From: Lane Scott, Kristi Z (OPCL)
Subject: FW: As promised
To: Wood, Alexander W (OPCL)
Sent: October 1, 2015 1:37 PM (UTC-04:00)
Attached: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx

---

From: Harp, Jennifer C. (OPCL)
Sent: Friday, June 12, 2015 1:56 PM
To: Moss, Robin (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: FW: As promised

Hi Robin,

You asked for the draft cell site simulator policy. It's attached to this email from Erika.

From: Brown Lee, Erika (ODAG)
Sent: Thursday, May 07, 2015 10:27 AM
To: Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Subject: FW: As promised

Hi Kristi – per our conversation, attached is the draft policy. Please let me know if you have any comments.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

From: Tyrangiel, Elana (OLP)
Sent: Thursday, May 07, 2015 9:31 AM

Document ID: 0.7.12327.48866

To: Brown Lee, Erika (ODAG)
Subject: As promised

Happy to walk through this with you – let me know if that's helpful. I look forward to hearing what you think!

Document ID: 0.7.12327.48866

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: QFRs from the Joint Law Enforcement Hearing for Review
To: Wood, Alexander W (OPCL)
Sent: May 13, 2015 10:43 AM (UTC-04:00)

I'll call to explain.

From: Wood, Alexander W (OPCL)
Sent: Wednesday, May 13, 2015 10:40 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: QFRs from the Joint Law Enforcement Hearing for Review

I'll try. Do you know where that option is?

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 13, 2015 10:39 AM
To: Wood, Alexander W (OPCL)
Subject: RE: QFRs from the Joint Law Enforcement Hearing for Review

Hi Alex,

Can you (b) (5) [redacted] ? Let me know if it doesn't go through.

Thanks,

Kristi

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 13, 2015 10:36 AM
To: Wood, Alexander W (OPCL); Raut, Anant (ATR)
Subject: RE: QFRs from the Joint Law Enforcement Hearing for Review

A/A,

OLP is drafting a Departmental Policy. The QFRs should be consistent with that policy. I'll send it to you both for your reference.

Thanks,

Kristi

From: Wood, Alexander W (OPCL)
Sent: Wednesday, May 13, 2015 10:32 AM
To: Raut, Anant (ATR)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: FW: QFRs from the Joint Law Enforcement Hearing for Review

Anant,

Thanks for the comments. I will (b) (5) [redacted] but we should do a little digging on comments/questions number 4 and 5; that is, your question on (b) (5) [redacted]. Can you work with Robin Moss in our office on seeing whether any (b) (5) [redacted] based on these two subject areas. If not, we may want to inquire with DEA on it.

Thanks,

Document ID: 0.7.12327.55585-000013

Alex

From: Raut, Anant (ATR)
Sent: Tuesday, May 12, 2015 3:45 PM
To: Wood, Alexander W (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: RE: QFRs from the Joint Law Enforcement Hearing for Review

I may have overflagged some issues.

From: Wood, Alexander W (OPCL)
Sent: Tuesday, May 12, 2015 1:52 PM
To: Raut, Anant (ATR)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: FW: QFRs from the Joint Law Enforcement Hearing for Review

Hi Anant,

Kristi asked me to have you review a number of QFRs that have come in. These are part of our daily emails we get from OLA on review of testimony/legislation. We review to see whether there are any privacy issues – from a Privacy Act perspective or privacy policy perspective. Also, you should look out to see whether there are descriptions of any Department-wide or component systems which may or may not collect information on individuals. We double check to see whether any privacy documentation exists for such systems; or if documentation should exist.

I will forward the rest of the emails to you. Let me know if you have any questions.

Comments are due by Monday so if there is anything of substance please let me know by mid-day Friday.

Thanks,
Alex

From: Riley, Ann J. (OLA)
Sent: Tuesday, May 12, 2015 1:44 PM
To: (b)(6), (7)(C) per OCDETF (OCDETF); (b)(6), (7)(C) per OCDETF (OCDETF); (b)(6), (7)(C) per OCDETF (OCDETF); Padden, Thomas (OCDETF); Coombes, William B. (CIV); Farley, Farrah (CIV); Libutti, Timothy A. (CIV); Brink, David; Hendley, Scott; Lofton, Betty; Opl, Legislation; Wroblewski, Jonathan; USAEO-Legislative (USA); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per FBI (DO) (FBI); (b)(6), (7)(C) per USMS (USMS); (b)(6), (7)(C), (7)(F) per USMS (USMS); Davis, Valorie A (OLP); Matthews, Matrina (OLP); White, Cleo (OLP); Brown Lee, Erika (ODAG); Chung, Joo (OPCL); Harp, Jennifer C. (OPCL); Lane Scott, Kristi Z (OPCL); Wood, Alexander W (OPCL)
Subject: FW: QFRs from the Joint Law Enforcement Hearing for Review

Please review the attached DEA QFRs and provide any comments or edits by 12pm noon, Monday, May 18th.

Thank you,
Ann

Ann J. Riley
Attorney Advisor
Office of Legislative Affairs
U.S. Department of Justice
(b) (6) | O: (b) (6) | M: (b) (6)

Document ID: 0.7.12327.55585-000013

From: Tyrangiel, Elana (OLP)
Subject: Testimony PLCY Stodder - Stingray - For OMB clearance
To: Fried, Hannah (OLP)
Sent: October 16, 2015 9:39 AM (UTC-04:00)
Attached: Testimony PLCY Stodder - Stingray - For OMB clearance.docx

Document ID: 0.7.12327.47918

Department of Justice

FOR IMMEDIATE RELEASE
THURSDAY, SEPTEMBER 3, 2015
WWW.JUSTICE.GOV

DAG
(202) 514-2007
TTY (866) 544-5309

JUSTICE DEPARTMENT ANNOUNCES ENHANCED POLICY FOR USE OF CELL-SITE SIMULATORS

Increased Privacy Protections and Higher Legal Standards to Be Required

WASHINGTON – The Justice Department today announced a new policy for its use of cell-site simulators that will enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard and increase privacy protections in relation to law enforcement's use of this critical technology.

The policy, which goes into effect immediately and applies department-wide, will provide department components with standard guidance for the use of cell-site simulators in the department's domestic criminal investigations and will establish new management controls for the use of the technology.

"With the issuance of this policy, the Department of Justice reaffirms its commitment to hold itself to the highest standards as it performs its critical work to protect public safety," said Deputy Attorney General Sally Quillian Yates. "Cell-site simulator technology has been instrumental in aiding law enforcement in a broad array of investigations, including kidnappings, fugitive investigations and complicated narcotics cases. This new policy ensures our protocols for this technology are consistent, well-managed and respectful of individuals' privacy and civil liberties."

Cell-site simulators are just one tool among many traditional law enforcement techniques and are deployed only in the fraction of cases in which the capability is best suited to achieve specific public safety objectives.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.

Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data

Document ID: 0.7.12327.26246-000002

contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

While the department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search warrant and circumstances make obtaining a search warrant impracticable. Department components will be required to track and report the number of times the technology is deployed under these exceptions.

To ensure that the use of the technology is well managed and consistent across the department, the policy requires appropriate supervision and approval.

# # #

15-XXX

DO NOT REPLY TO THIS MESSAGE. IF YOU HAVE QUESTIONS, PLEASE USE THE CONTACTS IN THE MESSAGE OR CALL THE OFFICE OF PUBLIC AFFAIRS AT 202-514-2007.

Document ID: 0.7.12327.26246-000002

From: Wade Tyson, Jill C (OLA)
Subject: Fwd: Department of Justice testimony - PDAAG Elana Tyrangiel
To: Fried, Hannah (OLP)
Cc: Losick, Eric P. (OLA); Traster, Benjamin (OLA)
Sent: October 20, 2015 10:04 AM (UTC-04:00)
Attached: Tyrangiel Testimony 10 21 2015.pdf, ATT00001.htm

Begin forwarded message:

From: "Wade Tyson, Jill C (OLA)" <(b) (6) >
Date: October 20, 2015 at 10:03:33 AM EDT
To: Troy Stock <(b) (6) >, Brian Quinn <(b) (6) >, Cordell Hull <(b) (6) >, Sean Brebbia <(b) (6) >
Cc: "Wade Tyson, Jill C (OLA)" <(b) (6) >
Subject: Department of Justice testimony - PDAAG Elana Tyrangiel

Please find attached the Department of Justice written statement for the Record, which is submitted in advance of the Committee's October 21, 2015, hearing regarding cell-site simulator devices and related policies.

Please confirm receipt. Thank you.
-JCT

Document ID: 0.7.12327.26248

Department of Justice

STATEMENT OF
ELANA TYRANGIEL
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

BEFORE THE
SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U. S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"EXAMINING LAW ENFORCEMENT USE OF
CELL PHONE TRACKING DEVICES"

PRESENTED
OCTOBER 21, 2015

Document ID: 0.7.12327.26248-000002

Statement of
Elana Tyrangiel
Principal Deputy Assistant Attorney General

Before the
Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives

At a Hearing Entitled
"Examining Law Enforcement Use of Cell Phone Tracking Devices"

October 21, 2015

Chairman Hurd, Ranking Member Kelly, and Members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Justice regarding the Department's Policy Guidance on the Use of Cell-Site Simulator Technology. This topic is important to the Department, as cell site simulators fulfill critical operational needs for all of the Department's law enforcement agencies. The technology has been used, for example, to help locate kidnapped children, to assist in apprehending dangerous and violent fugitives, and to aid in complicated investigations into drug trafficking.

As with all evolving technologies, the Department must continue to assess the use of cell-site simulators to ensure that its policies and practices enable law enforcement to carry out its public safety objectives while continuing to uphold the Department's commitments to individuals' privacy and civil liberties. We are pleased to engage with the Subcommittee in a discussion about the Department's policy.

Cell-site simulators are devices that can help law enforcement agents locate a known cellular device, or identify an unknown device used by a known suspect. The technology works by collecting limited signaling information from cellular devices in the simulator's vicinity, providing the relative signal strength and general direction of a subject cellular telephone. Cell-site simulators are one tool among many traditional law enforcement techniques, and the Department deploys them only in the fraction of cases in which the technology is best suited to achieve specific public safety objectives.

As you know, the Department recently issued a new policy governing its use of cell-site simulators in domestic criminal investigations. The policy is intended to enhance transparency and accountability, improve training and supervision, establish a higher and more consistent legal standard, and increase privacy protections.

Document ID: 0.7.12327.26248-000002

The policy provides Department components with standard guidance for the use of cell-site simulators and establishes management controls for the use of the technology. These include training and supervisory protocols, data handling requirements, and auditing and tracking measures. The Department intends these requirements to ensure that our use of this technology is well-managed, consistent across the Department, and respectful of individuals' privacy and civil liberties. We hope and believe the policy properly accomplishes these objectives, while addressing any confusion or misperception surrounding the Department's use of cell-site simulators.

* * *

The Department's policy covers all use of cell-site simulators by Department personnel in support of domestic criminal investigations, including when they are working in cooperation with state or local law enforcement agencies. Cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication.

The policy has four basic elements:

First, the policy establishes a variety of management controls and training requirements. Specifically, all operators of cell-site simulators must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert. Each agency will also identify training protocols. Those protocols must include training on privacy and civil liberties and must be developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

In addition, agencies must designate an executive-level point of contact responsible for implementing the policy in each jurisdiction. Before the technology is deployed, its use must be approved by an appropriate individual who has obtained the grade of a first-level supervisor. Emergency use must be approved by a second-level supervisor. And, to the extent these devices are occasionally used on an aircraft, that use must be approved by an executive-level supervisor or by a branch or unit chief at agency headquarters. These measures will help to ensure that only trained personnel use cell-site simulators and that the technology is used in accordance with the requirements of the policy.

Second, the policy adopts a consistent legal standard for the Department's use of cell-site simulators in domestic criminal investigations. While the Department has, in the past, obtained appropriate legal authorization to use cell-site simulators pursuant to orders under the Pen Register Statute, law enforcement agents now generally must obtain a search warrant supported by probable cause before using such a device. The policy recognizes two limited exceptions to the warrant requirement:

- When the Fourth Amendment does not require a warrant due to exigent circumstances, this policy does not require a warrant either. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement

Document ID: 0.7.12327.26248-000002

are so compelling that they render a warrantless search objectively reasonable (e.g., the need to protect human life or the hot pursuit of a fleeing felon). Agents, however, still must comply with the provisions of the Pen Register Statute, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. When emergency pen register authority is sought, approval must be obtained from a Deputy Assistant Attorney General in the Department's Criminal Division.

- There also may be very limited circumstances in which the Fourth Amendment does not require a warrant (for example, because the cell-site simulator will be used in a place where there is no expectation of privacy) and circumstances on the ground make obtaining a warrant impracticable. To use this exception, an agent first would need to seek approval from executive-level personnel from his law enforcement agency, approval from the relevant U.S. Attorney, *and* approval from a Deputy Assistant Attorney General in the Criminal Division. We expect this exception to be used only in very limited cases. In those cases, an agent still would need to obtain a court order under the Pen Register Statute as described above. The Criminal Division will track the number of times the use of a cell-site simulator is approved under this provision, as well as the circumstances underlying each such use.

