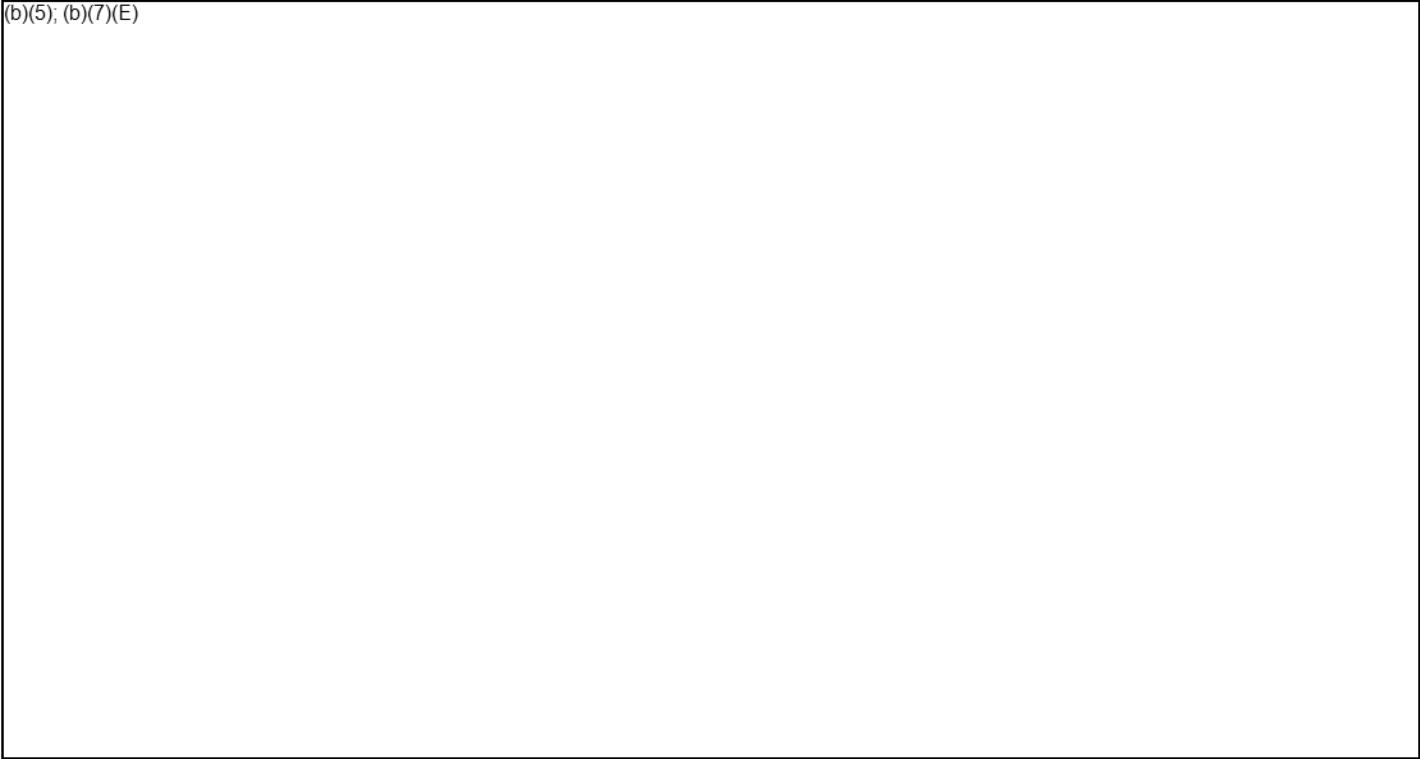
(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



September 2017



**Homeland  
Security**

October 19, 2015

**POLICY DIRECTIVE 047-02**

**MEMORANDUM FOR:** Sarah Saldaña  
Assistant Secretary  
U.S. Immigration and Customs Enforcement

Joseph Clancy  
Director  
United States Secret Service

R. Gil Kerlikowske  
Commissioner  
U.S. Customs and Border Protection

Admiral Paul F. Zukunft  
Commandant  
United States Coast Guard

Peter Neffenger  
Administrator  
Transportation Security Administration

L. Eric Patterson  
Director  
Federal Protective Service

**FROM:** Alejandro N. Mayorkas  
Deputy Secretary

A handwritten signature in black ink, appearing to read "AN Mayorkas", written over the printed name of the Deputy Secretary.

**SUBJECT: Department Policy Regarding the Use of Cell-Site  
Simulator Technology**

Cell-site simulators are invaluable law enforcement tools that locate or identify mobile devices during active criminal investigations. They allow law enforcement to locate both subjects of an investigation and their victims. This policy is being issued in light of the Department of Justice's recent legal analysis of the use of the valuable cell-site simulator technology.

As with any law enforcement capability, the Department of Homeland Security (“DHS” or 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, DHS 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 respect for individuals’ privacy and civil liberties.

By this memorandum, I am directing immediate implementation of a DHS-wide policy on the use of cell-site simulator technology. This policy provides guidance and establishes common principles for the use of cell-site simulators across DHS. This policy applies to the use of cell-site simulator technology inside the United States in furtherance of criminal investigations. Affected DHS Components may issue additional specific guidance consistent with this policy.

## **BACKGROUND**

Law enforcement agents can use cell-site simulators to help locate cellular devices the unique identifiers of which 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.

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 device. 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.

By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is, however, limited. Cell-site simulators provide only the relative signal strength and general direction of the subject cellular device; 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's law enforcement Components 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 device itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the device. Moreover, cell-site simulators used by the Department's law enforcement Components do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

## **MANAGEMENT CONTROLS & ACCOUNTABILITY**

Department personnel require training and practice to properly operate cell-site simulators. Determinations regarding the appropriate use of this capability always should be informed by technological proficiency and experienced assessments of the suitability of the equipment for any given operation. To that end, the following management controls and approval processes will help ensure that only knowledgeable and accountable personnel will use the technology.

1. Each Component that uses cell-site simulators shall develop operational policy or procedures to govern the use of this technology consistent with this policy. When developing operational policy or procedures to govern the use of this technology consistent with Department policy, Components will coordinate with the DHS Office of the General Counsel, the Office of Policy, the Privacy Office, and the Office for Civil Rights and Civil Liberties.
2. Department personnel must be trained and supervised appropriately. Cell-site simulators may 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.
3. Within 30 days from the date of this policy, DHS law enforcement Components that use cell-site simulators shall designate an executive-level point of contact at the Component's headquarters office. The point of contact will be responsible for the implementation of this policy and for promoting compliance with its provisions, within his or her area of responsibility.
4. Prior to deployment of the technology, use of a cell-site simulator by the Component must be approved by 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 a Special Agent in Charge or the executive-level point of contact for the area of responsibility, as described in paragraph 3 of this section.

5. Each Component that uses cell-site simulators shall identify training protocols (including training on privacy and civil liberties) and protocols identifying which officials will have approval authority.

## **LEGAL PROCESS & 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 Components must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or applicable state equivalent), except as provided below.

As a practical matter, because agents or operators, in consultation with 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.

### *Exigent Circumstances under the Fourth Amendment*

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval—consistent with the circumstances delineated in the Pen Register Statute’s emergency provisions—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. Further, this policy requires that the case agent or operator first 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, the case agent or operator must contact the duty Assistant U.S. Attorney in the local U.S. Attorney's Office, who will coordinate approval within the Department of Justice.<sup>1</sup> Upon approval, the Assistant U.S. Attorney or state or local prosecutor must also apply for a court order within 48 hours as required by 18 U.S.C. § 3125.<sup>2</sup> 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.

#### *Exceptional Circumstances*

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. For example, potential uses of the technology in furtherance of protective duties pursuant to 18 U.S.C. § 3056 and 18 U.S.C. § 3056A. In these limited circumstances, agents must first obtain approval from executive-level personnel at the Component's headquarters and the relevant U.S. Attorney, who coordinates approval within the Department of 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, if circumstances necessitate emergency pen register authority, compliance with the provisions outlined in 18 U.S.C. § 3125 is required (see provisions in *Exigent Circumstances under the Fourth Amendment*, directly above).

---

<sup>1</sup> In non-federal cases, the case agent or operator must contact the prosecutor and any other applicable points of contact for the state or local jurisdiction.

<sup>2</sup> 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).

## APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

In all circumstances, candor to the court is of paramount importance. When making any application to a court, DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Law enforcement personnel must consult with the prosecutors<sup>3</sup> 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.<sup>4</sup>

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 devices on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology. The description should also indicate that investigators will use the information to determine 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 of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. Generally, in a majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. The application may also note, if accurate, that any potential service disruption 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 device. 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.

