From:	McKenney, William <(b)(6) (b)(6)
To:	Sterling, Brian <(b)(6) (b)(6) (b)(6)
CC:	
Subject:	RE: 21-008-AUD-CBP Cell Phone Surveillance Audit - Agenda
Date:	2021/02/02 10:22:59
Priority:	Normal
Type:	Note

Hi Brian-

Not quite sure off the top of my head, so I forwarded on to (b)(6) for her thoughts.

Bill

From: Sterling, Brian <(b)(6)
Sent: Tuesday, February 2, 2021 10:18 AM
To: Fleischaker, Deborah (b)(6) McKenney, William <(b)(6)
Cc: (b)(6)
Subject: FW: 21-008-AUD-CBP Cell Phone Surveillance Audit - Agenda

Good Morning Deborah and Bill,

SIIP is scheduled for an interview with the OIG on Thursday, Feb. 4 concerning DHS use of cellphone surveillance devices and commercial location databases and our policy work a few years ago. We just received the agenda (attached). (b)(5)
(b)(5)

Thanks,
Brian

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: Staver, Michael <(b)(6)
Sent: Tuesday, February 2, 2021 9:57 AM
To: Allen, James (b)(6) <(b)(6) Sterling, Brian <(b)(6)>

Cc: Nahlik, Jennifer (b)(6)
Subject: 21-008-AUD-CBP Cell Phone Surveillance Audit - Agenda

Good Morning,

Attached is an agenda for our meeting on Thursday. We are happy to answer any questions now or at the meeting.

Thank you,

Michael Staver
Audit Manager, DHS-OIG
(b)(6)

Sender:	McKenney, William (b)(6) (b)(6)
Recipient:	Sterling, Brian (b)(6) (b)(6); Fleischaker, Deborah (b)(6) (b)(6) (b)(6)
Sent Date:	2021/02/02 10:22:58
Delivered Date:	2021/02/02 10:22:59

Acquisition Review Decision

Source Selection Sensitive

Request ID:	HQ2019-3317	**PR Number or PIID:**	20111511
Request Title:	CND PAIG Tools		
Component:	Customs and Border Protection		
Amount:	$1,003,744	**TEPV:**	$1,003,744
HQC(s):	Thomas II, Charles; Fisher-McGowans, Deneal;		
Submitted:	Monday, May 20, 2019		

Summary of Acquisition

Customs and Border Protection (CBP) requires the renewal of multiple software tools (Lumina, CipherTrace, and Venntel) in support of the Counter Network Division's (CND) Publically Available Information Group (PAID) initiatives. Additionally, this procurement includes an increase to the Venntel licenses to further expand the pilot.

Acquired Items

IT Tower	Application	**Cost Pool**	Software
IT Sub-Tower	Business Software		

SME Recommendation

Enterprise Architecture (EA)	(b)(6)	Recommend Approval
Information Security (IS)		Recommend Approval
Infrastructure		Recommend Approval
Office of Accessible Systems & Technology (OAST)		Recommend Approval
Privacy (PRIV)		Recommend Approval
Program Accountability Risk Management (PARM)		Recommend Approval

HQ Coordinator Final Recommendation to DHS CIO

Recommend Approval with Post-Conditions

HQ Coordinator Notes

Post Conditions

Description	Due Date
Vendor; Contract #; and Award Amount	11/5/2019

DHS CIO Decision

Approved

Disapproval Comments (if applicable)

The Component Chief Information Officer is responsible for ensuring that a copy of this Acquisition Review Decision (ARD) and any attachments are provided to the Contract Officer who will award this requirement. If the DHS CIO response above is "Approved" or "Conditionally Approved", the Procurement Office is authored to proceed with the acquisition. The Component is responsible for ensuring compliance with all appropriation and procurement laws, regulations, and policies regarding this acquisition. The Contract Officer is responsible for ensuring that all conditions that modify the contract/statement of work as identified in the ARD are fully executed in the resultant award.