Third, the policy enhances transparency to courts. As always, candor to courts is of utmost importance. The policy requires law enforcement agents to consult with prosecutors, and to include sufficient information in their warrant applications to ensure that courts understand that a cell-site simulator may be used. Specifically, the policy requires that the application or supporting affidavit include a general description of the technique to be employed, a statement that the target cellular device and other devices in the area might experience a temporary disruption of service, and an explanation of how law enforcement will treat the data the cell-site simulator obtains.

Fourth, in order to ensure that individuals' privacy interests are protected, the policy establishes consistent requirements for handling the data obtained by cell-site simulators. As used by the Department – and as now required by the policy – the devices do not, as noted above, obtain the contents of any communication or any data from the phone itself, whether emails, texts, or contact lists. Nor do they obtain subscriber account information such as name, address, or telephone number. But even for the limited types of information simulators do collect, the policy establishes requirements for deletion.

When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. In instances when it is used to identify an unknown cellular device, all data must be deleted as soon as the target device is identified, and in any event no less than once every 30 days. Agencies will be required to implement an auditing program to ensure adherence to these deletion requirements.

Document ID: 0.7.12327.26248-000002

* * *

In conclusion, I would like to reemphasize that cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives: this technology saves lives, enabling law enforcement to rescue endangered victims and apprehend dangerous criminals. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. Our policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

The Department of Justice stands ready to work with the Subcommittee as it addresses the use of these valuable technologies, and we appreciate the opportunity to discuss this issue with you.

Document ID: 0.7.12327.26248-000002

From: Wade Tyson, Jill C (OLA)
Subject: Fwd: DHS Testimony: "Examining Law Enforcement Use of Cell Phone Tracking Devices"
To: Fried, Hannah (OLP)
Sent: October 20, 2015 10:33 AM (UTC-04:00)
Attached: Testimony PLCY Stodder - final.pdf, ATT00001.htm, AS Seth Stodder Bio 2015.pdf, ATT00002.htm

Begin forwarded message:

From: "Henry, Iain" <(b)(6) per DHS>
Date: October 20, 2015 at 10:10:34 AM EDT
To: "Wade Tyson, Jill C (OLA)" <(b) (6)>
Subject: FW: DHS Testimony: "Examining Law Enforcement Use of Cell Phone Tracking Devices"

From: Vance, Sarah (OGRR) [mailto:(b) (6)]
Sent: Tuesday, October 20, 2015 10:08 AM
To: Henry, Iain <(b)(6) per DHS>
Cc: Johnson, Tia <(b)(6) per DHS>; LaRossa, Connie <(b)(6) per DHS>; Joh, Joseph <(b)(6) per DHS>; Balunis, Timm <(b)(6) per DHS>; Lovett, Edward <(b)(6) per DHS>; Casey, Sharon <(b) (6)>
Subject: RE: DHS Testimony: "Examining Law Enforcement Use of Cell Phone Tracking Devices"

Received. Thank you.

From: Henry, Iain [mailto:(b)(6) per DHS]
Sent: Tuesday, October 20, 2015 9:59 AM
To: Vance, Sarah (OGRR)
Cc: Johnson, Tia; LaRossa, Connie; Joh, Joseph; Balunis, Timm; Lovett, Edward
Subject: DHS Testimony: "Examining Law Enforcement Use of Cell Phone Tracking Devices"

Sarah,

Please see the attached testimony of Assistant Secretary Seth Stodder for the OGR Subcommittee on Information Technology hearing: "Examining Law Enforcement Use of Cell Phone Tracking Devices." Additional attachment: A/S Stodder's Bio.

V/R,
Iain Henry
Associate Director
Office of Legislative Affairs
Department of Homeland Security
(O) (b)(6) per DHS
(C) (b)(6) per DHS
(b)(6) per DHS

Document ID: 0.7.12327.26259

Seth M. M. Stodder

Assistant Secretary for Threat Prevention and Security Policy
Office of Policy
U.S. Department of Homeland Security

Seth Stodder was appointed by President Obama to serve as Assistant Secretary of Homeland Security for Threat Prevention and Security Policy, within the Office of Policy, in June 2015. Assistant Secretary Stodder leads a team advising Secretary Johnson and senior DHS leadership on a wide variety of issues relating to security threats to the U.S. homeland, and on how to address them while preserving the civil liberties and privacy rights we all cherish. Among other things, Assistant Secretary Stodder oversees DHS policy development on the screening of people moving through the global and domestic travel and transportation systems and across U.S. borders, visa policy, law enforcement policy, among many other issues.

A longtime expert in national and homeland security law and policy, Assistant Secretary Stodder also teaches Counterterrorism, Civil Liberties, and Privacy Law at the University of Southern California Law School. Prior to his appointment at DHS, Assistant Secretary Stodder was a partner in the law firm of Obagi & Stodder LLP, practicing civil and criminal trial and appellate litigation and immigration law, and also President of Palindrome Strategies, LLC., a consulting firm advising on a variety of issues relating to homeland security. He also served as a Senior Associate with the Center for Strategic and International Studies, a Senior Fellow at the George Washington University Homeland Security Policy Institute, and was closely involved in the development of the first Quadrennial Homeland Security Review and the National Strategy for Global Supply Chain Security. Earlier in his career, Assistant Secretary Stodder was a lawyer at Gibson Dunn & Crutcher LLP, as well as Akin Gump Strauss Hauer & Feld LLP, practicing appellate and constitutional law.

This is Assistant Secretary Stodder's second tour of duty at DHS. Earlier in his career, Assistant Secretary Stodder served in the Bush Administration as Director of Policy and Planning for U.S. Customs and Border Protection, and Counselor/Senior Policy Advisor for CBP Commissioner Robert C. Bonner. In that role, he was closely involved in the development and implementation of the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), and the pre-departure APIS/PNR and "24 Hour Rule" information collection requirements, among a variety of other initiatives focused not only on securing the borders of the United States, but also on facilitating the secure flow of lawful travel and trade across our borders and throughout the global economy.

Assistant Secretary Stodder is a member of the U.S. Supreme Court and California bars, has a J.D. from the University of Southern California Law School, and a B.A. from Haverford College. He is from Los Angeles, California.

Document ID: 0.7.12327.26259-000001

Seth M. Stodder

Assistant Secretary, Threat Prevention and Security Policy

Office of Policy

U.S. Department of Homeland Security

testifying before the

Committee on Oversight and Government Reform

Subcommittee on Information Technology

United States House

"Examining Law Enforcement Use of Cell Phone Tracking Devices"

on

Wednesday, October 21, 2015
2:00 p.m.
2154 House Office Building
Washington DC 20515

Document ID: 0.7.12327.26259-000004

Prepared Testimony

Seth M. Stodder
Assistant Secretary for Threat Prevention and Security Policy
Office of Policy
U.S. Department of Homeland Security

United States House Committee on Oversight and Government Reform
Subcommittee on Information Technology

October 21, 2015

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee, thank you for the opportunity to be here today to talk with you about how the Department of Homeland Security ("DHS" or the "Department") uses cell-site simulator technology. I will discuss this important law enforcement tool in the context of how cell-site simulators work and how DHS uses cell-site simulators. I will also provide an overview of the new DHS policy on the use of cell-site simulator technology.

Cell-site simulators, also known as International Mobile Subscriber Identity or "IMSI" catchers, are invaluable law enforcement tools that enable law enforcement personnel to identify and generally locate the mobile devices of both the subjects of an active criminal investigation and their victims. Cell-site simulators work by collecting limited signaling information from cellular devices in the cell-site simulator's vicinity, providing the relative signal strength and general direction of a subject cellular device. It is a tool that, when used in conjunction with other investigative efforts such as physical surveillance, can and has directly led to law enforcement saving lives and removing dangerous criminals from the street.

Before I describe how DHS uses this technology, I would like to dispel some common misconceptions about this technology and what it can and cannot do. Cell-site simulation technology allows law enforcement personnel to emit signals similar to a cell phone tower, resulting in nearby mobile phones and other wireless communication devices connecting to the simulated tower instead of the phone carrier's established tower. The simulator is then able to register the mobile device's unique identification number and identify an approximate location of the device. This technology does not provide the subscriber's account information; meaning no personal information, such as the account holder's name, address, or telephone number, can be detected by this device. Additionally, cell-site simulators provide only the relative signal strength and general direction of a subject's cellular telephone; the technology does not function as a GPS locator and cannot collect GPS location information from mobile devices. Cell-site simulators used by DHS do not collect the contents of any communication, including data

Document ID: 0.7.12327.26259-000004

contained on the phone itself, e.g., call content, transaction data, emails, text messages, contact lists, or images.

Within DHS, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the U.S. Secret Service (USSS) use this technology in the furtherance of their ongoing criminal investigations. HSI personnel deploy the devices during critical stages of investigations of a wide range of criminal activity, such as narcotics trafficking, human trafficking, and kidnapping, and to rescue the underage victims of child exploitation and prostitution rings. USSS personnel use this technology in support of its protective and investigative missions, and in its joint law enforcement operations with state and local law enforcement. By helping to locate a cellular device known to be used by a particular subject or to determine what mobile device a subject is carrying, this technology can greatly advance an investigation by enabling law enforcement agents to locate and arrest subjects who are otherwise difficult to find.

The new DHS policy regarding the use of cell-site simulator technology ensures that management controls and accountability processes are in place; defines the legal requirements and procedures for using the technology; articulates what is to be included in an application to the court seeking authorization to use the technology; defines strict guidelines on data collection and disposal; and ensures training and oversight.

Management controls and accountability are cornerstones of compliance for any policy. The DHS-wide policy requires that each Component that uses cell-site simulators develop operational policy or procedures to govern the use of the technology that is consistent with the overarching DHS policy, and to do so in coordination with the DHS Office of the General Counsel, Office of Policy, Privacy Office, and Office for Civil Rights and Civil Liberties. The policy also requires that each Component designate an executive point of contact, at the Component's headquarters level, who will have overall responsibility for implementation of this policy, and for promoting compliance with its provisions. The policy articulates supervisory approval requirements for deployment of the technology. Additionally, the policy requires that cell-site simulators be operated only by trained personnel who have been authorized by their Component to use the technology and whose training has been administered by a qualified Component expert. This includes training on privacy and civil liberties protections.

The Department's cell-site simulator policy requires that DHS agents or operators, prior to using a cell-site simulator, generally obtain a search warrant supported by probable cause. The DHS policy does provide for two exceptions to the warrant requirement consistent with applicable law. The first exception is in the case of "exigent circumstances" in which law enforcement needs are so compelling that they render a warrantless search objectively reasonable under the Fourth Amendment. Under the exigent circumstances exception, agents must still comply with the Pen Register Statute and with the policy's requirement to obtain the approval of a supervisor. The second

Document ID: 0.7.12327.26259-000004

exception is in cases of "exceptional circumstances" in which the law does not require a search warrant and obtaining a warrant would be impracticable. For example, in furtherance of protective duties, USSS may encounter exceptional circumstances that would make obtaining a search warrant impracticable. In these limited circumstances, USSS agents or operators must first obtain approval from executive-level personnel at USSS headquarters and the relevant U.S. Attorney, who will coordinate approval within the DOJ. DHS expects cases of exigent and exceptional circumstances to be limited.

When making any application to a court for the use of cell-site simulator technology, the Department's policy requires that DHS law enforcement personnel must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. DHS law enforcement personnel must consult with prosecutors in advance of using a cell-site simulator, to include state and local prosecutors when DHS is engaged with state and local law enforcement for non-federal cases. DHS works in close partnership with state and local law enforcement, and the Department provides technological assistance under a variety of circumstances. The DHS policy applies to all instances in which Department Components use cell-site simulators in support of other Federal agencies and/or state and local law enforcement agencies.

The DHS policy also requires that applications for the use of cell-site simulators inform the court that cellular devices in the area of influence of the cell-site simulator might experience a temporary disruption of service from the service provider. In the overwhelming majority of cases, any disruptions are exceptionally minor in nature and virtually undetectable to end users. To dispel another misconception – law enforcement use of cell-site simulator technology will not disconnect end users from calls in progress.

As previously stated, the scope of identification information collected when using cell-site simulator technology is limited to the phone manufacturer's or service provider's unique identifier (IMSI) for the device. Once these identifiers are obtained, law enforcement agents must undertake additional legal process (such as serving a subpoena on a service provider) to obtain subscriber information, or to initiate a wiretap pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in order to monitor a suspect's wire or electronic communications occurring over said device. Nevertheless, the DHS policy includes strict data collection and disposal standards to ensure that DHS law enforcement practices concerning the collection and retention of data are lawful and respect the important privacy interests of individuals. Specifically, the Department's policy for the use of cell-site simulators requires that immediately following the completion of a mission, the operator of a cell-site simulator must delete all data collected. For example, when the equipment is used to locate a known cellular phone used by a suspect, data is deleted as soon as the target is located; when the equipment is used to identify a particular device used by a suspect, data is deleted as soon as the suspect device is identified, and no less than once every 30 days. To further safeguard

Document ID: 0.7.12327.26259-000004

privacy, the policy also requires that prior to deploying equipment for another mission, the operator verifies that the equipment has been cleared of any previous operational data.