---

<sup>3</sup> While this provision typically will implicate notification to Assistant U.S. Attorneys, it also extends to state and local prosecutors when such personnel are engaged in operations involving cell-site simulators.

<sup>4</sup> 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 Department of Justice's 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 and consult with appropriate agency counsel for compliance with DHS policies.

## DATA COLLECTION & DISPOSAL

DHS is committed to ensuring that law enforcement practices concerning the collection or retention<sup>5</sup> of data are lawful and respect the important privacy interests of individuals. As part of this commitment, DHS's law enforcement Components 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,<sup>6</sup> the Department's use of cell-site simulators shall include the following practices:

1. Immediately following the completion of a mission, an operator of a cell-site simulator must delete all data.<sup>7</sup>
2. When the equipment is used to locate a target, data must be deleted as soon as the target is located.
3. When the equipment is used to identify a target, data must be deleted as soon as the target is identified, and no less than once every 30 days.
4. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.
5. Components shall implement an auditing program to ensure that the data is deleted in the manner described above. To the extent feasible, this auditing program will include 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 has the proper legal authority to collect and view data.

---

<sup>5</sup> 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.

<sup>6</sup> 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.

<sup>7</sup> A typical mission may last anywhere from less than one day and up to several days.

## **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. In all cases, law enforcement authorities in the United States must conduct their missions lawfully and in a manner that respects the rights of the citizens they serve. This policy applies to all instances in which 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**

Each DHS law enforcement Component shall provide this policy, and training as appropriate, to all relevant employees. Periodic review of this policy and training shall be the responsibility of each Component, based upon guidance from DHS oversight offices, 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). Any significant changes in technology or Component information collection, maintenance, use, or retention protocols may also trigger oversight responsibilities, and be reviewed before being implemented accordingly.<sup>8</sup>

Each field office shall report to its Component 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.<sup>9</sup>

Moreover, 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.

## **IMPROPER USE OF CELL-SITE SIMULATORS**

Accountability is an essential element in maintaining the integrity of our Federal law enforcement agencies. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the appropriate Component office that handles such allegations.

---

<sup>8</sup> For example, a significant change in technology could trigger the need for an updated or new privacy impact assessment.

<sup>9</sup> Records reflecting the number of times the cell-site simulators were used may also be required for ongoing oversight by the DHS oversight offices.

## **SCOPE OF THIS POLICY**

This policy guidance 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.

**From:** (b)(6); (b)(7)(C)  
**Sent:** 28 Mar 2019 15:33:38 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** can you assist?  
**Attachments:** DTAS Presentation 9.12.18 FLETC.PPTX  
**Importance:** High

(b)(6); (b)(7)(C)

(b)(5)

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) office)  
(202) 308- (b)(6); (b)(7)(C) cell)

(b)(6); (b)(7)(C)



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL~~

~~GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5  
USC §§ 552(b)(5), (b)(7).~~





**Homeland Security Investigations      Designated  
Technical Agent School (DTAS)      Sept. 12, 2018 -  
FLETC Office of the Principal Legal Advisor  
(OPLA)**

Page 364

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 365

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 366

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 367

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 368

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 369

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 370

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 371

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 372

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 373

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 374

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 375

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 376

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 377

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 378

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 379

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 380

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 381

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 382

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 383

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 384

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 385

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 386

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 387

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 388

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 389

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 390

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 391

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 392

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 393

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 394

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 395

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 396

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 397

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 398

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 399

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 400

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 401

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 402

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 403

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 404

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 405

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 406

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 407

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 408

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 409

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 410

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 411

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 412

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 413

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 414

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 415

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 416

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 417

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 418

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 419

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 420

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 421

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 422

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 423

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 424

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 425

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 426

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 427

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 428

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 429

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 430

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 431

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 432

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 433

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 434

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 435

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 436

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 437

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 438

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 439

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 440

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 441

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 442

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 443

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 444

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 445

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 446

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 447

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

# Office of the Principal Legal Advisor (OPLA)

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)



Homeland  
Security  
Investigations

~~OPLA HSILD – Criminal Law Section~~  
~~Law Enforcement Sensitive~~  
2020-ICLI-00013 448

**From:** OPLA-CLS  
**Sent:** 24 May 2017 17:24:18 -0400

**To:** (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

**Subject:** Cell-Site Simulator Training to (b) (7)(E)  
**Attachments:** Cell-Site Simulator training to the client

Tech Ops just updated its agenda and OPLA will be presenting in the afternoon now.



**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 18:39:16 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Cell-Site Simulator training to the client

(b) (7)(E) Team,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of (b) (7)(E) to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with (b)(6); (b)(7)(C) the following was decided:

On Thursday May 25<sup>th</sup>, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.  
On Thursday, June 8<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.  
On Thursday June 26<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.  
On Thursday July 27<sup>th</sup>, from 11-12, either (b)(6); (b)(7)(C) will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (b)(7)(C) (office)  
202-50 (b)(7)(C) (mobile)

(b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~



**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 18:16:41 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** cell-site  
**Attachments:** Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf

(b)(6);  
(b)(7)(C)

I've attached the DHS policy for cell-site.

(b)(6); (b)(7)(C); (b)(5)

I'll stop by to touch base as well,

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
(202) 732- (b)(6); (b)(7)(C) office)  
(202) 308- (b)(6); (b)(7)(C) cell)

(b)(6); (b)(7)(C)



~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 9 Jun 2017 20:41:11 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: (b)(5); (b)(6) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(5); (b)(6) Tracking Warrant + (b)(5); (b)(6) Cir. decision)  
**Attachments:** Department Policy Regarding the Use of Cell-Site Simulator Technology.pdf, Tracking Warrant - (b)(6); (b)(7)(C) pdf, (b)(5); (b)(6) -opn[1].pdf

FYSA

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 4:38 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** (b)(5); (b)(6) and Use of Cell-Site Simulator Technology (attached: DHS Policy + (b)(6); (b)(7)(C) Tracking Warrant + (b)(5); (b)(6) Cir. decision)

(b)(6); (b)(7)(C)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(6); (b)(7)(C)

(b)(6);  
(b)(7)(C)

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

202-732-(b)(6); (w)  
202-904-(b)(7)(c)

(b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

Page 455

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 456

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 457

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 458

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 459

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 460

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 461

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 462

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 463

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 464

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 465

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 466

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 467

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 468

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 469

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 470

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 471

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 472

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 473

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 474

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 475

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 476

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 477

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 478

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 479

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 480

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 481

Withheld pursuant to exemption

(b)(5) ; (b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

**From:** OPLA-CLS  
**Sent:** 9 Jun 2017 11:11:44 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: query - CLS SME re Cell Site Simulator  
**Attachments:** 12-2258\_opn[1].pdf

Good Morning,

Please note the email below from (b)(6); (b)(7)(C) to the CLS inbox seeking guidance on the use of cell site simulator technology. Recommend someone from (b) (7)(E) team provide assistance.

Best,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) office)  
202-494-(b)(6); (b)(7)(C) mobile)

(b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*~~

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, June 09, 2017 10:41 AM  
**To:** OPLA-CLS  
**Subject:** query - CLS SME re Cell Site Simulator

CLS Colleagues:

(b)(5)



(b)(5)

If convenient, the duty attorney and/or SME is free to give me a call. I am in the office today.

Thank you

(b)(6);  
(b)(7)(C)

(b)(6); (b)(7)(C)

Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (w)  
202-904-(b)(7)(c)

(b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 20 Jul 2016 11:32:57 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: [CCIPS Electronic Evidence Tips] Cell-site simulators  
**Attachments:** 9.3.15 Final Issued Cell Site Simulator Guidance.pdf, Cell-site simulator canvassing warrant go-by 2015 09 10.docx, Cell-site simulator locating warrant go-by 2015 09 10.docx

(b)(6); (b)(7)(C)  
Assistant Chief Counsel  
Office of the Chief Counsel - Orlando  
U.S. Immigration and Customs Enforcement  
U.S. Department of Homeland Security  
13077 Veveras Drive #213A  
Jacksonville, Florida 32258  
(904) 288 (b)(6); (b)(7)(C) Office)  
(202) 436 (b)(6); (b)(7)(C) Cell)  
(b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, June 22, 2016 3:44 PM  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: [CCIPS Electronic Evidence Tips] Cell-site simulators

(b)(6); (b)(7)(C)  
Assistant Chief Counsel  
Office of the Chief Counsel - Orlando  
U.S. Immigration and Customs Enforcement  
U.S. Department of Homeland Security  
13077 Veveras Drive (b)(6);  
Jacksonville, Florida 32258  
(904) 288 (b)(6); (b)(7)(C) Office)  
(202) 436 (b)(6); (b)(7)(C) Cell)  
(b)(6); (b)(7)(C)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*  
This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its~~

---

**From:** CCIPS Tips [mailto:CCIPS.Tips@usdoj.gov]  
**Sent:** Tuesday, April 26, 2016 1:25 PM  
**To:** CCIPS Tips  
**Subject:** [CCIPS Electronic Evidence Tips] Cell-site simulators

# CCIPS Electronic Evidence Newsletter

*Cell-site simulators (April 2016)*

## Go-by of the Month

Attached are two go-bys for affidavits in support of search warrants that authorize the use of a cell-site simulator. The first go-by is designed to be used when law enforcement intends to utilize the cell-site simulator to locate a cellular phone or device whose unique identifiers are already known to law enforcement. The second go-by is designed to be used when law enforcement intends to utilize the cell-site simulator to determine the unique identifiers assigned to a particular phone or device.