9/12/2019

X (b)(6)

Signed by: (b)(6)

Signed by (b)(6) View details
on Thursday, September 12, 2019 3:42 PM (Eastern Daylight Time)

Acquisition Review Decision

Source Selection Sensitive

Additional Information

Contacts

Submitter	(b)(6)	**Phone**	(b)(6)	**Email**	(b)(6)
HQ Coordinator	(b)(6)	**Phone**		**Email**	

Investments

Investment	CBP - Automated Targeting System (ATS) Maintenance (P)	**Score**	5
IT Portfolio	Screening	**Major/Non-Major**	Major

Investment	CBP - Other	**Score**	
IT Portfolio	Benefits Administration	**Major/Non-Major**	

Acquired Items

IT Tower	Application	**Cost Pool**	Software
IT Sub-Tower	Business Software		

Background Information

Contract Type	Strategic Sourcing Vehicle - DHS	**Strategic Vehicle**	FirstSource II - IT Hardware and Software
Contract Action	License Renewal	**Form of Contract Award**	Firm Fixed Price
Vendor(s)			
Period of Performance	9/27/2019 to 9/26/2020	**Period**	Base
Number of Option Periods	0	**Re-Compete**	No

SME Review Notes and Recommendations to Contracting Officer

SME	Enterprise Architecture (EA) (b)(6)
Recommendation	Recommend Approval
SME Note	No comment provided.

SME	Information Security (IS) (b)(6)
Recommendation	Recommend Approval
SME Note	ISO Approved

SME	Infrastructure (b)(6)
Recommendation	Recommend Approval
SME Note	No comment provided.

SME	Office of Accessible Systems & Technology (OAST) (b)(6)
Recommendation	Recommend Approval
SME Note	No comment provided.

SME	Privacy (PRIV) (b)(6)
Recommendation	Recommend Approval
SME Note	No comment provided.

SME	Program Accountability Risk Management (PARM) (b)(6)
Recommendation	Recommend Approval
SME Note	No comment provided.

Post-Conditions

SME	HQ Coordinator (b)(6)
Description	Vendor; Contract #; and Award Amount
Response	
Adjudication	
SME Note	After the contract is awarded, the Component Coordinator is to enter into the request's Submission Form: a) the vendor name; b) the award amount); and c) the Contract #/Procurement Instrument Identifier (PIID).

Acquisition Review Decision

Source Selection Sensitive

Addendums

Completed Post-Conditions and Comments

No Completed Post-Conditions to display.

Addendums

Summary Form

No Summary Addendums to diplay.

Investment Form

No Investment Addendums to diplay.

Acquired Item Form

No Acquired Item Addendums to diplay.

From:	(b)(6)
To:	
Subject:	RE: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract
Date:	2020/11/04 13:34:00
Priority:	Normal
Type:	Note

Hi (b)(6),

I've been preparing for our discussion at 2, and wanted to proactively pass this along. Responses to questions Senator Markey posed to ICE in February, which we commented on in August.

(b)(6)
DHS CRCL
(b)(6)

From: (b)(6) >
Sent: Tuesday, November 3, 2020 11:15 AM
To: Sterling, Brian < (b)(6)
Cc: (b)(6)
Subject: RE: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract

Dear Brian and (b)(6),

Here is another article on the same topic:

https://urldefense.us/v2/url?u=https-3A__www.buzzfeednews.com_article_hamedaleaziz_ice-2Ddhs-2Dcell-2Dphone-2Ddata-2Dtracking-2Dgeolocation&d=DwIFAg&c=2pII3hXH8ww3j2g8pV19QHIf4SmK_I-EoI_p9P0CttE&r=iW3gyOPlcfH9aI_MgmxLB5o81lCyC2Za5urqHzP--bI&m=GtW-jpCeKqOKxJpLNdyQwygRfrJOO5HsJ9FLWNpD4w4&s=3dcB_LM1vxE6znBR2qDYv6SOawCCEQa8qkYuumaj-Ts&e=

This article may alter the draft questions for CBP from last week.