The Department's policy also requires that DHS Components implement an auditing program to ensure that the data is deleted in the manner described above. To the extent feasible, this auditing program includes hardware and software controls, for example through an equipment sign-in process that will include operator badge number and an affirmative acknowledgement by the operator that he or she is authorized by the Department to collect and view data.

DHS has been and remains committed to operating this equipment in a responsible manner. The recent implementation of this policy was meant to bring all DHS policies under a unified document and uniform DHS policy standard. The Department has always been committed to using cell-site simulators in a manner that is consistent with, and protects, the privacy rights of individuals.

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee, thank you for the opportunity to testify today. I look forward to answering your questions.

Document ID: 0.7.12327.26259-000004

From: Lan, Iris (ODAG)
Subject: FW: Stingray checklist
To: Jain, Samir (ODAG)
Sent: October 20, 2015 2:32 PM (UTC-04:00)
Attached: Cell-Site Simulator Policy Requirements Summary response 20151020-final.docx

FYI

From: (b)(6), (7)(C) per FBI (DO) (FBI) [mailto:(b)(6), (7)(C), (7)(E) per FBI]
Sent: Tuesday, October 20, 2015 11:11 AM
To: Hess, Amy S. (DO) (FBI); Lan, Iris (ODAG)
Subject: RE: Stingray checklist

Good morning Ms. Lan,

On behalf of EAD Hess, I am providing response to the Stingray Checklist. If you have any questions, please feel free to contact Amy or I.

Thank you,
(b)(6), (7)(C) p

(b)(6), (7)(C) per FBI
Special Assistant
Science and Technology Branch
(b)(6), (7)(C), (7)(E) per FBI
(b)(6), (7)(C), (7)(E) per FBI mobile

From: (b)(6), (7)(C) per FBI (DO) (FBI)
Sent: Thursday, October 15, 2015 4:46 PM
To: Hess, Amy S. (DO) (FBI)
Subject: Fwd: Stingray checklist

Amy - Please see Iris's note below. Can you please provide a POC that I can provide to Iris (or, please feel free to have your POC reach out to her directly) regarding cell site simulators?

Thanks much, (b)(6), (7)(C) pe

--
-------- Original message --------
From: "Lan, Iris (ODAG)" <(b) (6)
Date: 10/15/2015 1:35 PM (GMT-05:00)
To: (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>
Subject: Fwd: Stingray checklist

Hi (b)(6), (7)(C), can you help me find a good POC for the request below? Thanks, as always. Iris

Begin forwarded message:

From: "Jain, Samir (ODAG)"<(b) (6)
Date: October 15, 2015 at 1:33:29 PM EDT
To: "Lan, Iris (ODAG)"<(b) (6)>, "Grooms, Daniel (ODAG)"
<(b) (6)>, "Bonilla, Armando (ODAG)"
<(b) (6)>
Subject: FW: Stingray checklist

Hi all,

As you know, the DAG issued the policy re: DOJ use of cell-site simulators in early September, which imposes various requirements

on the LE components. Attached is a checklist of those requirements, some of which were supposed to have been done in the near term. I am hoping that each of you can check with your components (FBI, ATF, DEA, USMS) and confirm that they have in fact taken these steps (or if for some reason they haven't, a short term deadline by which they will do so). Elana is testifying next Wednesday re: the policy, so it would be good if she can say, if asked, that the components have in fact taken the steps necessary to comply with the policy. Feel free to cc me on emails to your components…. Thanks!

Samir

Document ID: 0.7.12339.9611

From: Jain, Samir (ODAG)
Subject: RE: Stingray - implementation checking in
To: Fried, Hannah (OLP)
Sent: October 20, 2015 5:09 PM (UTC-04:00)
Attached: Cell-Site Simulator Policy Requirements Summary response 20151020-final.....docx, FW_ Stingray checklist.eml, Re_ Stingray checklist.eml, CSS Checklist.pdf

Attached are the implementation reports….

From: Fried, Hannah (OLP)
Sent: Tuesday, October 20, 2015 12:52 PM
To: Jain, Samir (ODAG)
Subject: RE: Stingray - implementation checking in

Thanks again for following up about this. Did you all get the final word from FBI, DEA and ATF? We're doing the final rounds of prep for Elana this afternoon, for tomorrow's hearing, so I want to make sure we are good to go in addressing any implementation questions.

Thank you! Know you have a lot going on, and chasing this down can't be high on the list of favorite activities…. And let me know if it would be helpful for me just to check in with Danny directly; can do whatever is easiest for you.

From: Fried, Hannah (OLP)
Sent: Monday, October 19, 2015 7:20 PM
To: Jain, Samir (ODAG)
Subject: RE: Stingray - implementation checking in

Got it – thank you.

From: Jain, Samir (ODAG)
Sent: Monday, October 19, 2015 6:43 PM
To: Fried, Hannah (OLP)
Subject: RE: Stingray - implementation checking in

Sorry not to get back to you earlier – short answer is that USMS looks like they have taken the requisite steps; FBI is supposed to get back to us today, so will check in tomorrow morning if they haven't reported by then; have followed up with Danny re: ATF and DEA. Thx.

From: Fried, Hannah (OLP)
Sent: Monday, October 19, 2015 6:38 PM
To: Jain, Samir (ODAG)
Subject: RE: Stingray - implementation checking in

Document ID: 0.7.12327.26627

Hi again,

Sorry to follow up, but I did want to make sure we connected about this before the day was up. Give me a call, when you get a second? My desk is (b) (6) .

Thanks much!

Hannah

From: Fried, Hannah (OLP)
Sent: Monday, October 19, 2015 4:08 PM
To: Jain, Samir (ODAG)
Subject: Stingray - implementation checking in

Hey Samir – let me know when you have a moment to talk implementation.

Thanks,
Hannah
(b) (6)

Document ID: 0.7.12327.26627

From: Grooms, Daniel (ODAG)
Subject: FW: Stingray checklist
To: Jain, Samir (ODAG)
Sent: October 20, 2015 4:47 PM (UTC-04:00)
From DEA

-----Original Message-----
From: Gill, Mike R. [mailto:(b) (6)]
Sent: Tuesday, October 20, 2015 3:50 PM
To: BenAry, Michael P (DEA); Grooms, Daniel (ODAG); Quinn, Maura F. (DEA)
Subject: Re: Stingray checklist

Danny - See below from Maura Quinn on stingray policy progress. Let us know if you have any questions or need anything else. Thanks. - Mike

"Quinn, Maura F." <(b) (6) > wrote:

Gentlemen,
We have made good progress on implementing the new policy. Here are the action items that have been taken or are in progress:

- A message was sent to all DEA Offices implementing the DOJ Policy regarding the Use of Cell-Site Simulator Technology the same day the Policy was released.
- A Memorandum designating 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 was signed and disseminated by ADA Riley.
- We have provided a spreadsheet to each Office's Technical Operations Group to track the required DOJ statistics on cell-site simulator use. In addition, we have submitted a request through the CIO's Front Door process to design an interface that will allow users to electronically enter the required data and for reports to be generated from the resulting database.
- The Office of Investigative Technology has drafted additional training regarding the Policy which will include privacy and civil liberties training. We are in the process of coordinating with the other DOJ LEAs to come up with privacy and civil liberty training implementation recommendations for OPCL.
- (b)(5), (b)(7)(E) per DEA

Please let me know if you need anything else. Thanks, Maura

Document ID: 0.7.12327.26627-000003

From: Grooms, Daniel (ODAG)
Subject: Re: Stingray checklist
To: Jain, Samir (ODAG)
Sent: October 20, 2015 9:18 AM (UTC-04:00)

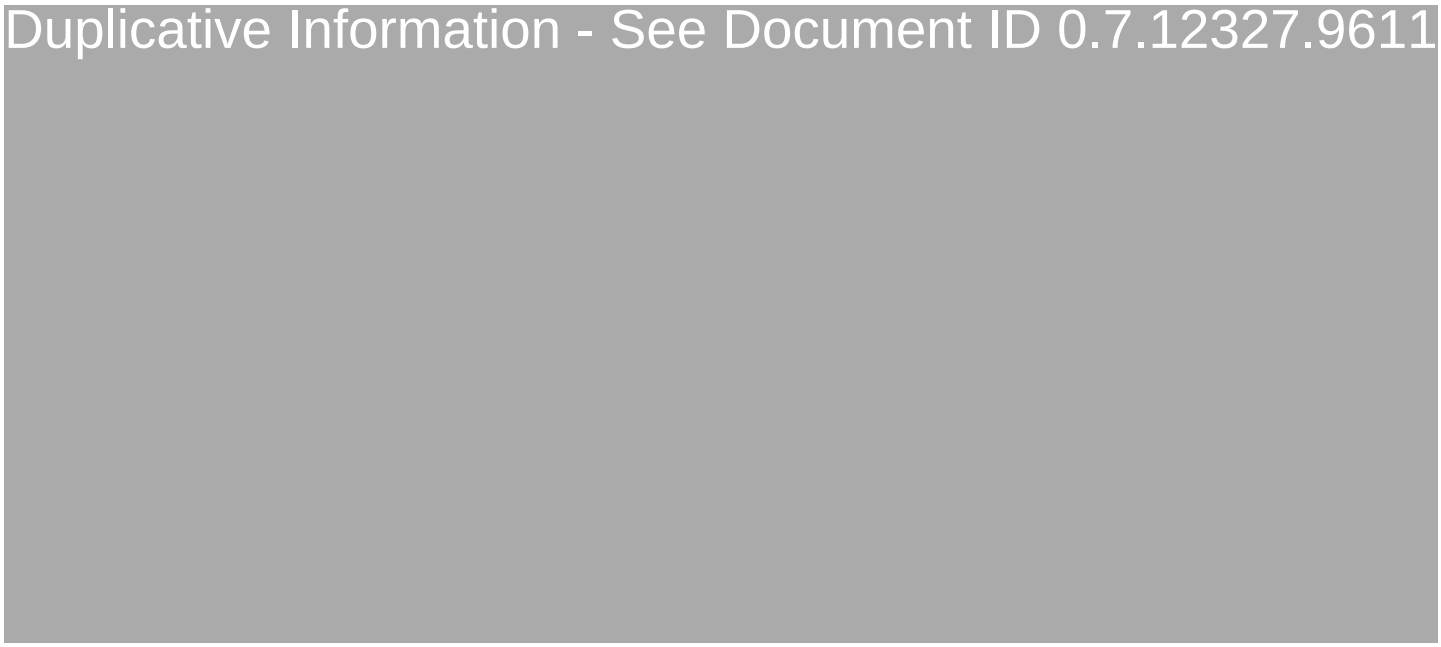
Here is the ATF response:

ATF has complied with all of the items on the checklist with the one exception noted below. Per our AD/Field Operations:

"There is one item that is pending that deals with identifying training protocols that includes civil liberties. TOB is awaiting guidance from the Department of Justice (DOJ) on the civil liberties aspect of the training to ensure we're consistent with their requirements as this is a broad area. TOB has drafted a training plan (with the ability to both deliver it electronically and in-person depending on the budget) and it will be implemented immediately after guidance is provided by DOJ on the civil liberties portion to ensure we meet DOJ's requirement in this important area."

On Oct 19, 2015, at 6:41 PM, Jain, Samir (ODAG) <(b) (6) > wrote:

> Just wanted to check in on whether you'd heard anything from ATF or DEA on this – Elana is testifying on Wednesday, so would be great if she can report that the components are on track…. Thanks.
>
> ---
> **From:** Jain, Samir (ODAG)
> **Sent:** Thursday, October 15, 2015 1:33 PM
> **To:** Lan, Iris (ODAG); Grooms, Daniel (ODAG); Bonilla, Armando (ODAG)
> **Subject:** FW: Stingray checklist



From: Wade Tyson, Jill C (OLA)
Subject: RE: CSS rider - OLP edits
To: Lynch, Michael K. (JMD)
Cc: Fried, Hannah (OLP); Pazur, Shannon (OLP)
Sent: October 29, 2015 6:27 PM (UTC-04:00)
Attached: SEC 563 Approps Amdt - cellsite simulator TPs - FINAL CLEAN 10.29.15.docx

To make Mike's life easier, here's the final clean version with the one FBI bullet added. Thanks again everyone.

From: Lynch, Michael K. (JMD)
Sent: Thursday, October 29, 2015 6:24 PM
To: Wade Tyson, Jill C (OLA)
Cc: Fried, Hannah (OLP); Pazur, Shannon (OLP)
Subject: Re: CSS rider - OLP edits

Thanks Jill and everyone who worked on this. I will make the edits to incorporate this.