Also attached is a copy of the Department of Justice's policy regarding the use of cell-site simulator technology, which is discussed in more detail below.

## Practice Tip

Cell-site simulators are mobile devices that law enforcement agents can use to locate a cellular device whose unique identifiers are already known to law enforcement or to determine the identifiers of an unknown device. As part of their normal operations, cellular devices seek to connect to the cell tower that offers the strongest signal, and devices thus regularly scan for signals transmitted by cell towers in order to identify the best tower to which to connect. Once it identifies the tower with the strongest signal, a cellular device transmits its unique identifiers - assigned either by the device manufacturer or the device's wireless provider - to that cell tower to register with it and thus to connect to the cellular network. Cell-site simulators mimic cell towers; in response to signals emitted by the simulator, the cellular devices in the proximity of the cell-site simulator identify the simulator as the cell tower with the strongest signal in the area. Those devices thus transmit their unique identifiers to the cell-site simulator in the same way that they would with a networked tower. Cell-site simulators can also provide the relative signal strength and general direction from which a target cellular device emitted signals. Cell-site simulators used by the Department must be configured as pen registers and thus cannot be used to collect the contents of any communication.

In September 2015, the Department of Justice promulgated a policy, which applies both to its investigative agencies and prosecutors, relating to the use of cell-site simulator technology. Among other things, the policy requires that a search warrant be obtained prior to the use of a cell-site simulator except (1) when there are exigent circumstances or (2) in very limited circumstances in which the law does not require a warrant, approval is first obtained from the relevant U.S. Attorney and a Criminal Division Deputy Assistant Attorney General, and the

provisions of the Pen Register Statute are complied with. Furthermore, because the information collected by a cell-site simulator constitutes dialing, routing, addressing, and signaling information for purposes of the Pen Register Statute, the policy also requires that the search warrant contain all the information that must be included in pen-trap order pursuant to 18 U.S.C. 3123(b) or that a pen-trap order be obtained concurrently with the search warrant. In addition, the policy requires that any application to a court seeking authorization to use a cell-site simulator state: (1) a description, in general terms, of the way that cell-site simulators collect information from cellular devices and the purpose for which the simulator will be used (i.e. to locate or identify a target device); (2) that cellular devices in proximity to the cell-site simulator might experience a temporary disruption of cellular service; and (3) how law enforcement intends to address deletion of data not associated with the target phone. Finally, the policy establishes requirements applicable to DOJ investigative agencies pertaining to, inter alia, agency approvals that must be obtained prior to using cell-site simulators, deletion of data, and reporting about the use of cell-site simulators.

## Key Case

*Magistrate Judge Refuses to Sign Pen/Trap Order that Would Authorize the Use of a Cell-Site Simulator.* In *In re Application of the U.S.*, 890 F.Supp.2d 747 (S.D.Tex. 2012), the magistrate judge was presented with an application for a pen-trap order that would have authorized the use of a cell-site simulator to identify the cellular phone being used by the target of an investigation. The magistrate denied the application. As an initial matter, the magistrate criticized the government's application for failing to "explain the technology, or the process by which the technology will be used to engage in electronic surveillance to gather the Subject's cell phone number" and for failing to "address what the government would do with the cell phone numbers and other information concerning seemingly innocent cell phone users whose information was recorded by the equipment." More significantly, the magistrate reasoned that the government could not rely upon the Pen Register Act when seeking to identify an unknown phone using a cell-site simulator because the government cannot provide a phone number or other numerical identifier associated with the target phone, which the magistrate believed must be included in a pen-trap order pursuant to 18 U.S.C. 3123(b). Citing to *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012), the magistrate judge also suggested that cell-site simulators are mobile tracking devices for which warrants are required.

CCIPS' Take: As this opinion demonstrates, some judges feel that a pen-trap order is insufficient to authorize the use of a cell-site simulator. By generally requiring the use of a warrant, the Department's policy minimizes the litigation risk associated with the use of cell-site simulators.

---

*This newsletter is a publication of the Computer Crime and Intellectual Property Section, in the Department of Justice's Criminal Division. If you would like additional guidance on electronic evidence issues, you can:*

- Consult the go-bys and guidance available on CCIPS Online at <http://dojnet.doj.gov/criminal/ccips/online/evidence.htm> (this link will work only if you can connect to the DOJ intranet);

- *Consult the the CCIPS manual on Searching and Seizing Computers and Obtaining Electronic Evidence, which is publicly available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.*
- *Call the CCIPS duty attorney at (202) 514-1026.*

*To subscribe or unsubscribe to future newsletters, please email [CCIPS.Tips@usdoj.gov](mailto:CCIPS.Tips@usdoj.gov). Unless there is a problem or question about your subscription request, you will not receive a confirmation email. This email list is restricted to federal prosecutors and federal law enforcement agents, and you must use a federal government email address to subscribe.*



The Deputy Attorney General


Washington, D.C. 20530

September 3, 2015

MEMORANDUM FOR HEADS OF LAW ENFORCEMENT COMPONENTS

ALL UNITED STATES ATTORNEYS

FROM:

Sally Quillian Yates   
Deputy Attorney General

SUBJECT:

Department Policy Regarding the  
Use of Cell-Site Simulator Technology

The attached document establishes policy for the Department of Justice regarding the use of cell-site simulator technology. This technology supports critical public safety objectives, such as apprehending fugitives, locating kidnapping victims, and assisting in drug investigations. As with other technological tools, cell-site simulators must be used effectively and in accordance with the law. The attached document establishes consistent policy for the legal process that must be obtained for use of this technology, the information that must be provided to courts in connection with seeking court authority, handling and deletion of data collected by cell-site simulators, and various management and training requirements. The new policy will enhance transparency and accountability, improve our training and supervision, establish a higher and more consistent legal standard, and increase privacy protections in relation to law enforcement's use of this technology.

I ask that you ensure that this policy is shared with all relevant personnel and that appropriate steps are taken to provide the necessary training and ensure compliance with the policy. Any questions regarding this policy should be directed to (b)(6); (b)(7)(C) Office of the Deputy Attorney General, at (202) 514-(b)(6);

Attachment

## **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.<sup>1</sup> 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.

---

<sup>1</sup> 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<sup>2</sup>**

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.

---

<sup>2</sup> 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,<sup>3</sup> 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.<sup>4</sup> Assuming the parameters of the statute are met, the ESU attorney will contact a DAAG in the Criminal Division<sup>5</sup> 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,

---

<sup>3</sup> 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).

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

<sup>5</sup> 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<sup>6</sup> 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.<sup>7</sup>

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.

---

<sup>6</sup> 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.

<sup>7</sup> 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<sup>8</sup> 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,<sup>9</sup> 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

---

<sup>8</sup> 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.

<sup>9</sup> 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.

# WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO OBTAIN IDENTIFIERS OF A CELL PHONE OR OTHER CELLULAR DEVICE AT PARTICULAR LOCATIONS (“CANVASSING”)

THIS GO-BY IS CURRENT AS OF SEPTEMBER 2015. TO GET THE MOST CURRENT VERSION OF THIS GO-BY AND THE LATEST GUIDANCE, VISIT CCIPS ONLINE:

<http://dojnet.doj.gov/criminal/ccips/online/location.htm>

For help with any issues involving the search and seizure of computers, cell phones, and electronic evidence, call the Computer Crime and Intellectual Property Section (“CCIPS”), Criminal Division, United States Department of Justice, at (202) 514-1026.