(b)(6) please let me know when you are available to connect.

I also wanted to ask you about another matter I am working on related to a complaint involving Maryland's data base which includes scanned drivers licenses and ICE ERO and HIS have access to it, but only HIS has a Privacy Impact Statement. I was given your name by my colleague here in Compliance. Perhaps we could talk this through when we arrange a time to discuss this Venntel contract and the briefing questions.

Thanks for your help.

Best,

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) - Mobile
(b)(6)

This message may contain information that is confidential, deliberative, law enforcement sensitive, and/or otherwise protected from public disclosure. If it has been sent to you in error, please reply immediately to advise the sender of the error and then destroy this message, any copies of this message and any printout of this message. If you are not the intended recipient of the message, any unauthorized dissemination, distribution or copying of the material in this message, and any attachments to the message, is strictly forbidden. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. §§ 552(b)(5), (b)(6), and/or (b)(7).

From: Sterling, Brian (b)(6)
Sent: Friday, October 30, 2020 4:01 PM
To: (b)(6)
Cc: (b)(6)
Subject: RE: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract

Thanks, (b)(6) SIIP would be happy to participate. I'm asking (b)(6) to take up this issue for us. He'll review the questions and get back to you next week.

Have a nice weekend!

Thanks,
Brian

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: (b)(6)
Sent: Friday, October 30, 2020 3:57 PM
To: Sterling, Brian <(b)(6)
Subject: Contact-DHS-21-0254 and Contact-DHS-21-0243 related to CBP and Venntel contract

Dear Brian,

Thanks again for our call earlier today.

At the meeting with Dana, Bill, Deborah, and others on the two above-referenced contacts this afternoon, Dana directed me to request a briefing from CBP prior to her making a decision whether to open a complaint. Compliance would like SIIP to participate in the briefing as well, please.

To that end, I have drafted several questions to send to CBP on the scope of the briefing based on the two articles below:

https://urldefense.us/v3/__https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant__;!!BClRuOV5cvtbuNI!QgqlxeApVZZ7X25Twz3lEiwIlZ2RwUNc9VC4DnSdBUUSnISLn_vgIGGGAhVS4MH6pqVjmnk5tRwe$

https://urldefense.us/v3/__https://www.nextgov.com/analytics-data/2020/10/senators-urge-investigation-after-cpb-admits-warrantless-cell-phone-surveillance/169562/__;!!BClRuOV5cvtbuNI!RzcNKDASjU9coXlg6Sg2mcmWxduY1Ux7cMsJb7_qK43hmdlulWxHAxTohFuUz9Gpn1xWKGvSu28$

I would appreciate your help by providing your input regarding these draft questions for the briefing, please:

(b)(5)

(b)(5)

Thanks for your feedback on these questions and offering your ideas for other questions, Brian.

Best,

(b)(6)

(b)(6)
Senior Policy Advisor, Compliance Branch
DHS, Office for Civil Rights and Civil Liberties
(b)(6) Mobile
(b)(6)

This message may contain information that is confidential, deliberative, law enforcement sensitive, and/or otherwise protected from public disclosure. If it has been sent to you in error, please reply immediately to advise the sender of the error and then destroy this message, any copies of this message and any printout of this message. If you are not the intended recipient of the message, any unauthorized dissemination, distribution or copying of the material in this message, and any attachments to the message, is strictly forbidden. This document is for INTERNAL GOVERNMENT USE ONLY and may be exempt from disclosure under the Freedom of Information Act, 5 U.S.C. §§ 552(b)(5), (b)(6), and/or (b)(7).