Mike

Sent from my iPhone

On Oct 29, 2015, at 5:51 PM, Wade Tyson, Jill C (OLA) <(b) (6) > wrote:

> Mike: Given the time crunch, Hannah recommends keeping this bullet in what we send to the Hill. It was part of the TPs from this spring. Thanks.
>
> - (b)(5), (7)(E) per FBI

From: Wade Tyson, Jill C (OLA)
Sent: Thursday, October 29, 2015 5:46 PM
To: Fried, Hannah (OLP)
Cc: Pazur, Shannon (OLP); Lynch, Michael K. (JMD)
Subject: RE: CSS rider - OLP edits

> Thanks for your tweaks. We will use your version, which is helpful. Unfortunately we don't have time to circulate this any further as it is due to the Hill tomorrow.
> -JCT

From: Fried, Hannah (OLP)
Sent: Thursday, October 29, 2015 5:11 PM
To: Wade Tyson, Jill C (OLA)
Cc: Pazur, Shannon (OLP)

Subject: CSS rider - OLP edits

Hey Jill,

Wanted to share this with you. If you haven't already sent this to FBI (and I think [redacted] hasn't received this from OLA), you may want to get their perspective on what obstacles the rider might present to the LEAs. We (OLP) remember a similar proposal – from the summer maybe? – that we and they both had concerns about.

Let me know how else we can help!

<< File: SEC 563 - OLA edits - smp.docx >>

<SEC 563 - OLA edits - smp.docx>

Document ID: 0.7.12327.48583

SEC. 563. None of the funds made available by this Act may be used to operate or disseminate a cell-site simulator or IMSI catcher in the United States except pursuant to a court order that identifies an individual, account, address, or personal device.

- Cell-site simulators are critical tools that play an essential role in the Department's law enforcement and public safety missions. The Department has deployed this technology, for example, in efforts to locate and recover kidnapping victims, in operations to apprehend dangerous and violent fugitives, and in complex drug trafficking investigations.

- In September 2015, the Department announced a new policy governing its use of cell-site simulators. The policy applies Department-wide, establishing common principles for the use of cell-site simulators in support of domestic criminal investigations.

- The policy seeks to accomplish four basic objectives: first, to improve training and supervision; second, to establish a higher and more consistent legal standard; third, to enhance transparency and accountability; and, finally, to increase privacy protections.

- Generally, the policy requires law enforcement agents to obtain a search warrant supported by probable cause before using a cell-site simulator in domestic criminal investigations. There are two limited exceptions to the warrant requirement:

    - The first is in exigent circumstances – a well-established exception under Fourth Amendment law – where the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable.

    - The second limited exception is for cases in which the Fourth Amendment does not require a warrant *and* circumstances make obtaining a search warrant impracticable.

- In either case, however, agents still must comply with the provisions of the Pen Register Statute, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation.

- The FBI does not always know the individual, account or personal device being used, as we may only have information about a suspect using a phone in a particular area, which would not be as specific as an address. As a result, we are concerned that we could not use the technology to find an unknown bad guy using a phone in hiding in a rural place where we don't know the actual identity of the person yet or the phone used.

- As with other capabilities, the Department is committed to using the technology in a manner that is consistent with the Constitution and all other legal authorities, while respecting individuals' privacy and civil liberties.

Document ID: 0.7.12327.48583-000001

From: Groman, Marc
Subject: Stingray Privacy Act
To: Neuman, Karen; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Sent: November 3, 2015 10:22 AM (UTC-05:00)

This bill is consistent with current DHS/DOJ Guidelines on the use of cell-site simulators, right?

http://chaffetz.house.gov/sites/chaffetz.house.gov/files/Cell%20Site%20Simulator%20Bill.pdf

GOP chairman joins with Dems on bill to limit cellphone spying
JULIAN HATTEM//THE HILL
The Republican head of the House Oversight Committee is teaming up with a pair of Democrats to try to enact new limits on the government's use of controversial cellphone-tracking technology. Rep. Jason Chaffetz (R-Utah) on Monday introduced the Stingray Privacy Act to prevent federal, state and local government agencies from using the briefcase-sized devices without a warrant. The Stingray devices are also known as IMSI-catchers and cell-site simulators. They mimic cellphone towers in order to pick up identifying waves from people's phones that contain information about their contacts, text messages and other data. "The abuse of Stingrays and other cell-site simulators by individuals, including law enforcement, could enable gross violations of privacy," Chaffetz said in a statement on Monday. Reps. John Conyers, Jr. (D-Mich.) and Peter Welch (D-Vt.) had signed on as original co-sponsors, he said.

Marc M. Groman
Senior Advisor for Privacy
Office of the Director, OMB
Executive Office of the President
EEOB, Room 239
(b) (6)
(b) (6)

Document ID: 0.7.12327.6037

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Stingray Privacy Act
To: Harp, Jennifer C. (OPCL)
Sent: November 3, 2015 10:30 AM (UTC-05:00)

FYI

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 10:22 AM
To: Neuman, Karen; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Stingray Privacy Act
To: Young, Brian A. (OPCL); Proia, Andrew (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Sent: November 3, 2015 10:32 AM (UTC-05:00)

FYI

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 10:22 AM
To: Neuman, Karen; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Cantor, Jonathan
Subject: RE: Stingray Privacy Act
To: Groman, Marc; Neuman, Karen; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Sent: November 3, 2015 10:35 AM (UTC-05:00)

Thanks for this, Marc

From: Groman, Marc
Sent: Tuesday, November 03, 2015 10:22:25 AM
To: Neuman, Karen; Cantor, Jonathan; Erika Brown-Lee; Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Stingray Privacy Act
To: Brown Lee, Erika (ODAG)
Sent: November 3, 2015 10:55 AM (UTC-05:00)

Hi Erika,

I did a quick compare of the DOJ Stingray Policy and the draft HR Chaffetz bill. The DOJ Policy is broader in a few respects, including the exceptions for exigent circumstances. Please let me know if you'd like to discuss.

Thanks,
Kristi

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 10:22 AM
To: Neuman, Karen; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Young, Brian A. (OPCL)
Subject: RE: Stingray Privacy Act
To: Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL)
Sent: November 3, 2015 11:07 AM (UTC-05:00)

Hi Kristi.

I probably should know. But where can I find the current DHS/DOJ Guidelines on the use of cell-site simulators?

Thanks,
Brian

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, November 03, 2015 10:32 AM
To: Young, Brian A. (OPCL); Proia, Andrew (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Subject: FW: Stingray Privacy Act

FYI

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 10:22 AM
To: Neuman, Karen; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Neuman, Karen
Subject: RE: Stingray Privacy Act
To: Groman, Marc; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Sent: November 3, 2015 11:08 AM (UTC-05:00)

Thanks.

Karen Neuman
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy Office
Telephone: (b) (6)
Fax: 202-343-4010

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 in error, please reply immediately to the sender and delete this message. Thank you.

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 11:07 AM
To: Neuman, Karen; Cantor, Jonathan; Erika Brown-Lee; Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: RE: Stingray Privacy Act

No rush. I just wanted to flag it for you.

From: Neuman, Karen [mailto:(b)(6) per DHS]
Sent: Tuesday, November 3, 2015 10:57 AM
To: Groman, Marc <(b) (6) >; Cantor, Jonathan <(b)(6) per DHS >; Erika Brown-Lee <(b) (6) >; Lane Scott, Kristi Z (OPCL) <(b) (6) >; Riley, Kellie <(b)(6) per DHS >
Subject: RE: Stingray Privacy Act

On a call. Thanks for sharing. Will take a look.

Karen Neuman
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy Office
Telephone: (b) (6)
Fax: 202-343-4010

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 in error, please reply immediately to the sender and delete this message. Thank you.

From: Groman, Marc [mailto:(b) (6)]
Sent: Tuesday, November 03, 2015 10:22 AM

To: Neuman, Karen; Cantor, Jonathan; Erika Brown-Lee; Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6037

From: Young, Brian A. (OPCL)
Subject: Re: Stingray Privacy Act
To: Proia, Andrew (OPCL)
Sent: November 3, 2015 12:01 PM (UTC-05:00)

Thanks Andrew.

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

On Nov 3, 2015, at 11:57 AM, Proia, Andrew (OPCL) <(b) (6) > wrote:

> http://www.justice.gov/opa/file/767321/download
>
> ---
>
> **From:** Young, Brian A. (OPCL)
> **Sent:** Tuesday, November 03, 2015 11:07 AM
> **To:** Lane Scott, Kristi Z (OPCL)
> **Cc:** Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL)
> **Subject:** RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.55677

From: Harp, Jennifer C. (OPCL)
Subject: RE: Stingray Privacy Act
To: Young, Brian A. (OPCL); Lane Scott, Kristi Z (OPCL)
Cc: Proia, Andrew (OPCL)
Sent: November 3, 2015 2:42 PM (UTC-05:00)

Hi Brian,

The relevant policies are below.

DOJ: http://www.justice.gov/opa/file/767321/download

DHS:
https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf

---

From: Young, Brian A. (OPCL)
Sent: Tuesday, November 03, 2015 11:07 AM
To: Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL)
Subject: RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.55677

From: Young, Brian A. (OPCL)
Subject: RE: Stingray Privacy Act
To: Harp, Jennifer C. (OPCL)
Sent: November 3, 2015 2:43 PM (UTC-05:00)

Thanks Jenny

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Harp, Jennifer C. (OPCL)
Sent: Tuesday, November 03, 2015 2:42 PM
To: Young, Brian A. (OPCL); Lane Scott, Kristi Z (OPCL)
Cc: Proia, Andrew (OPCL)
Subject: RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.55968

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Stingray Privacy Act
To: Harp, Jennifer C. (OPCL); Young, Brian A. (OPCL)
Cc: Proia, Andrew (OPCL)
Sent: November 3, 2015 2:46 PM (UTC-05:00)

Thanks, Jenny. I quickly compared the bill with the DOJ policy. I (b) (5) [redacted]. I think there are other slight differences were the bill doesn't align with the DOJ policy. Thoughts? Don't worry about spending too much time on this. I'll let you know what Erika decides.

From: Harp, Jennifer C. (OPCL)
Sent: Tuesday, November 03, 2015 2:42 PM
To: Young, Brian A. (OPCL); Lane Scott, Kristi Z (OPCL)
Cc: Proia, Andrew (OPCL)
Subject: RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.55968

From: Brown Lee, Erika (ODAG)
Subject: RE: Stingray Privacy Act
To: Neuman, Karen; Groman, Marc; Cantor, Jonathan; Lane Scott, Kristi Z (OPCL); Riley, Kellie
Sent: November 3, 2015 2:57 PM (UTC-05:00)

Thanks, Marc. We'll also take a look.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
(b) (6)

From: Neuman, Karen [mailto:(b)(6) per DHS]
Sent: Tuesday, November 03, 2015 11:08 AM
To: Groman, Marc; Cantor, Jonathan; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Riley, Kellie
Subject: RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.6038

From: Harp, Jennifer C. (OPCL)
Subject: RE: Stingray Privacy Act
To: Young, Brian A. (OPCL); Lane Scott, Kristi Z (OPCL)
Cc: Proia, Andrew (OPCL)
Sent: November 4, 2015 6:26 PM (UTC-05:00)

Here is the story on the draft bill: http://www.nextgov.com/defense/2015/11/new-bill-would-ban-warrantless-cellphone-tracking/123360/?oref=nextgov_today_nl

---

From: Young, Brian A. (OPCL)
Sent: Tuesday, November 03, 2015 3:29 PM
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Cc: Proia, Andrew (OPCL)
Subject: RE: Stingray Privacy Act

Hi all.

(b)(5) per FBI

(b)(5) per FBI

Thanks,
Brian

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, November 03, 2015 2:46 PM
To: Harp, Jennifer C. (OPCL); Young, Brian A. (OPCL)
Cc: Proia, Andrew (OPCL)
Subject: RE: Stingray Privacy Act

Duplicative Information - See Document ID 0.7.12327.55971

From: Cardwell, Christine (ODAG)
Subject: RE: Cell-site Simulator Policy
To: Lane Scott, Kristi Z (OPCL)
Cc: Brown Lee, Erika (ODAG)
Sent: November 12, 2015 5:01 PM (UTC-05:00)

Hi Kristi,

Please use conference call in number: (b) (6) ; Passcode: (b) (6)

Thanks, Christine

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, November 12, 2015 3:57 PM
To: Cardwell, Christine (ODAG)
Cc: Brown Lee, Erika (ODAG)
Subject: FW: Cell-site Simulator Policy

Hi Christine,

Can you reserve a conference line for 11/18 at 2:00?

Thanks,

Kristi

From: Quinn, Maura F. [mailto: (b) (6)]
Sent: Thursday, November 12, 2015 2:18 PM
To: Lane Scott, Kristi Z (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: RE: Cell-site Simulator Policy

Sure, either day in the afternoon works for me.

From: Lane Scott, Kristi Z (OPCL) (JMD)
Sent: Monday, November 09, 2015 5:27 PM
To: Quinn, Maura F.
Cc: Brown Lee, Erika (ODAG) (JMD)
Subject: RE: Cell-site Simulator Policy

Maura,

Thanks for the update. Are you available 11/17 or 11/18 for a call?