## USAGE NOTES:

- Use this go-by to enable law enforcement to use its own cell-site simulator equipment (sometimes called “triggerfish” or “stingray”) to collect signals emitted by wireless phones or other cellular devices and use these signals only to determine the identifiers of a particular person’s cellular device. This order should not be served on a provider.
- For Departmental policy regarding use cell-site simulators, please refer to the September 3, 2015, memorandum *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* available on CCIPS online.
- Because a cell-site simulator falls within the statutory definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. The warrant therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1). In addition, an attorney for the government should complete an AO 106 Application for a Search Warrant as specified below to comply with the application requirements of 18 U.S.C. § 3123 for a pen register order.
- To the extent possible, configure the equipment so that it collects information from as few cellular devices as practical.
- Be sure to follow the procedures described in the application for limiting additional uses of the data collected.
- This go-by is intended to be used with a standard AO 93 Search Warrant form. Do NOT use the AO 102 Application for a Tracking Warrant. Fill out your district’s AO 93 Search Warrant form this way:

1. Caption the warrant “In the Matter of the Use of a Cell-Site Simulator to Identify the Cellular Device Used by [[suspect]].” To caption the warrant in this manner, strike out “the Search of” in the existing caption of the AO 93.
  2. Below the parenthetical that asks you to “identify the person or describe the property to be searched and give its location,” write “See Attachment A.”
  3. Below the parenthetical that asks you to “identify the person or describe the property to be seized,” write “See Attachment B.”
  4. The AO 93 form includes spaces for the district in which the property to be searched is located. Rule 41(b) generally requires that the cellular device that you are targeting be in the issuing district either at the time of search, or at the time the warrant is issued. Pursuant to Rule 41(b)(2), investigators may use this technique outside the district provided the cellular device is within the district when the warrant is issued.
  5. Check the box that indicates that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705,” and fill out the appropriate sub-boxes and blanks to indicate the length of delay that you are seeking under 18 U.S.C. § 3103a(b). If you use the standard language contained in this go-by, you should check the first sub-box and indicate the number of days as “30.”
- To ensure compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, an attorney for the government should complete an AO 106 Application for a Search Warrant. *See* 18 U.S.C. §§ 3122(a), 3127(5). In the “The application is based on these facts” box, write: “See Affidavit in Support of an Application for a Search Warrant. To ensure technical compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, this warrant also functions as a pen register order. Consistent with the requirement for an application for a pen register order, I certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency]. *See* 18 U.S.C. §§ 3122(b), 3123(b).” Other boxes of the AO 106 should be completed in the same manner as the AO 93.
  - To ensure compliance with the notice requirements of Rule 41, CCIPS recommends giving notice of the warrant to the target of the canvassing operation. However, this notice can be delayed under 18 U.S.C. § 3103a(b). This go-by includes language seeking a 30-day delay of notice under 18 U.S.C. § 3103a(b), which permits notice to be delayed up to 30 days initially as long as certain statutory requirements are satisfied. If you need a longer delay, you can attempt to seek a delay to a “later date certain if the facts of the case justify a longer period of delay,” 18 U.S.C. § 3103a(b)(3), or can seek an extension of the original 30-day delay under 18 U.S.C. § 3103(a)(c).

- Include the following information in the warrant return/inventory: (1) the date and time when the acquisition of identifying information began, and (2) the period during which the government acquired identifying information.

- The Department of Justice Policy issued September 3, 2015, states:

Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations or specifications). ... 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.



IN THE UNITED STATES DISTRICT COURT  
FOR \_\_\_\_\_

IN THE MATTER OF THE USE OF A  
CELL-SITE SIMULATOR TO IDENTIFY  
THE CELLULAR DEVICE CARRIED BY  
[[SUSPECT]]

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique further described in Attachment B, in order to identify the cellular device or devices carried by **[[name and/or physical description of the suspect]]** (the “Target Cellular Device”), described in Attachment A.

2. I am a Special Agent with the [Agency], and have been since [Date].  
**[DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS  
QUALIFICATION TO SPEAK ABOUT THIS INVESTIGATION, CELLULAR  
DEVICES, AND OTHER TECHNICAL MATTERS].**

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This Court has authority to issue the requested warrant under Federal Rule of Criminal Procedure Rule 41(b)(1) & (2) because the Target Cellular Device is currently believed to be located inside this district because **[Provide evidence suggesting that Target Cellular Device is currently located in this district, e.g. the Target Cellular Device’s owner is known to spend most of his time in this district; the Target Cellular Device’s owner was seen in this district X days ago; etc.]**. Pursuant to Rule 41(b)(2), law enforcement may use the technique described in Attachment B outside the district provided the device is within the district when the warrant is issued.

5. **[USE THIS PARAGRAPH IF THE UNIQUE IDENTIFIERS ARE EVIDENCE OF A CRIME.]** Based on the facts set forth in this affidavit, there is probable cause to believe that violations of **[statutes]** have been committed, are being committed, and will be committed by **[suspect]**. There is also probable cause to believe that the identity of the Target Cellular Device will constitute evidence of those criminal violations. In addition, in order to obtain additional evidence relating to the Target Cellular Device, its user, and the criminal violations under investigation, law enforcement must first identify the Target Cellular Device. There is probable cause to believe that the use of the investigative technique described by the warrant will result in officers learning that identifying information.

6. Because collecting the information authorized by this warrant may fall within the statutory definitions of a “pen register” or a “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. *See* 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. *See* 18 U.S.C. § 3123(b)(1).

### **PROBABLE CAUSE**

7. **[[Give facts establishing probable cause. At a minimum, it is necessary to establish probable cause to believe that the suspect is likely to be carrying the Target Cellular Device, and that records about that cellular device's use will be pertinent to the investigation. If the Target Cellular Device is being carried by someone who is also a suspect, which will often be the case, then it is likely also necessary to identify the suspect and establish a connection between the suspect and the suspected crime. Also, explain why there is probable cause to collect identifying information for the next thirty days (or for some shorter period of time, if you amend this request to cover a period less than thirty days). If you specify particular locations in Attachment A for use of the technique, establish probable cause to believe that the Target Cellular Device will be present at those locations.]]**

### **MANNER OF EXECUTION**

8. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

9. To facilitate execution of this warrant, law enforcement may use an investigative device that sends signals to nearby cellular devices, including the Target Cellular Device, and in

reply, the nearby cellular devices will broadcast signals that include their unique identifiers. The investigative device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell to communicate with others. Law enforcement will use this investigative device when they have reason to believe that **[[name and/or physical description of the suspect]]** is present. Law enforcement will collect the identifiers emitted by cellular devices in the immediate vicinity of the Target Cellular Device when the subject is in multiple locations and/or multiple times at a common location and use this information to identify the Target Cellular Device, as only the Target Cellular Device's unique identifiers will be present in all or nearly all locations. Once investigators ascertain the identity of the Target Cellular Device, they will cease using the investigative technique. Because there is probable cause to determine the identity of the Target Cellular Device, there is probable cause to use the investigative technique described by the warrant to determine the identity of the Target Cellular Device.

10. The investigative device may interrupt cellular service of cellular devices within its immediate vicinity. Any service disruption will be brief and temporary, and all operations will attempt to limit the interference cellular devices. Once law enforcement has identified the Target Cellular Device, it will delete all information concerning non-targeted cellular devices. Absent further order of the court, law enforcement will make no investigative use of information concerning non-targeted cellular devices other than distinguishing the Target Cellular Device from all other devices.

## AUTHORIZATION REQUEST

11. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

12. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the person carrying the Target Cellular Device would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

13. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to identify the Target Cellular Device outside of daytime hours.

14. **[[If your district does not have standard forms/procedures for filing under seal, you can insert this language in the affidavit:** I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is

neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.]]

15. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

---

**[AGENT NAME]**  
Special Agent  
**[AGENCY]**

Subscribed and sworn to before me  
on \_\_\_\_\_:

---

UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B when the officers to whom it is directed have reason to believe that **[[name and/or physical description of the suspect]]** is present.

**[[Include the following if locations where the technique will be used are readily ascertainable at the time of drafting.]]** This technique may be used at the following locations: **[[List the locations at which you intend to use the canvassing technique. When possible, limit the locations included to the vicinity of precisely described areas. For locations that do not have an immediate, apparent connection to the suspect, it may be helpful to include a reference to why you believe the suspect will be present at the location. For example: the suspect's home (home address); the suspect's place of employment (work address); the suspect's daily commute between his home and place of employment.]]**

## ATTACHMENT B

The “Target Cellular Device” is the cellular device or devices carried by **[[name and/or physical description of the suspect]]**. Pursuant to an investigation of [identify of **subject of investigation**, if known] for a violation of [offense], this warrant authorizes the officers to whom it is directed to identify the Target Cellular Device by collecting radio signals, including the unique identifiers, emitted by the Target Cellular Device and other cellular devices in its vicinity for a period of thirty days, during all times of day and night.

Absent further order of a court, law enforcement will make no affirmative investigative use of any identifiers collected from cellular devices other than the Target Cellular Device, except to identify the Target Cellular Device and distinguish it from the other cellular devices. Once investigators ascertain the identity of the Target Cellular Device, they will end the collection, and any information collected concerning cellular devices other than the Target Cellular Device will be deleted.