Sender:	(b)(6)
Recipient:	
Sent Date:	2020/11/04 13:34:30
Delivered Date:	2020/11/04 13:34:00
From:	(b)(6)
To:	CRCL Exec Sec (b)(6) (b)(6) (b)(6)
CC:	(b)(6) Dallam, Elizabeth (b)(6) (b)(6) Porto, Victoria (b)(6) (b)(6) Mina, Peter (b)(6) (b)(6)

	Venture, Veronica (b)(6) (b)(6) Salvano-Dunn, Dana (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6)
Subject:	RE: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)
Date:	2020/08/10 17:18:41
Priority:	Normal
Type:	Note

I've reviewed SIIP's redline and comment and note I-Section's clearance and on behalf of Deputy Officer Mina, clear . CRCL ExecSec – please return the attached document with the following language:

"CRCL clears with a minor redline to ensure this AS1 letter is fully responsive to this Congressional inquiry. CRCL POC is Brian Sterling, (b)(6)"

Thank you!

(b)(6)

From: Sterling, Brian (b)(6)
Sent: Monday, August 10, 2020 4:57 PM
To: (b)(6) (b)(6); CRCL Exec Sec (b)(6)
Cc: (b)(6) Dallam, Elizabeth (b)(6); PORTO, VICTORIA (b)(6); Mina, Peter (b)(6) Venture, Veronica (b)(6); Salvano-Dunn, Dana (b)(6); (b)(6) (b)(6)
Subject: RE: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)

Hi (b)(6)

SIIP recommends CRCL return the attached edits/comment proposing additional language to provide clarity.

INTERNAL,FOR THE RECORD

(b)(5)

(b)(5)

We intend to follow up with ICE to obtain policy documentation for the privacy protection limitations reported by ICE. We will then assess further engagement with ICE, and possibly the Department.

Thanks,
Brian

Brian Sterling
DHS CRCL
(b)(6) (desk)
(mobile)

From: CRCL Exec Sec (b)(6)
Sent: Monday, August 10, 2020 10:17 AM
To: Dallam, Elizabeth (b)(6); (b)(6); (b)(6); (b)(6); (b)(6); (b)(6); Sterling, Brian (b)(6)
Cc: Venture, Veronica (b)(6); Mina, Peter (b)(6); Salvano-Dunn, Dana (b)(6); PORTO, VICTORIA (b)(6); (b)(6); (b)(6); CRCL Exec Sec (b)(6); (b)(6)
Subject: Task Status Report: ICE DRAFT FOR CLEARANCE - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)

Good morning, SIIP/I-section:
Sorry this draft was inadvertently not circulated. It was originally tasked in February. Please see the attached and advise if there are comments.

<< File: Markey Draft Enclosure - 08.03.2020.docx >> << File: Markey Draft Cover Letter - 08.03.2020.docx >>

-----Original Message-----
From: (b)(6)
Sent: Monday, August 10, 2020 7:44 AM
To: CRCL Exec Sec (b)(6)
Subject: Clearance Status Requested. (Service 1191089) (Intranet Quorum IMA007540485)

CRCL / PRIV:

Regarding WF 1191089 – please provide a status update.

Thank you for your time, consideration, and help with this request.

Best,

(b)(6)
Correspondence Specialist
Office of the Executive Secretariat
Office of the Director
U.S. Immigration and Customs Enforcement
(b)(6) (o)
(c)
(b)(6)

Contact: The Honorable Edward J. Markey

https://IQ.dhs.gov/iq/UX/serviceitem.aspx?id=1191089&iAccount=IQ

Sincerely,

(b)(6)
DHS/CRCL/CRCL ExecSec
(b)(6) office
mobile

-----Original Task-----
Subject: ICE DRAFT FOR CLEARANCE TO COME - AS1 Correspondence re: reports that DHS purchased data and software that tracks the location for immigration enforcement purposes (WF #1191089)
Priority: Normal
Due date: Thu 2/20/2020

Status: Not Started
% Complete: 0%
Actual work: 0 hours

Requested by: CRCL Exec Sec

Lead: SIIP
~~Coord.: I section~~
Cc: Ronnie, Peter, Dana, Becky, (b)(6)

ICE draft to be circulated at a later date for CRCL comment/clearance.