Best,

Kristi

Kristi Lane Scott
Acting Director
Office of Privacy and Civil Liberties
U.S. Department of Justice
1331 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20530

Document ID: 0.7.12327.6059

(b) (6) (office)
(b) (6) (mobile)
202.307.0693 (fax)
(S) (b) (6)
(TS) (b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Quinn, Maura F. [mailto:(b) (6)]
Sent: Wednesday, November 04, 2015 10:07 AM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: RE: Cell-site Simulator Policy

Hi Erica,
I am at a conference tomorrow and Friday but I have attached a draft of the privacy section of our training for you to take a look at. I am available to discuss next week. Thanks, Maura

---

From: Brown Lee, Erika (ODAG) (JMD)
Sent: Tuesday, November 03, 2015 5:57 PM
To: Quinn, Maura F.
Cc: Lane Scott, Kristi Z (OPCL) (JMD)
Subject: Cell-site Simulator Policy

Hi Maura – thanks for your message. Are you available Thursday afternoon or Friday morning to discuss the privacy training section of the policy?

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Cell-site Simulator Policy
To: Quinn, Maura F. (DEA)
Cc: Brown Lee, Erika (ODAG)
Sent: November 17, 2015 11:38 AM (UTC-05:00)

Hi Maura,

I'll call you now to confirm dates/times.

Thanks,

Kristi

From: Quinn, Maura F. [mailto:(b) (6)]
Sent: Tuesday, November 17, 2015 11:36 AM
To: Lane Scott, Kristi Z (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: RE: Cell-site Simulator Policy

Hi Kristi,
Did we settle on a day/time to discuss? Thanks, Maura

From: Quinn, Maura F.
Sent: Thursday, November 12, 2015 2:18 PM
To: Lane Scott, Kristi Z (OPCL) (JMD)
Cc: Brown Lee, Erika (ODAG) (JMD)
Subject: RE: Cell-site Simulator Policy

Duplicative Information - See Document ID 0.7.12327.6059

Lane Scott, Kristi Z (OPCL)

Subject:	Cell Site Simulator Training
Location:	Call
Start:	Friday, November 20, 2015 10:00 AM
End:	Friday, November 20, 2015 10:30 AM
Recurrence:	(none)
Meeting Status:	Meeting organizer
Organizer:	Lane Scott, Kristi Z (OPCL)
Required Attendees:	Quinn, Maura F. (DEA); Brown Lee, Erika (ODAG); Cardwell, Christine (ODAG)

Erika/Kristi will call Maura.

Document ID: 0.7.12327.55995

From: Lane Scott, Kristi Z (OPCL)
Subject: Cell Site Simulator Training
To: Quinn, Maura F. (DEA); Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Cardwell, Christine (ODAG)
Sent: November 17, 2015 11:46 AM (UTC-05:00)

Erika/Kristi will call Maura.

Document ID: 0.7.12327.5062

From: Lane Scott, Kristi Z (OPCL)
Subject: Cell Site Sim Call
To: Brown Lee, Erika (ODAG)
Sent: November 20, 2015 9:02 AM (UTC-05:00)

Hi Erika,

I'm (b) (6) today. I can call in to the cell site simulator call at 10:00.

Kristi Lane Scott
DOJ/OPCL

Document ID: 0.7.12327.6083

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Cell-site Simulator Policy
To: Proia, Andrew (OPCL); Harp, Jennifer C. (OPCL)
Cc: Brown Lee, Erika (ODAG); Young, Brian A. (OPCL); Mayer, Hannah J. (OPCL)
Sent: November 23, 2015 4:33 PM (UTC-05:00)
Attached: Protecting Privacy and Civil Liberties When Using Cell-Site Simulators.docx

Andrew,

As we discussed, we'll need to prepare 3-5 slides relating to the Privacy Act's minimization and retention requirements. Let's aim for a draft by COB 12/2.

Thanks,

Kristi

From: Quinn, Maura F. [mailto:(b) (6)]
Sent: Tuesday, November 17, 2015 11:43 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: FW: Cell-site Simulator Policy

Duplicative Information - See Document ID 0.7.12327.55997

From: Goldsmith, Andrew (ODAG)
Subject: RE: Stingray Brady/Giglio Guidance
To: (b)(6), (7)(C) per EOUSA (USACO); Tyrangiel, Elana (OLP); Jain, Samir (ODAG); OBrien, Paul; Pazur, Shannon (OLP)
Cc: Wilkinson, Monty (USAEO); Wong, Norman (USAEO)
Sent: November 24, 2015 3:00 PM (UTC-05:00)
Attached: B&G Cell-site Simulator Memo.pdf

This is what the package will look like. I made minor changes to the memo (first and last paragraphs). I plan on sending this out tomorrow, so please let me know if you catch any typos, have suggested edits, etc. thanks.

-----Original Message-----
From: (b)(6), (7)(C) per EOUSA (USACO) [mailto:(b)(6), (7)(C) per EOUSA]
Sent: Monday, November 23, 2015 4:59 PM
To: Tyrangiel, Elana (OLP); Goldsmith, Andrew (ODAG); Jain, Samir (ODAG); OBrien, Paul; Pazur, Shannon (OLP)
Cc: Wilkinson, Monty (USAEO); Wong, Norman (USAEO)
Subject: RE: Stingray Brady/Giglio Guidance

I'm with Elana -- just the policy, not the cover memo, which doesn't add anything for this purpose. John

-----Original Message-----
From: Tyrangiel, Elana (OLP) [mailto:(b) (6)]
Sent: Monday, November 23, 2015 1:50 PM
To: Goldsmith, Andrew (ODAG) (JMD); (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG) (JMD); OBrien, Paul (CRM); Pazur, Shannon (OLP) (JMD)
Cc: Wilkinson, Monty (USAEO); Wong, Norman (USAEO)
Subject: RE: Stingray Brady/Giglio Guidance

This is a copy of the policy with the DAG's memo attached. Because the memo is directed to component heads and U.S. Attorneys (and requests further distribution), I'm not sure it makes sense to send it -- it may make more sense simply to send the policy. But see what you think.

Thanks,
Elana

-----Original Message-----
From: Goldsmith, Andrew (ODAG)
Sent: Monday, November 23, 2015 2:15 PM
To: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); OBrien, Paul; Pazur, Shannon (OLP)
Cc: Wilkinson, Monty (USAEO); Wong, Norman (USAEO)
Subject: RE: Stingray Brady/Giglio Guidance

Here's the "final" version. I've also attached the original 9/3/15 guidance memo. Was there a cover memo to that 9/3 memo (and, if so, should it be resent in this distribution)? I can send out the new memo to all Crim Chiefs and ask that they distribute it all federal prosecutors in their office (and do the same with CRM, and NSD too?Any other Main litigating divisions?). Or have EOUSA do something similar. And I can send it to the POCs for FBI, DEA, ATF, and USMS and ask that they distribute to all agency counsel. Thoughts?

-----Original Message-----
From: (b)(6), (7)(C) per EOUSA (USACO) [mailto:(b)(6), (7)(C) per EOUSA]

Document ID: 0.7.12327.24320

Sent: Thursday, November 19, 2015 10:43 AM
To: Goldsmith, Andrew (ODAG); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); OBrien, Paul; Pazur, Shannon (OLP)
Cc: Wilkinson, Monty (USAEO); Wong, Norman (USAEO)
Subject: RE: Stingray Brady/Giglio Guidance

Given that this is directed to DOJ prosecutors and agency counsel, is there an easy way to push it out just to that audience?

-----Original Message-----
From: Goldsmith, Andrew (ODAG) [mailto:(b) (6)]
Sent: Thursday, November 19, 2015 8:04 AM
To: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG) (JMD); Tyrangiel, Elana (OLP) (JMD); OBrien, Paul (CRM); Pazur, Shannon (OLP) (JMD)
Subject: RE: Stingray Brady/Giglio Guidance

I've received no comments from the LE Components, so we may be ready to send this out soon. Any initial thoughts on the sender/format/etc., particularly in light of how the initial guidance memo was distributed?

-----Original Message-----
From: Goldsmith, Andrew (ODAG)
Sent: Tuesday, November 17, 2015 9:46 AM
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS)
Cc: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); (b)(6), (7)(C) per EOUSA (USACAC); Fried, Hannah (OLP); OBrien, Paul; (b)(6), (7)(C) per EOUSA (USAILN); Pazur, Shannon (OLP)
Subject: RE: Stingray Brady/Giglio Guidance

Thank you all for your helpful comments. Based on those comments, here's a draft version of the revised guidance we plan to distribute in the next few days.

-----Original Message-----
From: Goldsmith, Andrew (ODAG)
Sent: Friday, September 25, 2015 3:28 PM
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); Goggin, Wendy H. (DEA); Driscoll, Derrick (USMS)
Cc: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); (b)(6), (7)(C) per EOUSA (USACAC); Fried, Hannah (OLP); OBrien, Paul; (b)(6), (7)(C) per EOUSA (USAILN)
Subject: RE: Stingray Brady/Giglio Guidance

Colleagues - attached please find guidance we've drafted to address the potential Brady/Giglio implications of the recently-issued "Department of Justice Policy Guidance:
Use of Cell-Site Simulator Technology." The plan is to issue this guidance to federal prosecutors and agency counsel (with the expectation that agency counsel would then distribute it to managers, supervisors, and line agents, as they deem appropriate). If you can take a look at this and share your thoughts by COB next Friday, October 2nd, it would be greatly appreciated. Enjoy the weekend - Andrew

Document ID: 0.7.12327.24320

From: Goldsmith, Andrew (ODAG)
Subject: Brady and Giglio Issues Associated with Operating Cell-Site Simulator Technology
To: 'USAEO-CrimChiefs'; USAEO-CrimDiscoveryCoordinators-all
Cc: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); OBrien, Paul; Pazur, Shannon (OLP)
Sent: November 25, 2015 2:15 PM (UTC-05:00)
Attached: B&G Cell-site Simulator Memo.pdf

Criminal Chiefs/Criminal Discovery Coordinators:

On September 3, 2015, the Department issued a policy concerning the use of cell-site simulator technology. Over the past few months, we've been developing guidance regarding the potential *Brady* and *Giglio* issues that may stem from use of that technology. Attached to this email is a memorandum reflecting this guidance, as well as the policy itself. The guidance was developed in conjunction with the ad hoc Criminal Discovery Working Group, OLP, the AGAC, and CRM, with input from the FBI, DEA, ATF, and USMS. **Please distribute the memorandum to all prosecutors in your office.** Similarly, the FBI, DEA, ATF, and USMS will be distributing the guidance to counsel who work on cases that may involve the use of cell-site simulators in their field offices and at headquarters.

Recognize that while the September 2015 policy itself is a publicly-available document, this guidance memorandum is *not* intended to be shared outside the Department.

Please let me know if you have any questions. And I hope everyone has a safe and enjoyable Thanksgiving holiday. – Andrew

Document ID: 0.7.12327.24343

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

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

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

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

BACKGROUND

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

Basic Uses

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

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

Document ID: 0.7.12327.24343-000001

How They Function

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

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

What They Do and Do Not Obtain

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

MANAGEMENT CONTROLS AND ACCOUNTABILITY[2]

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

1. Department personnel must be trained and supervised appropriately. Cell-site simulators may be operated only by trained personnel who have been authorized by their agency to use the technology and whose training has been administered by a qualified agency component or expert.

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

Document ID: 0.7.12327.24343-000001

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.

Document ID: 0.7.12327.24343-000001

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

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

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

In this circumstance, the use of a cell-site simulator still must comply with the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, which ordinarily requires judicial authorization before use of the cell-site simulator, based on the government's certification that the information sought is relevant to an ongoing criminal investigation. In addition,

---

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

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

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

Document ID: 0.7.12327.24343-000001

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

APPLICATIONS FOR USE OF CELL-SITE SIMULATORS

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

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

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

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

---

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

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

Document ID: 0.7.12327.24343-000001

DATA COLLECTION AND DISPOSAL

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

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.

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

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

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

STATE AND LOCAL PARTNERS

The Department often works closely with its State and Local law enforcement partners and provides technological assistance under a variety of circumstances. This policy applies to all instances in which Department components use cell-site simulators in support of other Federal agencies and/or State and Local law enforcement agencies.

TRAINING AND COORDINATION, AND ONGOING MANAGEMENT

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

---

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

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

Document ID: 0.7.12327.24343-000001

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.

Document ID: 0.7.12327.24343-000001

From: Goldsmith, Andrew (ODAG)
Subject: RE: Stingray Brady/Giglio Guidance
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS)
Cc: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); Pazur, Shannon (OLP); OBrien, Paul
Sent: November 25, 2015 2:20 PM (UTC-05:00)
Attached: B&G Cell-site Simulator Memo.pdf

Attached to this email is the final version of the memorandum regarding the potential Brady and Giglio issues that may stem from use of cell-site simulator technology, as well as the September 2015 policy itself. Please distribute the memorandum to counsel in your respective field offices and at headquarters who work on cases that may involve the use of cell-site simulators.