This warrant does not authorize the interception of any telephone calls, text messages, or other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).



# WARRANT FOR THE USE OF A CELL-SITE SIMULATOR TO IDENTIFY THE LOCATION OF A KNOWN CELL PHONE OR OTHER CELLULAR DEVICE

THIS GO-BY IS CURRENT AS OF SEPTEMBER 2015. TO GET THE MOST CURRENT VERSION OF THIS GO-BY AND THE LATEST GUIDANCE, VISIT CCIPS ONLINE:

<http://dojnet.doj.gov/criminal/ccips/online/location.htm>

For help with any issues involving the search and seizure of computers, cell phones, and electronic evidence, call the Computer Crime and Intellectual Property Section (“CCIPS”), Criminal Division, United States Department of Justice, at (202) 514-1026.

## USAGE NOTES:

- Use this go-by to enable law enforcement to use its own cell-site simulator equipment (sometimes called “triggerfish” or “stingray” and also including additional “finishing tool” devices) to collect signals emitted by wireless phones or other cellular devices and use these signals to determine the location of a particular person’s cellular device. This warrant should not be served on a provider.
- For Departmental policy regarding use cell-site simulators, please refer to the September 3, 2015, memorandum *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* available on CCIPS online.
- Because a cell-site simulator falls within the statutory definitions of a “pen register” or a “trap and trace device,” see 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. The warrant therefore includes all the information required to be included in a pen register order. See 18 U.S.C. § 3123(b)(1). In addition, an attorney for the government should complete an AO 106 Application for a Search Warrant as specified below to comply with the application requirements of 18 U.S.C. § 3123 for a pen register order.
- This go-by is intended to be used with a standard AO 93 Search Warrant form. Do NOT use the AO 102 Application for a Tracking Warrant. Fill out your district’s AO 93 Search Warrant form this way:
  1. Caption the warrant “In the Matter of the Use of a Cell-Site Simulator to Locate the Cellular Device Assigned Call Number [(xxx) xxx-xxxx].” To caption the warrant in this manner, strike out “the Search of” in the existing caption of the AO 93. Note: If you have another identifier for the cellular device, such as the

International Mobile Subscriber Identity (IMSI) or Electronic Serial Number (ESN), you should include that identifier as well. You may also identify the cellular device by only its IMSI or ESN, rather than by call number, if that approach better suits the needs of your case.

2. Below the parenthetical that asks you to “identify the person or describe the property to be searched and give its location,” write “See Attachment A.”
  3. Below the parenthetical that asks you to “identify the person or describe the property to be seized,” write “See Attachment B.”
  4. The AO 93 form includes spaces for the district in which the property to be searched is located. Rule 41(b) generally requires that the cellular device that you are targeting be in the issuing district either at the time of search, or at the time the warrant is issued. If you are uncertain of the district in which the device is located, you may be able to locate it through a range of techniques, including by using a 2703(d) order for obtaining historical cell-site information. A go-by for this is available on CCIPS online:  
[http://dojnet.doj.gov/criminal/ccips/online/2703/2703\(d\)Orders/2703d go-by for non-content \(ISP list\).doc](http://dojnet.doj.gov/criminal/ccips/online/2703/2703(d)Orders/2703d%20go-by%20for%20non-content%20(ISP%20list).doc). Pursuant to Rule 41(b)(2), investigators may locate the device outside the district provided the device is within the district when the warrant is issued.
  5. Check the box that indicates that “immediate notification may have an adverse result listed in 18 U.S.C. § 2705,” and fill out the appropriate sub-boxes and blanks to indicate the length of delay that you are seeking under 18 U.S.C. § 3103a(b). If you use the standard language contained in this go-by, you should check the first sub-box and indicate the number of days as “30.”
- To ensure compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, an attorney for the government should complete an AO 106 Application for a Search Warrant. *See* 18 U.S.C. §§ 3122(a), 3127(5). In the “The application is based on these facts” box, write: “See Affidavit in Support of an Application for a Search Warrant. To ensure technical compliance with the Pen Register Statute, 18 U.S.C. §§ 3121-3127, this warrant also functions as a pen register order. Consistent with the requirement for an application for a pen register order, I certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency]. *See* 18 U.S.C. §§ 3122(b), 3123(b).” Other boxes of the AO 106 should be completed in the same manner as the AO 93.
  - To ensure compliance with the notice requirements of Rule 41, CCIPS recommends giving notice of the warrant either to the

person(s) who actually used the target cellular device or to the registered owner (if different). However, this notice can be delayed under 18 U.S.C. § 3103a(b). This go-by includes language seeking a 30-day delay of notice under 18 U.S.C. § 3103a(b), which permits notice to be delayed up to 30 days initially as long as certain statutory requirements are satisfied. If you need a longer delay, you can attempt to seek a delay to a “later date certain if the facts of the case justify a longer period of delay,” 18 U.S.C. § 3103a(b)(3), or can seek an extension of the original 30-day delay under 18 U.S.C. § 3103(a)(c).

- Include the following information in the warrant return/inventory: (1) the date and time when the acquisition of identifying information began, and (2) the period during which the government acquired identifying information.
- If you are seeking only an order directing a cell phone service provider to disclose prospective cell tower/sector records (sometimes called “cell-site data”) or more precise location information, this is the wrong go-by. Appropriate go-bys are available on CCIPS online:  
[http://dojnet.doj.gov/criminal/ccips/online/location.htm#Applications\\_and\\_Orders](http://dojnet.doj.gov/criminal/ccips/online/location.htm#Applications_and_Orders).
- The Department of Justice Policy issued September 3, 2015, states:  

Courts in certain jurisdictions may require additional technical information regarding the cell-site simulator's operation (e.g., tradecraft, capabilities, limitations or specifications). ... 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.

IN THE UNITED STATES DISTRICT COURT  
FOR \_\_\_\_\_

IN THE MATTER OF THE USE OF A  
CELL-SITE SIMULATOR TO LOCATE  
THE CELLULAR DEVICE ASSIGNED  
CALL NUMBER [(xxx) xxx-xxxx], [WITH  
INTERNATIONAL MOBILE SUBSCRIBER  
IDENTITY / ELECTRONIC SERIAL  
NUMBER xxxxxxxx]

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, [AGENT NAME], being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ an electronic investigative technique, which is described in Attachment B, to determine the location of the cellular device assigned call number [[(xxx) xxx-xxxx]], (the "Target Cellular Device"), which is described in Attachment A.

2. I am a [Special Agent] with the [Agency], and have been since [Date].  
**[DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS  
QUALIFICATION TO SPEAK ABOUT THIS INVESTIGATION, CELLULAR  
DEVICES, AND OTHER TECHNICAL MATTERS].**

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. One purpose of applying for this warrant is to determine with precision the Target Cellular Device's location. However, there is reason to believe the Target Cellular Device is currently located somewhere within this district because **[Provide evidence suggesting that Target Cellular Device is currently located in this district, e.g. the Target Cellular Device's owner is known to spend most of his time in this district; the telephone number area code associated with the Target Cellular Device corresponds to this district; the Target Cellular Device's owner was seen in this district X days ago; Cell-site data obtained for the Target Cellular Device indicated that it was normally to be found in this district, or found in this district X days ago; etc.]**. Pursuant to Rule 41(b)(2), law enforcement may locate the Target Cellular Device outside the district provided the device is within the district when the warrant is issued.

5. **[USE THIS PARAGRAPH IF THE LOCATION INFORMATION IS EVIDENCE OF A CRIME.]** Based on the facts set forth in this affidavit, there is probable cause to believe that violations of **[statutes]** have been committed, are being committed, and will be committed by **[suspects or unknown persons]**. There is also probable cause to believe that the location of the Target Cellular Device will constitute evidence of those criminal violations **[[, including leading to the identification of individuals who are engaged in the commission of these offenses and identifying locations where the target engages in criminal activity]]**.

6. **[USE THIS PARAGRAPH IF THE LOCATION INFORMATION WILL HELP TO EFFECTUATE AN ARREST]**

**AND/OR LOCATE A FUGITIVE.]** Based on the facts set forth in this affidavit, there is probable cause to believe that **[Fugitive]** has violated **[statutes]**. **[Fugitive]** was charged with these crimes on **[date]** and is the subject of an arrest warrant issued on **[date]**. **[[If appropriate: There is also probable cause to believe that [Fugitive] is aware of these charges and has fled.]]** There is also probable cause to believe that the Target Cellular Device’s location will assist law enforcement in arresting **[Fugitive]**, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

7. Because collecting the information authorized by this warrant may fall within the statutory definitions of a “pen register” or a “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), this warrant is designed to comply with the Pen Register Statute as well as Rule 41. *See* 18 U.S.C. §§ 3121-3127. This warrant therefore includes all the information required to be included in a pen register order. *See* 18 U.S.C. § 3123(b)(1).