<< File: WF1191089 incoming.pdf >>

~msr

-----Original Message-----
From: CRCL Exec Sec
Sent: Thursday, February 13, 2020 11:30 AM
To: Sterling, Brian <(b)(6); Dallam, Elizabeth <(b)(6)
Rogal, (b)(6); Cucinella, Amy <(b)(6) (b)(6)
<(b)(6) Venture, Veronica <(b)(6); Mina, Peter
<(b)(6) Salvano-Dunn, Dana <(b)(6); Tosado, Rebekah
<(b)(6) (b)(6)
Cc: CRCL Exec Sec <(b)(6) (b)(6)
Subject: AS1 Correspondence re: reports that DHS purchased data and software that tracks the location of individuals and is using this for immigration enforcement purposes.Clearing Component (WF #1191089)

SIIP/I-section: tasker to be sent. Please let me know if others should be included.

Sincerely,

(b)(6)
DHS/CRCL/CRCL ExecSec
(b)(6) office
mobile

-----Original Message-----
From: (b)(6)
Sent: Thursday, February 13, 2020 9:53 AM
To: CRCL Exec Sec <(b)(6)
Subject: Clearing Component (Service 1191089) (Intranet Quorum IMA007360444)

MGMT / OLA / OGC / CBP / PRIV / CRCL: ICE has the lead to prepare a draft in response to the attached incoming. Please share this incoming with your leadership. If your leadership has any comments, concerns, or issues that should be incorporated into the draft response, please share them with the drafting component within 24 hours so that the issues can be addressed prior to submitting the draft to ESEC

Contact: The Honorable Edward J. Markey

https://IQ.dhs.gov/iq/UX/serviceitem.aspx?id=1191089&iAccount=IQ

Sender:	(b)(6)
Recipient:	CRCL Exec Sec <(b)(6)

	(b)(6) (b)(6) Porto, Victoria (b)(6) (b)(6) Mina, Peter (b)(6) (b)(6) Venture, Veronica (b)(6) (b)(6) Salvano-Dunn, Dana (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6)
Sent Date:	2020/08/10 17:18:08
Delivered Date:	2020/08/10 17:18:41

Page 17

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 18

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 19

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 20

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Deputy Secretary
U.S. Department of Homeland Security
Washington, DC 20528

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

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. [1] 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.[2] 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).

---

[1] 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.

[2] 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).

DHS-001-10083-002684

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[3] 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.[4]

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.

---

[3] 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.

[4] 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.

DHS-001-10083-002685

DATA COLLECTION & DISPOSAL

DHS is committed to ensuring that law enforcement practices concerning the collection or retention[5] 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,[6] 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.[7]

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.

---

[5] 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.

[6] 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.

[7] A typical mission may last anywhere from less than one day and up to several days.

DHS-001-10083-002686

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.[8]

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.[9]

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.

---

[8] For example, a significant change in technology could trigger the need for an updated or new privacy impact assessment.

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

DHS-001-10083-002687

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.

DHS-001-10083-002688

From:	(b)(6)
To:	Sterling, Brian <(b)(6) (b)(6)
Subject:	FW: DUE 12 NOON, 10/5: ODNI-116 - Request for Views - S. ___, "The Fourth Amendment Is Not For Sale Act" Assignment (CMM-14793)
Date:	2020/10/02 16:55:56
Priority:	Normal
Type:	Note

(b)(5)

(b)(5)

Sender:	(b)(6)
Recipient:	Sterling, Brian <(b)(6) (b)(6)
Sent Date:	2020/10/02 16:54:25
Delivered Date:	2020/10/02 16:55:56
From:	Sterling, Brian (b)(6) (b)(6)
CC:	Sterling, Brian (b)(5) (b)(6)
BCC:	CRCL Exec Sec (b)(6) (b)(6) Sterling, Brian (b)(5) (b)(6)
Subject:	DUE 12 NOON, 10/5: ODNI-116 - Request for Views - S. ___, "The Fourth Amendment Is Not For Sale

	Act" Assignment (CMM-14793)
Date:	2020/09/25 16:12:33
Priority:	Normal
Type:	Task

Hi (b)(6)

Please review and return a clearance recommendation with any comments to me by COB Friday, Oct. 2.