Recognize that while the September 2015 policy itself is a publicly-available document, this guidance memorandum is not intended to be shared outside the Department.

Please let me know if you have any questions. And I hope everyone has a safe and enjoyable Thanksgiving holiday. – Andrew

-----Original Message-----
From: Goldsmith, Andrew (ODAG)
Sent: Tuesday, November 17, 2015 9:46 AM
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS)
Cc: (b)(6), (7)(C) per EOUSA (USACO); Jain, Samir (ODAG); Tyrangiel, Elana (OLP); (b)(6), (7)(C) per EOUSA (USACAC); Fried, Hannah (OLP); OBrien, Paul; (b)(6), (7)(C) per EOUSA (USAILN); Pazur, Shannon (OLP)
Subject: RE: Stingray Brady/Giglio Guidance

Duplicative Information - See Document ID 0.7.12327.24320

From: Goldsmith, Andrew (ODAG)
Subject: Fwd: Brady and Giglio Issues Associated with Operating Cell-Site Simulator Technology
To: Pierce, Emily (OPA)
Cc: Axelrod, Matthew (ODAG); Childs, Heather G. (ODAG); Jain, Samir (ODAG)
Sent: November 25, 2015 3:07 PM (UTC-05:00)
Attached: B&G Cell-site Simulator Memo.pdf, ATT00001.htm

Emily - Given how much press the Stingray policy itself received, we wanted to make you aware of the Brady/Giglio guidance memo (and the fact that it's not intended to be made public), just so you're not blind-sided if you receive a press inquiry. Enjoy the holiday! - Andrew

Sent from my iPhone

Begin forwarded message:

From: "Goldsmith, Andrew (ODAG)" <(b) (6) >
To: "'USAEO-CrimChiefs'" <USAEO-CrimChiefs@usa.doj.gov>, "USAEO-CrimDiscoveryCoordinators-all" <USAEO-CrimDiscoveryCoordinators-all@usa.doj.gov>
Cc: (b)(6), (7)(C) per EOUSA (USACO)" <(b)(6), (7)(C) per EOUSA>, "Jain, Samir (ODAG)" <(b) (6) >, "Tyrangiel, Elana (OLP)" <(b) (6) >, "OBrien, Paul" <(b) (6) >, "Pazur, Shannon (OLP)" <(b) (6) >
Subject: Brady and Giglio Issues Associated with Operating Cell-Site Simulator Technology

Duplicative Information - See Document ID 0.7.12327.24343

From: Proia, Andrew (OPCL)
Subject: Cell Site P&CL Slides
To: Harp, Jennifer C. (OPCL); Lane Scott, Kristi Z (OPCL)
Sent: November 30, 2015 4:48 PM (UTC-05:00)
Attached: Protecting Privacy and Civil Liberties When Using Cell-Site Simulators.docx, Privacy & Civil Liberties Training--Cell Site Simulators (v1).pptx

Kristi & Jenny,
Attached to this e-mail is my first draft of the privacy and civil liberties training slides for DEA. I took a (b) (5) approach and (b) (5) . The final two slides are the best practices prepared by DEA for their operators and case agents (see attached word document).

The slides are intentionally bland as I iron out the slide's content. If you both agree that the content is on the right track, I can format the slides in a manner consistent with our other OPCL slide decks.

I'm open to any thoughts or comments you might have.

Thanks!

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Bordley, Ed (USMS)
Subject: Cell Site Simulator Training
To: Lane Scott, Kristi Z (OPCL)
Sent: December 4, 2015 10:53 AM (UTC-05:00)
Attached: TOG PCL training.eml

Hi Kristi,
I've attached a PowerPoint that I'd like to use portions of for the USMS cell site simulator training responsibility. We've included ethics training as well.

Thanks much,
Ed Bordley
Associate General Counsel
U.S. Marshals Service
Washington, DC 20530-1000
(b) (6) (off)
(703) 603-7004 (fax)

Document ID: 0.7.12327.56307

From: (b)(6), (7)(C), (7)(F) per USMS (USMS)
Subject: TOG PCL training
To: (b)(6), (7)(C), (7)(F) per USMS (USMS); Bordley, Ed (USMS)
Sent: November 25, 2015 11:50 AM (UTC-05:00)
Attached: tog pcl 11-15.pptm

(b)(6), (7)(C), /Ed,

Attached is a draft TOG PCL PPT for you to review. I think it gives us a good starting point for this task.

Thanks,
(b)(6), (7)(C), (7)(F) per USMS

Document ID: 0.7.12327.56307-000001

From: Lane Scott, Kristi Z (OPCL)
Subject: Fwd: Cell Site Simulator Training
To: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL); Young, Brian A. (OPCL)
Sent: December 4, 2015 11:42 AM (UTC-05:00)
Attached: TOG PCL training.eml, ATT00001.htm

J/A,

Please review and incorporate any relevant points into the DEA slide deck.

Thanks,
Kristi

Begin forwarded message:

From: "Bordley, Ed (USMS)" <(b) (6)>
Date: December 4, 2015 at 10:53:02 AM EST
To: "Lane Scott, Kristi Z (OPCL)" <(b) (6)>
Subject: Cell Site Simulator Training

Duplicative Information - See Document ID 0.7.12327.56307

From: Lane Scott, Kristi Z (OPCL)
Subject: Fwd: Cell-site Simulator Training Materials
To: Brown Lee, Erika (ODAG)
Sent: December 4, 2015 11:42 AM (UTC-05:00)

FYI

Begin forwarded message:

From: "Proia, Andrew (OPCL)" <(b) (6) >
Date: December 4, 2015 at 11:33:38 AM EST
To: "Quinn, Maura F. (DEA)" <(b) (6) >
Cc: "Lane Scott, Kristi Z (OPCL)" <(b) (6) >
Subject: Cell-site Simulator Training Materials

Ms. Quinn,

I am assisting Kristi and Erika with your request for privacy training materials in relation to the recent cell-site simulator policy. We expect to have the prepared materials to you within the next week.

If you have any questions or comments, please do not hesitate to get in contact with me.

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Brown Lee, Erika (ODAG)
Subject: OPCL Resources
To: Lofthus, Lee J (JMD); Lauria, Jolene A (JMD)
Sent: December 7, 2015 7:38 PM (UTC-05:00)

Lee, Jolene,

I'm writing to follow up on our meeting last month regarding resources for OPCL, as the circumstances for the Department's privacy office have grown even more critical since we met.

(b) (5) [redacted]

1. (b) (5) [redacted]
2. (b) (5) [redacted]
3. (b) (5) [redacted]
4. (b) (5) [redacted]
5. (b) (5) [redacted]
6. (b) (5) [redacted]
7. (b) (5) [redacted]
8. (b) (5) [redacted]

(b) (5) [redacted]

I very much appreciate all your efforts to assist OPCL. Please let me know if there is any additional information I can provide or if you'd like to discuss further.

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice

Document ID: 0.7.12327.6086

950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

Document ID: 0.7.12327.6086

From: Lane Scott, Kristi Z (OPCL)
Subject: Fwd: OPCL Resources
To: Harp, Jennifer C. (OPCL)
Sent: December 7, 2015 7:55 PM (UTC-05:00)

FYI

Kristi Lane Scott
DOJ/OPCL

Begin forwarded message:

From: "Brown Lee, Erika (ODAG)" <(b) (6) >
Date: December 7, 2015 at 7:37:30 PM EST
To: "Lofthus, Lee J (JMD)" <(b) (6) >, "Lauria, Jolene A (JMD)" <(b) (6) >
Subject: OPCL Resources

Duplicative Information - See Document ID 0.7.12327.6086

From: Proia, Andrew (OPCL)
Subject: FW: DOJ Cell-site Simulator P/CL Slides
To: Lane Scott, Kristi Z (OPCL); Young, Brian A. (OPCL); Harp, Jennifer C. (OPCL)
Sent: December 21, 2015 2:52 PM (UTC-05:00)
Attached: Privacy & Civil Liberties Training--Cell Site Simulators (v2).pptx, DOJ Policy-Use of Cell Site Simulator Technology.pdf

All,

A friendly reminder of the P/CL slides for CSS I've prepared for review. If you have any comments, please let me know.

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT/DELIBERATIVE PROCESS PRIVILEGED

From: Proia, Andrew (OPCL)
Sent: Friday, December 11, 2015 9:28 AM
To: Lane Scott, Kristi Z (OPCL); Young, Brian A. (OPCL); Harp, Jennifer C. (OPCL)
Subject: DOJ Cell-site Simulator P/CL Slides

All,

Please find attached to this e-mail the updated cell-site simulator "training" slides.

You'll notice that I added (b) (5) . However, I don't go into too much detail on this section, as (b) (5)

Also, I've added supplemental information in the notes below the slides to help explain the slide content.

I'd appreciate any feedback before we send this out. I'm happy to answer any questions, as well.

Enjoy!

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

Document ID: 0.7.12327.56577

From: Proia, Andrew (OPCL)
Subject: CSS P/CL Updated Slides
To: Lane Scott, Kristi Z (OPCL)
Sent: December 22, 2015 4:48 PM (UTC-05:00)
Attached: Privacy & Civil Liberties Training--Cell Site Simulators (v3).pptx

Kristi,

Please review these updated slides. Once approved, I can send them to Erika for review.

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

Document ID: 0.7.12327.56607

From: Proia, Andrew (OPCL)
Subject: FW: Cell Site Simulator Technology--Privacy & Civil Liberties Slides
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: December 30, 2015 2:36 PM (UTC-05:00)
Attached: Privacy & Civil Liberties Training--Cell Site Simulators (v3).pptx

Erika,

This is just a friendly reminder related to the prepared privacy and civil liberties slides for the Department's use of cell-site simulator technology.

Please let me know if you have any questions.

Thanks, Erika!

Andrew

From: Proia, Andrew (OPCL)
Sent: Wednesday, December 23, 2015 12:03 PM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); Young, Brian A. (OPCL); Harp, Jennifer C. (OPCL)
Subject: Cell Site Simulator Technology--Privacy & Civil Liberties Slides

Duplicative Information - See Document ID 0.7.12327.6096

From: Brown Lee, Erika (ODAG)
Subject: RE: Cell Site Simulator Technology--Privacy & Civil Liberties Slides
To: Proia, Andrew (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: January 4, 2016 5:39 PM (UTC-05:00)
Attached: Privacy Civil Liberties Training--Cell Site Simulators (v3)- - EBL edits.pptx

Hi Andrew – thanks again for your work and your patience with my review. As I mentioned on our call, the slide deck is very well done. Attached are a few minor edits. As I couldn't get the redline feature to work, the edits are in comment boxes. Let me know if they don't come through.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel:(b) (6)
(b) (6)
TS:(b) (6)

From: Proia, Andrew (OPCL)
Sent: Wednesday, December 30, 2015 2:36 PM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: FW: Cell Site Simulator Technology--Privacy & Civil Liberties Slides

Duplicative Information - See Document ID 0.7.12327.6097

From: Proia, Andrew (OPCL)
Subject: OPCL P/CL Slides---Cell Site Simulator Technology Policy
To: Quinn, Maura F. (DEA)
Cc: Lane Scott, Kristi Z (OPCL); Brown Lee, Erika (ODAG)
Sent: January 6, 2016 11:12 AM (UTC-05:00)
Attached: Privacy & Civil Liberties Training--Cell Site Simulators (1-5-2016).pptx

Maura,

I apologize for the delay. Please find attached to this e-mail the prepared privacy and civil liberties training slides regarding the Department's cell-site simulator technology policy.

If you have any questions or comments, please feel free to get in contact with me, Erika, or Kristi.

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Proia, Andrew (OPCL)
Subject: RE: Cell Site Simulator Technology--Privacy & Civil Liberties Slides
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: January 6, 2016 11:18 AM (UTC-05:00)

Thanks, Erika!

I was able to make the necessary changes proposed in your comment bubbles and passed along the slides to DEA.

Please let me know if I can be of any additional assistance.

Regards,

Andrew A. Proia
Attorney Advisor
U.S. Department of Justice
Office of Privacy and Civil Liberties (OPCL)
National Place Building, Suite 1000
1331 Pennsylvania Avenue NW
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)
(b) (6)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Brown Lee, Erika (ODAG)
Sent: Monday, January 04, 2016 5:39 PM
To: Proia, Andrew (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: RE: Cell Site Simulator Technology--Privacy & Civil Liberties Slides

Duplicative Information - See Document ID 0.7.12327.6709

From: Quinn, Maura F.
Subject: RE: OPCL P/CL Slides---Cell Site Simulator Technology Policy
To: Proia, Andrew (OPCL)
Cc: Lane Scott, Kristi Z (OPCL); Brown Lee, Erika (ODAG)
Sent: January 6, 2016 5:01 PM (UTC-05:00)

Great, thanks. We'll take a look and get back to you with any comments we have.