### **PROBABLE CAUSE**

8. **[[Give facts establishing the probable cause described above. Among other things, this section generally should (1) establish a connection between the Target Cellular Device and the suspected crime and/or targeted individual, (2) identify the subscriber name and address for the Target Cellular Device [this information can be obtained with a subpoena to the wireless provider for the call number], (3) identify the primary user(s) of the Target Cellular Device, if known, and (4) explain why there is probable cause to monitor the cellular device’s location for the next thirty days (or for some shorter period of time, if you amend this request to cover a period less than thirty days).]]**

## MANNER OF EXECUTION

9. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

10. To facilitate execution of this warrant, law enforcement may use an investigative device or devices capable of broadcasting signals that will be received by the Target Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular Device and use that information to determine the Target Cellular Device's location, even if it is located inside a house, apartment, or other building.

11. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law

enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

### **AUTHORIZATION REQUEST**

12. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed warrant also will function as a pen register order under 18 U.S.C. § 3123.

13. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days from the end of the period of authorized surveillance. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cellular Device would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and [continue to] flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).



14. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cellular Device outside of daytime hours.

15. **[[If your district does not have standard forms/procedures for filing under seal, you can insert this language in the affidavit:** I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.]]

16. A search warrant may not be legally necessary to compel the investigative technique described herein. Nevertheless, I hereby submit this warrant application out of an abundance of caution.

Respectfully submitted,

---

**[AGENT NAME]**  
Special Agent  
**[AGENCY]**

Subscribed and sworn to before me  
On: \_\_\_\_\_

---

UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number (xxx) xxx-xxxx, [with International Mobile Subscriber Identity / Electronic Serial Number xxxxxxxx], whose wireless provider is [WIRELESS PROVIDER], and whose listed subscriber is [name/unknown].

**ATTACHMENT B**

Pursuant to an investigation of [identify of subject of investigation, if known] for a violation of [offense], this Warrant authorizes the officers to whom it is directed to determine the location of the cellular device identified in Attachment A by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to radio signals sent to the cellular device by the officers;

for a period of thirty days, during all times of day and night. This warrant does not authorize the interception of any telephone calls, text messages, other electronic communications, and this warrant prohibits the seizure of any tangible property. The Court finds reasonable necessity for the use of the technique authorized above. *See* 18 U.S.C. § 3103a(b)(2).

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 20:16:25 +0000  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: Cell-Site Simulator training to the client

(b)(6);  
(b)(7)(C)

Can I work from (b) (7)(E) on 5/25?

Thanks (b)(6);  
(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, April 19, 2017 2:39 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** Cell-Site Simulator training to the client

(b) (7)(E) Team,

We have been asked to provide an hour long training on ICE's cell-site simulator policy on behalf of (b) (7)(E) to its field TEOs. There are four sessions that will be held this summer at the Lorton VA facility. After discussing with Joe and Anne, the following was decided:

On Thursday May 25<sup>th</sup>, from 11-12, all of the Tech Ops team will travel to Lorton and watch me give the presentation on cell-site simulators.

On Thursday, June 8<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.

On Thursday June 26<sup>th</sup>, from 11-12, (b)(6); (b)(7)(C) will give the presentation and (b)(6); (b)(7)(C) will join him.

On Thursday July 27<sup>th</sup>, from 11-12, either (b)(6); (b)(7)(C) will give the presentation, and it can be left to the two of you to decide who will go.

I believe the presentation and policy is on the S:Drive, and if it isn't, I will make sure it is this afternoon. Please let me know if you have any questions or comments, calendar invites will be forthcoming.

Sincerely,  
(b)(6); (b)(7)(C)

---

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-73 (b)(6); (b)(7)(C) office)

202-500-<sup>(b)(6);</sup><sub>(b)(7)</sub> (mobile)

(b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** 6 Sep 2018 15:00:57 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** DTAS presentation; FLETC; Sept. 12, 2018  
**Attachments:** Drone.docx, DTAS Presentation 9.12.18 FLETC.PPTX  
**Importance:** High

(b)(6);  
(b)(7)(C)

I am still cleaning these up today prior to sending them to the DTAS coordinator.

I worked from the docs (b)(6); (b)(7)(C) forwarded to me.

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

I used the current TFO slides as much as possible as the basis for the presentation.

Specifically:

(b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

I'll keep working to clean these up. I'll get through this presentation, and, hopefully from the questions from students and discussion with class coordinators I can continue to revise it in case CLS is asked to do it again.

Thanks,

(b)(6); (b)(7)(C)

Associate Legal Advisor

Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement

(202) 732-(b)(6);  
(b)(7)(C) (office)  
(202) 308-(b)(6);  
(b)(7)(C) (cell)

(b)(6); (b)(7)(C)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient.~~

~~Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

*ICE Office of the Principal Legal  
Advisor*

**U.S. Department of Homeland  
Security**

500 12th Street, S.W.  
Washington, DC 20536-5900



**U.S. Immigration  
and Customs  
Enforcement**

MEMORANDUM FOR:

(b)(6); (b)(7)(C)

Chief  
Criminal Law Section  
Office of the Principal Legal Advisor

FROM:

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section

SUBJECT:

(b)(5); (b)(7)(E)

DATE:

July 17, 2018

This Memorandum to file is in response to several meetings the Criminal Law Section (CLS) has had with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) regarding (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 1 Jun 2017 14:08:52 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Emailing: Draft HSI Cell-Site - Memo  
**Attachments:** Draft HSI Cell-Site - Memo.doc

Your message is ready to be sent with the following file or link attachments:

Draft HSI Cell-Site - Memo

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.



**U.S. Department of Homeland Security**  
500 12th Street, SW  
Washington, D.C. 20536



**U.S. Immigration  
and Customs  
Enforcement**

MEMORANDUM FOR: Assistant Directors  
Deputy Assistant Directors  
Special Agents in Charge  
Attachés

FROM: Peter T. Edge  
Executive Associate Director

SUBJECT: Use of Cell-Site Simulator Technology

Purpose:

(b)(5); (b)(7)(E)

SUBJECT: Use of Cell-Site Simulator Technology  
Page 2 of 7

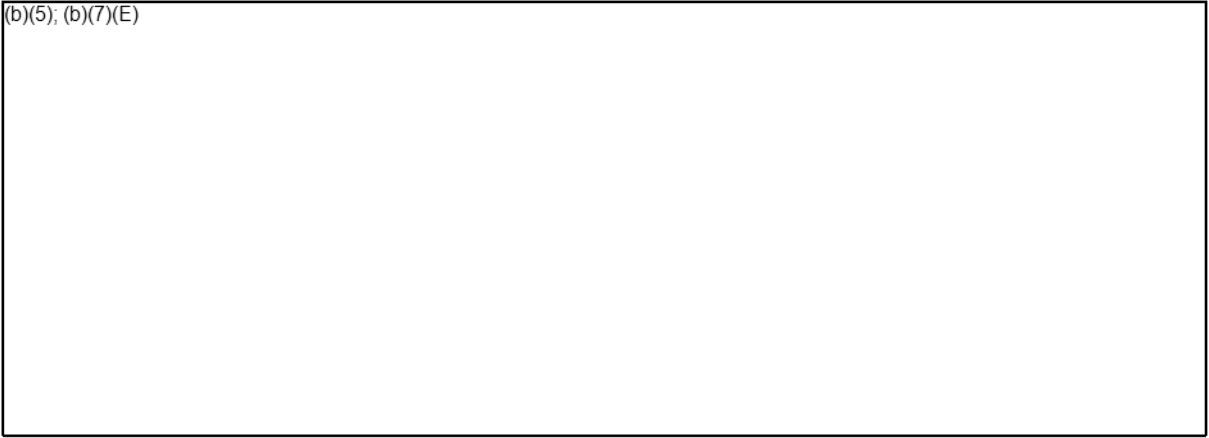
Background:

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

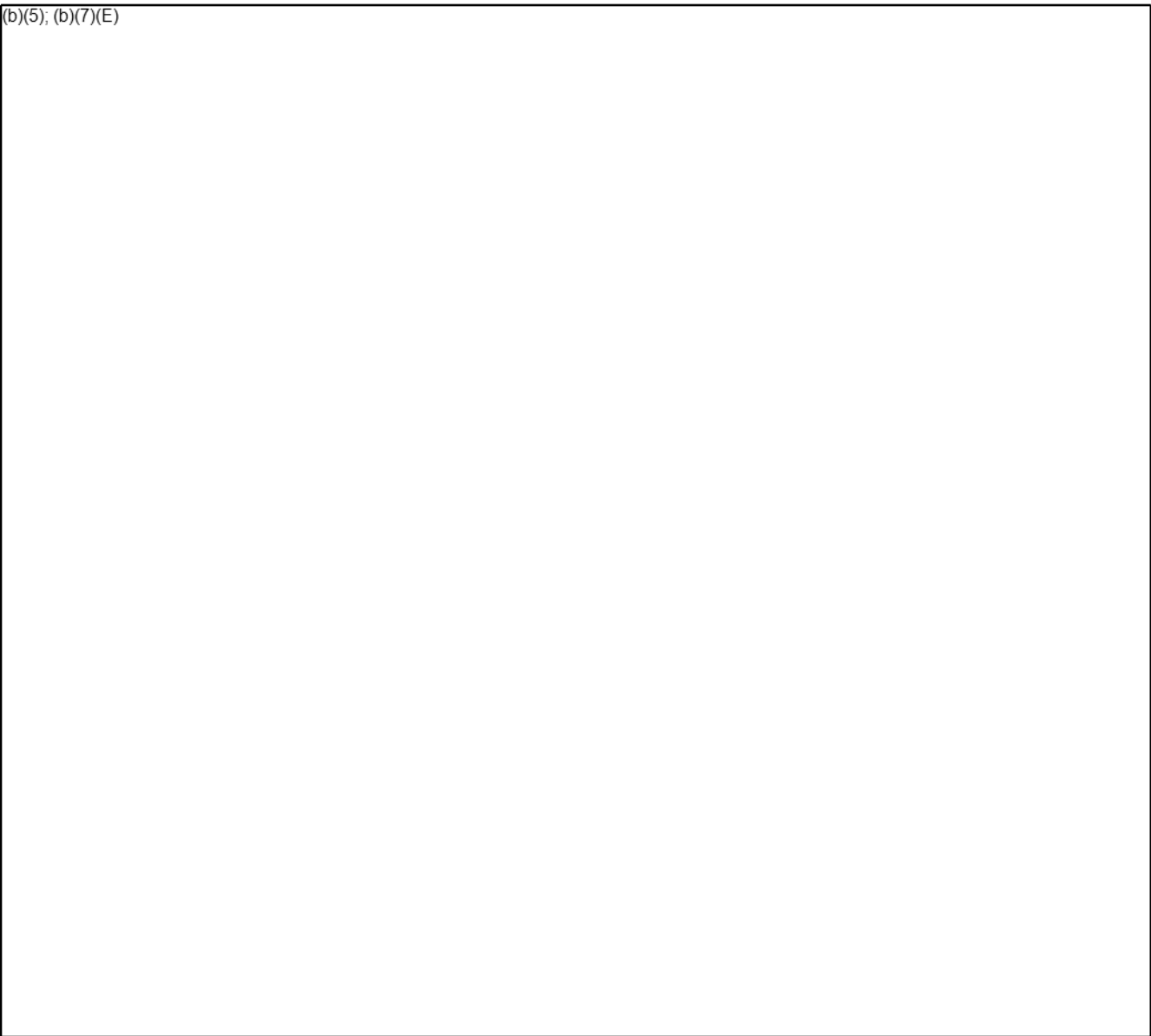
~~LAW ENFORCEMENT SENSITIVE~~

(b)(5); (b)(7)(E)



Legal Process and Court Orders

(b)(5); (b)(7)(E)



SUBJECT: Use of Cell-Site Simulator Technology  
Page 4 of 7

(b)(5); (b)(7)(E)

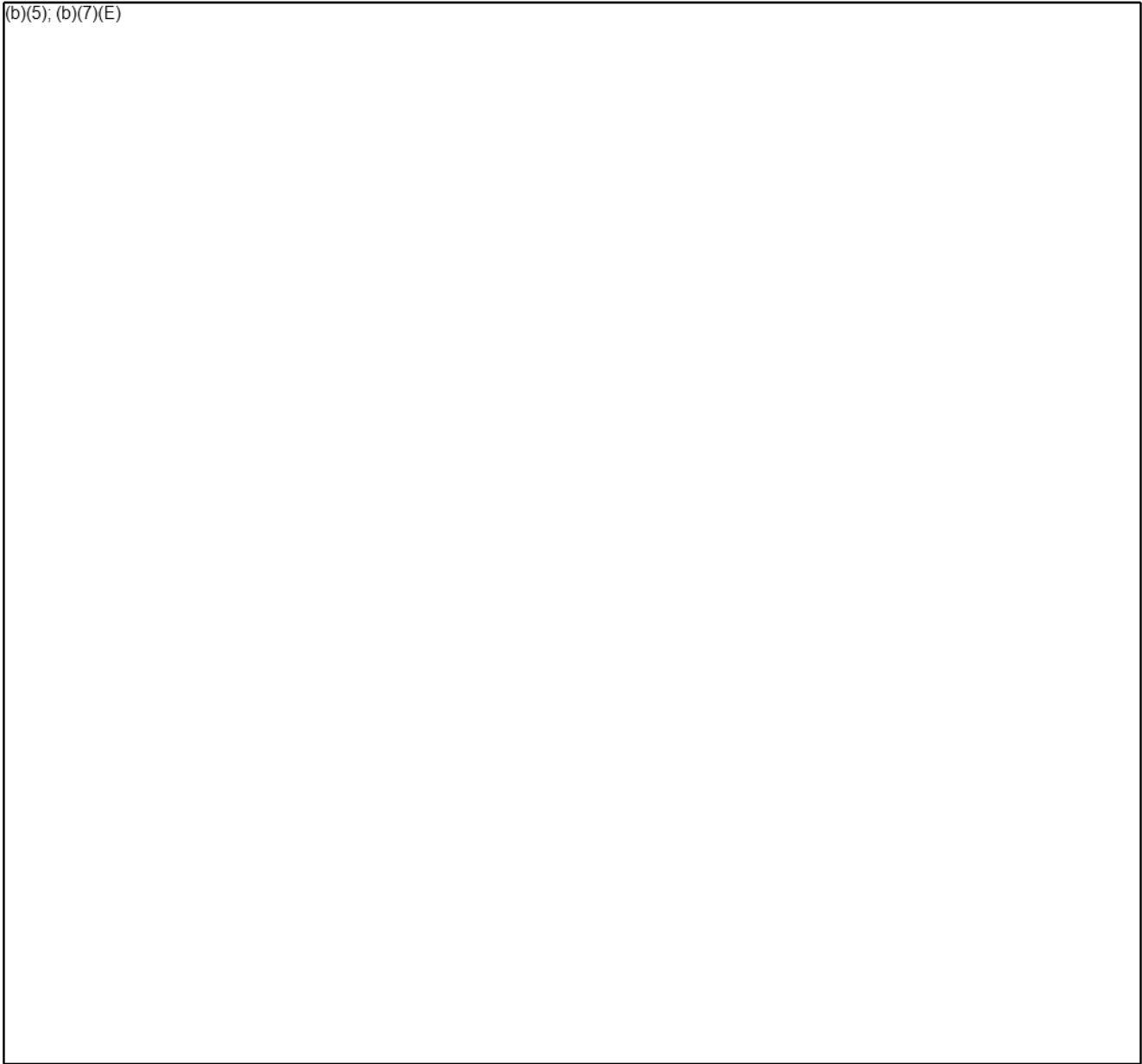
(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)


~~LAW ENFORCEMENT SENSITIVE~~

Applications for Use of Cell-Site Simulators

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)



~~LAW ENFORCEMENT SENSITIVE~~

Data Collection, Recordkeeping, and Disposal

(b)(5); (b)(7)(E)

State and Local Partners

(b)(5); (b)(7)(E)

Coordination and Ongoing Management

(b)(5); (b)(7)(E)

Improper Use of Cell-Site Simulators

Accountability is an essential element in maintaining the integrity of HSI. Allegations of violations of any orders that implement this policy, as with other allegations of misconduct, will be referred to the Joint Intake Center and/or the ICE Office of Professional Responsibility.

No Private Right

This policy guidance 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.

(b)(5); WIF Draft

**LAW ENFORCEMENT SENSITIVE**

**From:** (b)(6); (b)(7)(C)  
**Sent:** 19 Apr 2017 16:28:51 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: Cell-Site Simulator training to the client

Works for me.

(b)(6); (b)(7)(C)

Deputy Chief  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (b)(7)(C) Desk)  
202-536-(b)(7)(C) Cell)

~~\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\*~~

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Date:** Wednesday, Apr 19, 2017, 4:16 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** (b)(6); (b)(7)(C)  
**Subject:** FW: Cell-Site Simulator training to the client

(b)(6); (b)(7)(C)

Can I work from Tech Ops on 5/25?