Thanks,
Brian

Lead: SIIP
Cc: Ronnie, Peter, Dana, Victoria, Nicole

~msr

From: (b)(6)
Sent: Friday, September 25, 2020 3:56 PM
To: CRCL Exec Sec (b)(6)
Subject: PARTNERSJIRA: Request for Component Comments on LRM ODNI-116 - Request for Views - S. ___, "The Fourth Amendment Is Not For Sale Act" Assignment (CMM-14793)

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

DEADLINE - 12:00, Oct 05 2020

LRM ODNI-116 - Request for Views - S. ___, "The Fourth Amendment Is Not For Sale Act" Assignment

Attached is a draft bill for which Senate Select Committee on Intelligence (SSCI) staff are seeking technical drafting assistance from IC elements. Also attached is a one-page summary sheet prepared by Senator Wyden's staff.

(b)(5)

for foreign intelligence purposes, and it would remove the ability of the Attorney General to grant civil immunity to third parties providing certain surveillance assistance not required or permitted by statute. **Handling note: The attached draft bill is non-public and has not yet been introduced. Please handle as USG only.**

(b)(6) is assigned to this matter. Please contact (b)(6) or (b)(6) if you have any questions.

(b)(5)

In preparing your component's response to this request, please follow your component's guidance and ensure that the response is cleared by the component prior to submission.

Please respond to this request for input no later than 12:00 on Oct 05 2020. If you do not respond by the deadline, OGC may assume that you have no comment on this matter.

IMPORTANT—WHEN RESPONDING TO THIS REQUEST, PLEASE REPLY TO THIS EMAIL MESSAGE WITHOUT CHANGING THE SUBJECT LINE.

Thank you.

(b)(6)
Department of Homeland Security
(b)(6)
(b)(6)

Sender:	Sterling, Brian (b)(6) (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=F2C7AB3F38C54CAAA560C5161A0C66E6-STERLING, B>
Recipient:	CRCL Exec Sec (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6) Sterling, Brian (b)(6) (b)(6)
Sent Date:	2020/09/25 16:12:33

The Fourth Amendment Is Not For Sale Act

Federal agencies are using legal loopholes to collect massive amounts of information on Americans without a court order, violating the spirit of the Fourth Amendment. While there are strict rules for consumer-facing companies — phone companies like AT&T and Verizon and tech companies like Google and Facebook — loopholes in the law currently permit data brokers and other firms without a direct relationship to consumers to sell Americans' private information to the government without a court order.

Media reports earlier this year revealed that a data broker named Venntel is selling location data collected from Americans' smartphones to government agencies. While it would be unlawful for app developers to sell data directly to the government, a legal loophole permits app developers to sell data to a data broker, which can then sell that data to the government. According to media reports, other data brokers have tracked people at places of worship and at protests.

Another controversial data broker, Clearview.AI, has compiled a massive database of billions of photos, which it downloaded in bulk from Facebook, LinkedIn, Twitter & YouTube, in violation of their terms of service. Clearview.AI uses these illicitly obtained photos to power a facial recognition service it sells to government agencies, which they can search without a court order.