From: Proia, Andrew (OPCL) (JMD)
Sent: Wednesday, January 06, 2016 11:12 AM
To: Quinn, Maura F.
Cc: Lane Scott, Kristi Z (OPCL) (JMD); Brown Lee, Erika (ODAG) (JMD)
Subject: OPCL P/CL Slides---Cell Site Simulator Technology Policy

Duplicative Information - See Document ID 0.7.12327.6711

From: Quinn, Maura F.
Subject: FW: OPCL P/CL Slides---Cell Site Simulator Technology Policy
To: Proia, Andrew (OPCL)
Cc: Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL)
Sent: January 8, 2016 11:20 AM (UTC-05:00)

Hi Andrew,
We thought the training looked really good, thanks for putting it together. We only had a few comments/suggestions, please see below. Thanks, Maura

Slide # 7: recommend revising to read: (b) (5) [redacted] This is important because (b) (5) [redacted]

Slides # 9- #11: (b) (5) [redacted]

- @ slide 10: (b) (5) [redacted]
- @ slide 9 (in notes): (b) (5) [redacted]

RECOMMEND that this (b) (5) [redacted]

Similarly, slide # 10 should be revised to include an additional bullet:

(b) (5) [redacted]

This approach is similar to (b) (5) [redacted]

- (b) (5) [redacted]

From: Proia, Andrew (OPCL) (JMD)
Sent: Wednesday, January 06, 2016 11:12 AM
To: Quinn, Maura F.
Cc: Lane Scott, Kristi Z (OPCL) (JMD); Brown Lee, Erika (ODAG) (JMD)
Subject: OPCL P/CL Slides---Cell Site Simulator Technology Policy

Duplicative Information - See Document ID 0.7.12327.6711

From: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum
To: Lane Scott, Kristi Z (OPCL)
Sent: January 19, 2016 5:19 PM (UTC-05:00)

You're it! Just tried you.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel:(b) (6)
(b) (6)
TS:(b) (6)

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, January 19, 2016 12:12 PM
To: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum

I went to Corner Bakery. I think we are playing phone tag☺ I'm at my desk now.

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, January 19, 2016 11:48 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum

Hi Kristi – just tried you.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel:(b) (6)
(b) (6)
TS:(b) (6)

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, January 19, 2016 11:33 AM
To: Harp, Jennifer C. (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum

Let's use last year's speech as a model. Erika also wanted to include the Cell Site Simulator and UAS policies.

From: Harp, Jennifer C. (OPCL)
Sent: Tuesday, January 19, 2016 11:28 AM
To: Lane Scott, Kristi Z (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum

Happy to!

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, January 19, 2016 11:27 AM
To: Harp, Jennifer C. (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: FW: DAG Remarks at Privacy Forum

Hi Jenny,

I will need your help on this. Thanks!

Kristi

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, January 19, 2016 8:45 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: DAG Remarks at Privacy Forum

Hi Kristi - we need to submit the DAG's comments for the Forum by COB tomorrow. Can we talk this morning to outline the comments?

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

Document ID: 0.7.12327.6730

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum
To: Brown Lee, Erika (ODAG)
Sent: January 19, 2016 6:23 PM (UTC-05:00)

I'm back at my desk. Christine mentioned that you are still around. I'll try you in a bit!

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, January 19, 2016 5:19 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum

Duplicative Information - See Document ID 0.7.12327.6730

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum
To: Brown Lee, Erika (ODAG)
Sent: January 19, 2016 7:05 PM (UTC-05:00)

It has been a busy day! I'm getting in my car. Feel free to call me on my cell.

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, January 19, 2016 5:19 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum

Duplicative Information - See Document ID 0.7.12327.6730

From: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum
To: Lane Scott, Kristi Z (OPCL)
Sent: January 20, 2016 3:09 PM (UTC-05:00)

Hi Kristi – still on a call re JR, but Josh has pinged for comments. How is the draft coming? Will call you shortly.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, January 19, 2016 7:05 PM
To: Brown Lee, Erika (ODAG)
Subject: RE: DAG Remarks at Privacy Forum

It has been a busy day! I'm getting in my car. Feel free to call me on my cell.

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, January 19, 2016 5:19 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Remarks at Privacy Forum

Duplicative Information - See Document ID 0.7.12327.6730

From: Harp, Jennifer C. (OPCL)
Subject: FW: Privacy topics
To: Lane Scott, Kristi Z (OPCL)
Sent: January 20, 2016 7:11 PM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-20-16).docx

I've attached an initial draft. Feel free to make whatever changes you'd like! It's the same length as DAG Cole's speech last year.

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, January 20, 2016 6:29 PM
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Subject: RE: Privacy topics

Duplicative Information - See Document ID 0.7.12327.6741

From: Brown Lee, Erika (ODAG)
Subject: Fwd: Privacy topics
To: (b)(6) Erika Brown Lee
Sent: January 20, 2016 10:45 PM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-20-16).docx, ATT00001.htm

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)

Begin forwarded message:

From: "Lane Scott, Kristi Z (OPCL)" <(b) (6)>
Date: January 20, 2016 at 10:34:52 PM EST
To: "Brown Lee, Erika (ODAG)" <(b) (6)>
Cc: "Harp, Jennifer C. (OPCL)" <(b) (6)>
Subject: RE: Privacy topics

I've attached the draft for your review. Jenny formatted the document per last year's instructions. While the introductory remarks are similar, you'll find updated language that is relevant to DAG Yates' accomplishments (Breach updates, Cell Site, UAS).

The roads are terrible. I hope they salt overnight.

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, January 20, 2016 10:28 PM
To: Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Subject: Re: Privacy topics

That's terrible! Very glad you got home safely. It may be easier to review concurrently and would save time sometime.

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)

On Jan 20, 2016, at 10:14 PM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

Document ID: 0.7.12327.6741

I'm editing it now. It took me 3 hours to get home☹ I just walked in the door. I hope to have the draft within the hour.

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, January 20, 2016 10:12 PM
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Subject: Re: Privacy topics

Kristi, Jenny - any chance there's a draft? I'll need to turn before 10 am.

Many thanks,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel:(b) (6)
(b) (6)

On Jan 20, 2016, at 6:29 PM, Brown Lee, Erika (ODAG) <(b) (6) > wrote:

> Thanks – I know you're working on it!
>
> ***Erika Brown Lee***
> ***Chief Privacy and Civil Liberties Officer***
> Office of the Deputy Attorney General
> U.S. Department of Justice
> 950 Pennsylvania Avenue, NW
> Washington, D.C. 20530
> Tel:(b) (6)
> (b) (6)
> TS:(b) (6)
>
> ---
>
> **From:** Lane Scott, Kristi Z (OPCL)
> **Sent:** Wednesday, January 20, 2016 6:10 PM
> **To:** Brown Lee, Erika (ODAG); Harp, Jennifer C. (OPCL)
> **Subject:** RE: Privacy topics
>
> Thanks, Erika. We're working on the speech now. I know we need to get this to Josh ASAP. We'll send you our draft later tonight, in order to turn it around in the morning.
>
> ---
>
> **From:** Brown Lee, Erika (ODAG)
> **Sent:** Wednesday, January 20, 2016 3:44 PM
> **To:** Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
> **Subject:** Privacy topics

Document ID: 0.7.12327.6741

Kristi, Jenny - attached is the final version privacy topics that could be incorporated into the DAG's comments for the Privacy Forum.

Best,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

Document ID: 0.7.12327.6741

From: Erika Brown Lee
Subject: Privacy Forum Remarks
To: Brown Lee, Erika (ODAG)
Sent: January 21, 2016 8:57 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx

Document ID: 0.7.12327.6745

From: Brown Lee, Erika (ODAG)
Subject: Fwd: Privacy Forum Remarks
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Sent: January 21, 2016 9:11 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx, ATT00001.htm

Hi Kristi, Jenny - can you review the edited remarks as soon as possible? Note that I've changed the text that (b) (5) .

Many thanks,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)

Begin forwarded message:

From: Erika Brown Lee <(b) (6) >
Date: January 21, 2016 at 8:56:55 AM EST
To: Erika Marie Brown Lee <(b) (6) >
Subject: Privacy Forum Remarks

Document ID: 0.7.12327.6747

From: Young, Brian A. (OPCL)
Subject: RE: DAG Privacy Forum Remarks Draft (1-21-16)
To: Lane Scott, Kristi Z (OPCL)
Sent: January 21, 2016 10:29 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16) - bay edits.docx

Here are my comments:
Sorry so late!

-Brian

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, January 21, 2016 10:27 AM
To: Young, Brian A. (OPCL)
Subject: RE: DAG Privacy Forum Remarks Draft (1-21-16)

Any major ones. I have to hit send now☹

From: Young, Brian A. (OPCL)
Sent: Thursday, January 21, 2016 10:19 AM
To: Proia, Andrew (OPCL); Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Subject: RE: DAG Privacy Forum Remarks Draft (1-21-16)

I will have a few too. Half way through…

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Proia, Andrew (OPCL)
Sent: Thursday, January 21, 2016 10:19 AM
To: Lane Scott, Kristi Z (OPCL)
Cc: Young, Brian A. (OPCL); Harp, Jennifer C. (OPCL)

Subject: RE: DAG Privacy Forum Remarks Draft (1-21-16)

Please see some minor edits/comments

Overall, amazing job in such a tight window. Let me know if you have any questions

Andrew

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, January 21, 2016 9:58 AM
To: Young, Brian A. (OPCL); Proia, Andrew (OPCL)
Cc: Brown Lee, Erika (ODAG)
Subject: DAG Privacy Forum Remarks Draft (1-21-16)

Hi Brian and Andrew,

Can you spot check this document within the next 10 minutes? I am concurrently reviewing. Please send me red line edits NLT 10:15. I need to turn this around to Erika by 10:20. I apologize for the rush.

Thanks,

Kristi

Document ID: 0.7.12327.57104

From: Young, Brian A. (OPCL)
Subject: FW: DAG Privacy Forum Remarks Draft (1-21-16)
To: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL)
Sent: January 21, 2016 10:31 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16) - bay edits.docx

FYI

Brian A. Young
Senior Counsel (Detailee from Federal Bureau of Investigation)
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
(b) (6) (office)
(b) (6) (mobile)
(202) 307-0693 (fax)

NOTICE: This email (including any attachments) is intended for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected by applicable law. If you are not the intended recipient (or the recipient's agent), you are hereby notified that any dissemination, distribution, copying, or use of this email or its contents is strictly prohibited. If you received this email in error, please notify the sender immediately and destroy all copies.

From: Young, Brian A. (OPCL)
Sent: Thursday, January 21, 2016 10:29 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: DAG Privacy Forum Remarks Draft (1-21-16)

Duplicative Information - See Document ID 0.7.12327.57104

From: Lane Scott, Kristi Z (OPCL)
Subject: DAG Privacy Forum Remarks Draft (1-21-16)
To: Brown Lee, Erika (ODAG)
Cc: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL); Young, Brian A. (OPCL)
Sent: January 21, 2016 10:39 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx

Hi Erika,

Here is the final version of the DAG's remarks.

Thanks,

Kristi

Document ID: 0.7.12327.6752

From: Lane Scott, Kristi Z (OPCL)
Subject: DAG Privacy Forum Remarks Draft (1-21-16) (USE THIS VERSION)
To: Brown Lee, Erika (ODAG)
Cc: Harp, Jennifer C. (OPCL); Proia, Andrew (OPCL); Young, Brian A. (OPCL)
Sent: January 21, 2016 10:46 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx

Hi Erika,

If you haven't hit send, please use this version. I caught a prepositional item.

Thanks,

Kristi

Document ID: 0.7.12327.57109

From: Lane Scott, Kristi Z (OPCL)
Subject: DAG Privacy Forum Remarks Draft (1-21-16)
To: Brown Lee, Erika (ODAG)
Sent: January 21, 2016 10:51 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx

Document ID: 0.7.12327.6755

From: Brown Lee, Erika (ODAG)
Subject: Draft Privacy Forum Remarks
To: Mogil, Joshua (ODAG)
Cc: Childs, Heather G. (ODAG)
Sent: January 21, 2016 11:09 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx, ATT00001.htm

Josh, Heather - attached are draft remarks for the DAG to deliver at next week's Privacy Forum. Please let me know there are any questions or additional info that would be helpful.

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)

Document ID: 0.7.12327.7072

From: Brown Lee, Erika (ODAG)
Subject: Draft Privacy Forum Remarks
To: Mogil, Joshua (ODAG)
Cc: Childs, Heather G. (ODAG)
Bcc: Brown Lee, Erika (ODAG)
Sent: January 21, 2016 11:09 AM (UTC-05:00)
Attached: DAG Privacy Forum Remarks Draft (1-21-16).docx, ATT00001.htm

Josh, Heather - attached are draft remarks for the DAG to deliver at next week's Privacy Forum. Please let me know there are any questions or additional info that would be helpful.