Thanks, (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wednesday, April 19, 2017 2:39 PM  
**To:** (b)(6); (b)(7)(C)



**From:** (b)(6); (b)(7)(C)  
**Sent:** 2 Mar 2017 13:10:47 -0500  
**To:** (b)(6); (b)(7)(C)  
**Subject:** FW: DOJ Video Surveillance Storage Challenges  
**Attachments:** DOJ Video Surveillance Storage Challenges.pdf, HSI Surveillance Technologies PIA (IGP 02 06 2017).docx

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6) (office)  
202-500-(b)(7) (mobile)

(b)(6); (b)(7)(C)

**\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\***

~~This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, February 28, 2017 8:37 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: DOJ Video Surveillance Storage Challenges

(b)(6);  
(b)(7)(C)

(b)(5); (b)(7)(E)

Thanks,

(b)(6); (b)(7)(C)

Section Chief / Supervisory Special Agent

Homeland Security Investigations  
Technical Operations Unit - Investigative Intercept Section

703-551-(b)(6); (b)(7)(C) fffice)

716-510-(b)(7)(C) ell)

(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Thursday, February 23, 2017 3:56 PM

**To:** (b)(6); (b)(7)(C)

**Subject:** DOJ Video Surveillance Storage Challenges

(b)(6); (b)(7)(C)

Don't know if you have a copy of this document.

I think it is beneficial for OPLA folks to see and review the policy for us.

(b)(7)(E)

(b)(6); (b)(7)(C)

(A) National Program Manager - Spectrum  
Department of Homeland Security  
ICE/HSI/Technical Operations (TechOps) HQ  
10501 Furnace Road Suite (b)(6); (b)(7)(C)  
Lorton, Virginia 22079  
Desk: 703-551-(b)(6); (b)(7)(C)  
Cell: 619-665-(b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)

**MAILING ADDRESS FOR ALL SPECTRUM EQUIPMENT:**

HSI Spectrum  
ATTN: (b)(6); (b)(7)(C)  
10501 Furnace Road, Suite (b)(6); (b)(7)(C) Lorton, Virginia 22079

**HELPDESK CONTACT INFO:**

**VECADS 24/7 Support Desk: (844) 4VECADS (1-844-483-2237) o** (b)(5); WIF Draft

**Spectrum Support Desk: (703) 551-(b)(6); (b)(7)(C) pr** (b)(5); WIF Draft

**ICE Service Desk: (888) 347-7762**

**Feeny Wireless (now known as Novatel) at [PROSupport@nvtl.com](mailto:PROSupport@nvtl.com)**



~~**CONFIDENTIALITY NOTICE:** This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.~~



Department of Justice  
*Office of the Chief Information Officer*

# Department of Justice Video Surveillance Storage Challenges

*May 27, 2016*

For Official Use Only

Page 543

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 544

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 545

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 546

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 547

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 548

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 549

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 550

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 551

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 552

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 553

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 554

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act



Page 555

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 556

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 557

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

**From:** (b)(6); (b)(7)(C)  
**Sent:** 11 Aug 2016 15:59:54 -0400  
**To:** (b)(6); (b)(7)(C)  
**Subject:** (b)(5); (b)(7)(E)  
**Attachments:** [redacted] OGC  
op....pdf

(b)(6); (b)(7)(C)

Associate Legal Advisor  
Criminal Law Section  
Homeland Security Investigations Law Division  
Office of the Principal Legal Advisor  
U.S. Immigration and Customs Enforcement  
202-732-(b)(6); (office)  
202-500-(b)(7)(C) (mobile)  
[redacted] (b)(6); (b)(7)(C)

~~\*\*\* WARNING \*\*\* ATTORNEY/CLIENT PRIVILEGE \*\*\* ATTORNEY WORK PRODUCT \*\*\*  
This document contains confidential and/or sensitive attorney/client privileged information or attorney work product and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please notify the sender if this message has been misdirected and immediately destroy all originals and copies. Any disclosure of this document must be approved by the Office of the Principal Legal Advisor, U.S. Immigration & Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY. FOIA exempt under 5 U.S.C. § 552(b)(5).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 9, 2016 5:54 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:** [redacted]  
**Subject:** FW: (b)(5); (b)(7)(E)

[redacted] (b)(5); (b)(6); (b)(7)(C); (b)(7)(E)

(b)(6); (b)(7)(C)

Deputy Assistant Director (A)  
Information Management Directorate  
ICE, Homeland Security Investigations  
703-551-(b)(6); (Tech Ops)  
202-732-(b)(7)(C) (PCN)  
202-486- [redacted] (C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 4:53:27 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

All,

Attached is the guidance from OGC in 2009 that HSI SA mentioned in their discussions with us this afternoon.

(b)(6); (b)(7)(C); (b)(7)(E)

500 12<sup>th</sup> Street SW | Mail Stop 5106 | Washington, D.C. 20536

Cell: (214) 882-(b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 3:47 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

(b)(6); (b)(7)(C) will wait for your response on this request – thanks

(b)(6); (b)(7)(C)  
Unit Chief  
ICE/HSI (b)(6); (b)(7)(C) desk | 202-341-(b)(6); (b)(7)(C) cell  
703-877-(b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Tuesday, August 09, 2016 3:38 PM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** RE: (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(6); (b)(7)(C)

Deputy Assistant Director (A)  
Information Management Directorate  
ICE, Homeland Security Investigations  
703-551-(b)(6); (b)(7)(C) Tech Ops)  
202-732-(b)(7)(C) PCN)  
202-486-(b)(7)(C) C)

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, August 08, 2016 10:43 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** RE: (b)(5); (b)(7)(E)

(b)(6); (b)(7)(C)

Please verify that this equipment is authorized to be purchased Tech Ops, OPLA, OCIO, OAQ, etc.

Thanks

(b)(6); (b)(7)(C)

Unit Chief  
ICE/HSI  
703-877-(b)(6); (b)(7)(C) desk | 202-341-(b)(6); (b)(7)(C) cell

---

**From:** (b)(6); (b)(7)(C)

**Sent:** Monday, August 08, 2016 10:32 AM

**To:** (b)(6); (b)(7)(C)

**Cc:**

**Subject:** (b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

Thanks

(b)(6); (b)(7)(C); (b)(7)(E)

500 12<sup>th</sup> Street SW | Mail Stop (b)(6);  
(b)(7)(C) Washington, D.C. 20536  
Cell: (214) 882-(b)(6);  
(b)(7)(C)



**Homeland  
Security**

**PRIVILEGED AND CONFIDENTIAL - ATTORNEY-CLIENT COMMUNICATION**

May 27, 2009

MEMORANDUM FOR:

(b)(6); (b)(7)(C)

Senior Advisor to the Deputy Under Secretary for Mission Integration  
~~Office of Intelligence and Analysis~~

FROM:

(b)(6); (b)(7)(C)

Associate General ~~Counsel~~ for Operations and Enforcement

(b)(6); (b)(7)(C)

Attorney-Advisor (Enforcement)

SUBJECT:

(b)(5); (b)(7)(E)

**Question Presented**

(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

(b)(5); (b)(7)(E)

(b)(7)(E); (b)(5)



(b)(5); (b)(7)(E)



(b)(5); (b)(7)(E)

**From:** (b)(6); (b)(7)(C)  
**Sent:** 22 Sep 2017 09:43:24 -0400  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** FW: New Adverse on Cell Site Simulators?

Did we know about this case?

(b)(6); (b)(7)(C)  
Chief  
CLS, HSILD, OPLA, ICE  
202-732-(b)(6);  
202-538-(b)(7)(C) Phone)

**\*\*\* Warning \*\*\* Attorney/Client Privilege \*\*\* Attorney Work Product \*\*\***

~~This communication and any attachments may contain confidential and/or sensitive attorney/client privileged information or attorney work product and/or law enforcement sensitive information. It is not for release, review, retransmission, dissemination, or use by anyone other than the intended recipient. Please notify the sender if this email has been misdirected and immediately destroy all originals and copies. Furthermore do not print, copy, re-transmit, disseminate, or otherwise use this information. Any disclosure of this communication or its attachments must be approved by the Office of the Principal Legal Advisor, U.S. Immigration and Customs Enforcement. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 USC §§ 552(b)(5), (b)(7).~~

**From:** (b)(6); (b)(7)(C)  
**Sent:** Friday, September 22, 2017 9:38 AM  
**To:** (b)(6); (b)(7)(C)  
**Cc:**  
**Subject:** New Adverse on Cell Site Simulators?

(b)(5)

# Police use of ‘StingRay’ cellphone tracker requires search warrant, appeals court rules

By [Tom Jackman](#) September 21 at 5:20 PM