The Fourth Amendment Is Not For Sale Act closes major loopholes in federal privacy law and ensures that the Electronic Communications Privacy Act, which regulates law enforcement access to Americans' information, and the Foreign Intelligence Surveillance Act, which regulates the intelligence agencies, are the exclusive means by which the government can surveil Americans. This bill:

- Requires the government to get a court order to force data brokers to disclose data — the same kind of court order needed to compel data from tech and phone companies.
- Stops law enforcement and intelligence agencies buying data on people in the U.S. and about Americans abroad, if the data was obtained from a user's account or device, or via deception, hacking, violations of a contract, privacy policy, or terms of service. As such, this bill prevents the government buying data from Clearview.AI.
- Extends existing privacy laws to infrastructure firms that own data cables & cell towers.
- Closes loopholes that permit the intelligence community to buy or otherwise acquire metadata about Americans' international calls, texts and emails to family and friends abroad, and obtain records about their web browsing of foreign websites — information that would normally require a court order to compel.
- Takes away the Attorney General's authority to grant civil immunity to providers and other third parties for assistance with surveillance not required or permitted by statute. Providers retain immunity for surveillance assistance ordered by a court.

From: (b)(6); (b)(7)(C)
Sent: 23 Jul 2019 18:06:56 +0000
To: (b)(6); (b)(7)(C)
Subject: FW: POC for Ad ID Date and Carpenter Case
Attachments: Venntel Gelocation Data Subscriptions (07 05 2019) DRAFT.docx

Attaching the latest draft of the ICE Venntel project privacy threshold analysis here (which Privacy is currently updating), and some of the email traffic outlining DHS OGC's interest, below.

(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 (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)
Sent: Monday, July 15, 2019 9:13 AM
To: (b)(6); (b)(7)(C)
Cc:
Subject: RE: POC for Ad ID Date and Carpenter Case

Thank you!

(b)(6); (b)(7)(C) I will be in touch a little later this week. We are trying to schedule a time for ICE Privacy, ICE OPLA, CBP Privacy, CBP OCC, S&T OGC, and S&T Privacy to hold a teleconference (b)(5) Our DHS HQ Privacy attorney, Alex Wood will also be a part of this conversation, as well as possibly an attorney or two from OGC Operations and Enforcement Law Division.

Best,
Minal

(b)(6)
Attorney - Technology Programs Law Division
Office of the General Counsel
Department of Homeland Security
(b)(6) (Office)
(Cell)
(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

From: (b)(6); (b)(7)(C)
Sent: Tuesday, July 9, 2019 1:41 PM
To: (b)(6) (b)(6); (b)(7)(C)
Cc: (b)(6); (b)(7)(C)
Subject: RE: POC for Ad ID Date and Carpenter Case

Hi (b)(6)
Apologies for the delayed response. The CLS POC will be (b)(6); (b)(7)(C) copied here.

(b)(6); (b)(7)(C)
Associate Legal Advisor
CLS, HSILD, OPLA, ICE
202-732-(b)(6); (b)(7)(C) (desk)
202-421- (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)
Sent: Wednesday, July 3, 2019 11:23 AM
To: (b)(6); (b)(7)(C)
Subject: RE: POC for Ad ID Date and Carpenter Case

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

(b)(5)

Attached is an email that may provide more context.

If you still think you are the correct POCs for this matter, please let me know and I will add you to the list. The S&T Privacy office is already having discussions with ICE Privacy – (b)(6); (b)(7)(C)
(b)(6); (b)(7)(C)

Have a wonderful Fourth!

Best,
(b)(6)

(b)(6)
Attorney - Technology Programs Law Division
Office of the General Counsel
Department of Homeland Security
(b)(6) (Office)
(Cell)
(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this message in error, please reply immediately to the sender and delete this message. Thank you.

From: (b)(6)
Sent: Tuesday, July 2, 2019 9:50 AM
To: (b)(6); (b)(7)(C)

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

Cc: (b)(6)

Subject: RE: POC for Ad ID Date and Carpenter Case

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

Many thanks! (b)(6) is our OGC point of contact who is working an S&T legal analysis. We greatly appreciate any insight and help that you can provide. (b)(6) will reach out to contact

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

Best regards,

(b)(6)

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

Sent: Tuesday, July 2, 2019 9:47 AM

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

(b)(6)

Subject: RE: POC for Ad ID Date and Carpenter Case

Thank you (b)(6); (b)(7)(C) for responding.