Best regards,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)

Document ID: 0.7.12327.7075

From: Brown Lee, Erika (ODAG)
Subject:
To: Erika Brown Lee
Sent: January 21, 2016 5:51 PM (UTC-05:00)
Attached: Component Status Memo.docx

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

Document ID: 0.7.12327.7077

From: Mogil, Joshua (ODAG)
Subject: Remarks- Electronic Copies
To: Yates, Sally (ODAG)
Cc: Childs, Heather G. (ODAG)
Sent: January 22, 2016 9:21 AM (UTC-05:00)
Attached: Tuesday- Privacy Forum Remarks.docx, Thurs- USMS Remarks.docx

Tuesday- Privacy Forum

Thursday- USMS (will be updated with a Chicago anecdote as per your request)

Hard copies are in your book.

-Josh

<<Tuesday- Privacy Forum Remarks.docx>> <<Thurs- USMS Remarks.docx>>

Document ID: 0.7.12327.10550

DOJ PRIVACY FORUM
DOJ Conference Center, Room 7411, RFK Main Justice Building
Tuesday, January 26th at 9:10-9:20 AM
POC: Erika Brown Lee, ODAG/CPCLO, (b) (6)

SUGGESTED REMARKS FOR DEPUTY ATTORNEY GENERAL SALLY YATES

Welcome, and thank you for participating in the Department of Justice's second Privacy Forum. The protection of privacy and civil liberties is a core value at DOJ, and I am pleased that you all have chosen to take part in timely and important discussions about principles that are integral to the Department's programs and initiatives.

The timing of the Forum is not a coincidence. This Thursday, January 28th, is Data Privacy Day, a day that is internationally recognized for the promotion of privacy. We have taken the opportunity to not only embrace the importance of privacy, but to build upon the existing partnerships in privacy that have been established across the Department; to increase awareness of the ways in which we can address and mitigate the privacy risks presented by the technologically advanced tools that help us achieve our mission; and to reinforce the Department's commitment to the privacy and civil liberties principles.

The complementary principles of privacy and civil liberties are fundamentally consistent with our mission to ensure the fair and impartial administration of justice. A crucial goal of the Department's privacy compliance is to

Document ID: 0.7.12327.6755-000001

make certain that the appropriate protections regarding privacy and civil liberties are embedded into our operational activities. We hope that the interactive discussions today will provide an opportunity to deepen the understanding of how privacy and civil liberties protections are implemented at the component and Department level, and enhance our ability to improve the effectiveness of our compliance program.

The importance of privacy and civil liberties is also reflected in composition of the senior leadership of the Department. As part of ODAG, in her capacity as the Department's Chief Privacy and Civil Liberties Officer and the Senior Agency Official for Privacy, Erika reports to both me and the Attorney General. The Chief Privacy and Civil Liberties Officer heads the Office of Privacy and Civil Liberties, which also has the support of ODAG. Together, the CPCLO and OPCL oversee the Department's privacy-related requirements and implement critical policy decisions.

Notwithstanding the Department's dedication to privacy, as our world becomes increasingly interconnected and as new technologies emerge, we must continue to give meaningful consideration to privacy and civil liberties within the programs and tools that we utilize in our varied missions. Those efforts must also continue to be evident through the directives and policies that govern our daily work. In fact, DOJ recently issued landmark policies for the use of two emerging technologies — Unmanned Aircraft Systems (UAS) and cell-site simulators — in

Document ID: 0.7.12327.6755-000001

domestic criminal investigations. These policies set forth important guidelines and procedures that ensure Department components adequately protect individual privacy, civil rights, and civil liberties.

The policies also require extensive training for DOJ personnel, set forth data handling requirements, and establish agency-level auditing programs. As the Department continues to develop technologies that are cost-effective, efficient, and life-saving, we are committed to ensuring compliance with federal privacy laws, regulations, and the Constitution.

Yet, while the Department has developed extensive policies regarding our *collection* of information, we are also faced with the challenge of ensuring that the information it maintains is *secure*. As you all know, last spring and summer, the Federal Government experienced extensive cybersecurity intrusions of protected IT systems. The series of breaches of OPM IT systems affected 21.5 million individuals, and involved background investigation records, including details such as Social Security Numbers, information about immediate family members, and biometric information, including fingerprints.

These unprecedented intrusions will have profound and lasting effects on the Federal Government, including significant cost burdens, counterintelligence risks, and threats to public trust. The incidents also underscore the urgent need for departments and agencies to re-evaluate how they store, retrieve, and maintain personally

Document ID: 0.7.12327.6755-000001

identifiable information. Information security has entered a new era, and we must be more proactive and vigilant about protecting our valuable information more than ever before. Privacy and information security are inextricably linked and both must be given equal importance.

As the threat of information security breaches and the potential for abuse of technology increases, it is incumbent upon every DOJ employee to know the legal requirements and Department policies associated with protecting personally identifiable information. The international community is also paying close attention to how we uphold our American values of privacy and civil liberties.

Consistent with the parameters of our mission work, we must increase transparency about not only the way we use technology and design secure IT systems, but also in how we share information. Our team of dedicated privacy officials works closely with all 40 plus DOJ components and all U.S. Attorney's Offices to carefully balance operational demands in order to preserve the legitimate privacy interests of government employees and the American public.

I'd like to conclude my remarks by re-emphasizing the benefits inherent in our concurrent efforts to ensure both effective law enforcement and robust privacy protections. Protecting privacy and civil liberties go hand-in-hand as part of the Department's duty to be responsible stewards of the information entrusted to our care, and to ensure that

Document ID: 0.7.12327.6755-000001

the laws of the United States are fairly and effectively carried out.

Thank you again for your participation in this important Department event, and Happy Privacy Day!

Document ID: 0.7.12327.6755-000001

From: Raj, Kiran (ODAG)
Subject: RE: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A
To: Dix, Melanie (ODAG); Goldsmith, Andrew (ODAG); Brown Lee, Erika (ODAG)
Cc: Tomney, Brian (ODAG); Ferber, Scott (ODAG); Grooms, Daniel (ODAG)
Sent: January 30, 2016 12:46 PM (UTC-05:00)
Attached: cellphone02A let ksr edits.doc, cellphone02B let KSR Edits.docx

Thanks, Melanie –

I know Scott Ferber and Danny have been working on this as well. Although this is not my area, I did have a few questions as I read through this. Please see attached for a few suggested edits and comments. It does seem that we should double check that DEA does not have any comments. The fact that they did not respond may not be a sufficient reason to assume that they have cleared on this letter.

Best,

Kiran

From: Dix, Melanie (ODAG)
Sent: Saturday, January 30, 2016 11:40 AM
To: Goldsmith, Andrew (ODAG); Raj, Kiran (ODAG); Brown Lee, Erika (ODAG)
Cc: Tomney, Brian (ODAG)
Subject: Fwd: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A

Hi all,

Rae took a look at this and cleared as to OLP. Would you all mind looking it over and letting us know if it looks ok to you or if you have comments? We need to respond to OLA on Monday.

Thanks!
Melanie

Sent from my iPhone

Begin forwarded message:

From: "Silas, Adrien (OLA)" <(b) (6)>
Date: January 29, 2016 at 4:03:13 PM EST
To: "Dix, Melanie (ODAG)" <(b) (6)>, "Tomney, Brian (ODAG)" <(b) (6)>, "Bruck, Andrew J. (ODAG)" <(b) (6)>, "Jain, Samir (ODAG)" <(b) (6)>, "Goldsmith, Andrew (ODAG)" <(b) (6)>
Cc: "Pazur, Shannon (OLP)" <(b) (6)>, "Wade Tyson, Jill C (OLA)" <(b) (6)>, "Losick, Eric P. (OLA)" <(b) (6)>, "Traster, Benjamin (OLA)" <(b) (6)>, "Atwell, Tonya M (JMD)" <(b) (6)>, "Cantilena, Jennifer (JMD)" <(b) (6)>, "Deeley, Kevin (JMD)" <(b) (6)>, "Klimavicz, Joseph (JMD)" <(b) (6)>, "Schlemmer, Maxwell A. (JMD)" <(b) (6)>, "Davis, Valorie A (OLP)" <(b) (6)>, "Matthews, Matrina (OLP)" <(b) (6)>, "White, Cleo (OLP)" <(b) (6)>, (b)(6) per NSD (NSD)" <(b) (6)>, (b)(6) per NSD (NSD)" <(b) (6)>, "NSD LRM Mailbox (NSD)" <Ex_NSDLrmMailbox@jmd.usdoj.gov>, (b)(6) per NSD (NSD)" <(b) (6)>, (b)(6) per NSD (NSD)" <(b) (6)>, "Boynton, Brian (OLC)" <(b) (6)>, "Datla, Kirti (OLC)" <(b) (6)>, "El-Khouri, Adele (OLC)" <(b) (6)>, "Flynn, Caroline (OLC)" <(b) (6)>, "Forrester, Nate (OLC)" <(b) (6)>, "McKenzie, Troy (OLC)" <(b) (6)>,

"policy, civil (CIV)" <cpolicy@CIV.USDOJ.GOV>, "Brink, David" <(b) (6) >, "Morales, Michelle" <(b) (6) >, "Opl, Legislation" <Legislation.OPL@CRM.USDOJ.GOV>, (b)(6), (7)(C) per EOUSA <(b)(6), (7)(C) per EOUSA>, "USAEO-Legislative (USA)" <(b)(6), (7)(C) per EOUSA>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO)(FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, (b)(6), (7)(C) per FBI (DO) (FBI)" <(b)(6), (7)(C), (7)(E) per FBI>, "Arrivillaga, Juan J (DEA)" <(b) (6) >, "Chavez, Eduardo A. (DEA)" <(b) (6) >, (b)(6), (b)(7)(C) per DEA (DEA)" <(b)(6), (b)(7)(C) per DEA>, "Kellstrom, Melissa A. (DEA)" <(b) (6) >, "Szulim, Sarah C. (DEA)" <(b) (6) >, "(b)(6), (b)(7)(C) per DEA (DEA)" <(b)(6), (b)(7)(C) per DEA>, ATF Intergovernmental Affairs <IntergovernmentalAffairs@atf.gov>, "ATFExecSec2@atf.gov" <ATFExecSec2@atf.gov>, (b)(6), (7)(C) per ATF (ATF)" <(b) (6) >, (b)(6), (7)(C) per ATF (ATF)" <(b) (6) >, (b)(6), (7)(C), (7)(F) per USMS (USMS)" <(b)(6), (7)(C), (7)(F) per USMS>, (b)(6), (7)(C), (7)(F) per USMS (USMS)" <(b)(6), (7)(C), (7)(F) per USMS>

Subject: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A

Any objection to submitting to OMB for clearance the attached draft OLP responses to congressional hearing questions?

1) The materials circulated to

JMD/CIO	CIV	DEA
OLP	CRM	ATF
NSD	EOUSA	USMS
OLC	FBI	

2) JMD/BUDGET (John Thompson), NSD ((b)(6) per NSD), and FBI ((b)(6), (7)(C) per FBI) submitted comments;

3) DEA did not respond; CIV did not respond, but by standing arrangement, when CIV does not respond, we go forward without CIV;

4) We would like to submit these to OMB quickly, as the hearing was in October and the Committee has asked us for the responses several times;

5) I have attached the OLA cover sheet.

Attached for OMB clearance are draft responses to congressional hearing questions arising from the October 21, 2015, appearance of principal deputy assistant attorney general Elana Tyrangiel before the House Committee on Oversight and Government Reform, at a hearing entitled “Examining Law Enforcement Use of Cell Phone Tracking Devices.” Please acknowledge receipt of this message. Thank you.

Document ID: 0.7.12327.7166

From: Goldsmith, Andrew (ODAG)
Subject: RE: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A
To: Brown Lee, Erika (ODAG); Raj, Kiran (ODAG); Dix, Melanie (ODAG); Tomney, Brian (ODAG); Ferber, Scott (ODAG); Grooms, Daniel (ODAG)
Sent: February 1, 2016 8:46 AM (UTC-05:00)
Attached: B&G Cell-site Simulator Memo.pdf

In case you're interested, here's the supplemental memo.

From: Goldsmith, Andrew (ODAG)
Sent: Sunday, January 31, 2016 10:35 AM
To: Brown Lee, Erika (ODAG); Raj, Kiran (ODAG)
Cc: Dix, Melanie (ODAG); Tomney, Brian (ODAG); Ferber, Scott (ODAG); Grooms, Daniel (ODAG)
Subject: RE: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A

I agree with Kiran's Comment #1 that we should (b) (5) .

From: Brown Lee, Erika (ODAG)
Sent: Saturday, January 30, 2016 1:39 PM
To: Raj, Kiran (ODAG)
Cc: Dix, Melanie (ODAG); Goldsmith, Andrew (ODAG); Tomney, Brian (ODAG); Ferber, Scott (ODAG); Grooms, Daniel (ODAG)
Subject: Re: OLA Wkflow 112375, Cell Phone Tracking Devices - OLP Q&A

No additional comments from me.

Thanks,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer
Office of the Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (b) (6)
(b) (6)
TS: (b) (6)

On Jan 30, 2016, at 12:45 PM, Raj, Kiran (ODAG) <(b) (6) > wrote:

Duplicative Information - See Document ID 0.7.12327.7166