(b)(5)

(b)(5) (b)(6) is the POC at DHS S&T who was looking for an HSI legal POC.

Regards

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

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

Sent: Monday, July 1, 2019 2:55 PM

To: (b)(6); (b)(7)(C); OPLA-CLS (b)(7)(E); OPLA-GILD (b)(7)(E)

Cc: (b)(6); (b)(7)(C)

Subject: RE: POC for Ad ID Date and Carpenter Case

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

For now I will be your POC on this matter. I do too, need more information.

Thanks,

(b)(6); (b)(7)(C)
Associate Legal Advisor
Government Information Law Division
Office of the Principal Legal Advisor
Immigration and Customs Enforcement
500 12th St. SW, (b)(6); (b)(7)(C)
Washington, DC 20536
Office: 202-73(b)(6); (b)(7)(C)
Cell: 202-868-
Email: (b)(6); (b)(7)(C)

Page 39

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 40

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 41

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 42

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 43

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 44

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 45

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 46

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 47

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6)
Sent: 19 Jun 2019 16:24:20 +0000
To: (b)(6); (b)(7)(C)
Cc: (b)(6)
Subject: FW: Venntel/Project Alexander
Attachments: RE_ Alexander Data.pdf, RE_ Supreme Court case to weigh in on location data privacy.pdf
Importance: High

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

(b)(5)

(b)(6)

(b)(6)
Privacy Officer (Acting)
Science and Technology Directorate
Department of Homeland Security
(b)(6)

From: Vogel, Lindsay (b)(6)
Sent: Wednesday, June 19, 2019 11:26 AM
To: (b)(6)
Subject: Venntel/Project Alexander

Hi (b)(6)

I understand that S&T has purchased information from Venntel as part of Project Alexander. The PTA was never approved because we had and continue to have significant concerns with this technology.

(b)(5)

Thanks,
Lindsay

Lindsay Lennon Vogel
Senior Director, Privacy Compliance
DHS Privacy Office
Desk: (b)(6)
Cell: (b)(6)

Page 50

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 51

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 52

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 53

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 54

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 55

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 56

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 57

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 58

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 59

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 60

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 61

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 62

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 63

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 64

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 65

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 66

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 67

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6)
To: (b)(6)
(b)(6)
Subject: RE: Supreme Court case to weigh in on location data privacy
Date: Friday, June 22, 2018 1:20:57 PM

(b)(5)

From: (b)(6)
Sent: Friday, June 22, 2018 11:42 AM
To: (b)(6)

(b)(6)
(b)(6)
(b)(6)
(b)(6)

Subject: Re: Supreme Court case to weigh in on location data privacy

Is there a difference between “cell tower location data” and app data that you “opt in too”?

(b)(6)
Senior Principal Systems Engineer / Analytics & Big Data Outcome Leader
The MITRE Corporation
Homeland Security Systems Engineering & Development Institute (HS SEDI) FFRDC
cell: (b)(6) *ph:* (b)(6)
(b)(6)

From: (b)(6)

Date: Thursday, June 21, 2018 at 10:58 PM

To: (b)(6)
(b)(6)
(b)(6)
(b)(6)
(b)(6)

Subject: Supreme Court case to weigh in on location data privacy

Supreme Court case to weigh in on location data privacy

A Fourth Amendment case, Carpenter vs. United States, currently being decided upon by the U.S. Supreme Court focuses on key digital privacy questions, and its decision has the potential to influence future location-tracking practices, Forbes reports. The case questions whether law enforcement’s warrantless access to seven months of cell tower location data, which was then used to study a defendant’s movements as part of a robbery investigation, is unconstitutional. While the government states the defendant had “no legitimate expectation of privacy,” the defense argues, that “cell phone location data does not necessarily involve any voluntary act on the part of users.” Privacy advocates have raised concern that if the decision rules in favor of government access to location data, citizens could be placed at greater risk for future surveillance by law enforcement.
Full Story