

**From:** Brown Lee, Erika (ODAG)  
**Subject:** Re: NAP 3.0 // Surveillance Conference Call Recap  
**To:** (b)(6) per NSD (NSD)  
**Cc:** Harp, Jennifer C. (OPCL); Lane Scott, Kristi Z (OPCL)  
**Sent:** July 9, 2015 12:30 PM (UTC-04:00)

Let's chat tomorrow or early next week.

*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 Jul 9, 2015, at 11:41 AM, (b)(6) per NSD (NSD) <(b) (6)> wrote:

Yes, please keep me in the loop – to the extent that it involves law enforcement equities, NSD would like to remain involved and I need to keep my front office apprised.

---

**From:** Harp, Jennifer C. (OPCL)  
**Sent:** Thursday, July 09, 2015 11:39 AM  
**To:** (b)(6) per NSD (NSD); Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL)  
**Subject:** RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5569



**U.S. Department of Justice**

**Office of Legislative Affairs**

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

April 17, 2015

The Honorable Charles E. Grassley  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

This responds to your letters dated December 23, 2014, and March 18, 2015, concerning cell-site simulator technologies. An identical response is being sent to Ranking Member Leahy, who co-signed your letter to us. We apologize for our delay in responding to your letters.

The Department is committed to using all law enforcement resources in a manner that is consistent with the requirements and protections of the Constitution and other legal authorities, and with appropriate respect for privacy and civil liberties. We are likewise committed to ensuring that the Department's practices are lawful and respect the important privacy interests of the American people.

As you are aware, the Department has provided multiple briefings to Committee staff. Specifically, the United States Marshals Service provided a briefing on February 11, 2015. The Federal Bureau of Investigation (FBI) provided briefings on July 17 and December 11, 2014. Additionally, the FBI held a document review of relevant FBI policies for Committee staff on February 24, 2015. The Drug Enforcement Administration also provided a briefing on April 7, 2015. Finally, the Bureau of Alcohol, Tobacco, Firearms, and Explosives is working with Committee staff to set up a briefing.

These briefings were held to provide to the Committee the requested information about certain sensitive law enforcement tools and techniques while avoiding making public the use of any specific, sensitive equipment and techniques that may be deployed in furtherance of law enforcement missions. To do so would allow kidnappers, fugitives, drug smugglers, and certain suspects to determine our capabilities and limitations in this area. Although we cannot discuss here the specific equipment and techniques that we may use, we can assure you that to the extent the Department's law enforcement components deploy certain technologies in investigations, we are committed to using them consistent with federal law.

The Honorable Charles E. Grassley  
Page Two

Your letter of March 18, 2015, also inquires about the Department policies that govern the use of certain technologies in law enforcement investigations. We agree the issues you raise are important and the Department is in the process of examining its policies to ensure that they reflect our continuing commitment to conducting its vital missions while according appropriate respect for privacy and civil liberties.

We hope this information is helpful. Please do not hesitate to contact this office if we may be of additional assistance.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Kadzik", with a stylized flourish at the end.

Peter J. Kadzik  
Assistant Attorney General



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

April 17, 2015

The Honorable Patrick J. Leahy  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Senator Leahy:

This responds to your letters dated December 23, 2014, and March 18, 2015, concerning cell-site simulator technologies. An identical response is being sent to Chairman Grassley, who co-signed your letter to us. We apologize for our delay in responding to your letters.

The Department is committed to using all law enforcement resources in a manner that is consistent with the requirements and protections of the Constitution and other legal authorities, and with appropriate respect for privacy and civil liberties. We are likewise committed to ensuring that the Department's practices are lawful and respect the important privacy interests of the American people.

As you are aware, the Department has provided multiple briefings to Committee staff. Specifically, the United States Marshals Service provided a briefing on February 11, 2015. The Federal Bureau of Investigation (FBI) provided briefings on July 17 and December 11, 2014. Additionally, the FBI held a document review of relevant FBI policies for Committee staff on February 24, 2015. The Drug Enforcement Administration also provided a briefing on April 7, 2015. Finally, the Bureau of Alcohol, Tobacco, Firearms, and Explosives is working with Committee staff to set up a briefing.

These briefings were held to provide to the Committee the requested information about certain sensitive law enforcement tools and techniques while avoiding making public the use of any specific, sensitive equipment and techniques that may be deployed in furtherance of law enforcement missions. To do so would allow kidnappers, fugitives, drug smugglers, and certain suspects to determine our capabilities and limitations in this area. Although we cannot discuss here the specific equipment and techniques that we may use, we can assure you that to the extent the Department's law enforcement components deploy certain technologies in investigations we are committed to using them consistent with federal law.



The Honorable Patrick J. Leahy  
Page Two

Your letter of March 18, 2015, also inquires about the Department policies that govern the use of certain technologies in law enforcement investigations. We agree the issues you raise are important and the Department is in the process of examining its policies to ensure that they reflect our continuing commitment to conducting its vital missions while according appropriate respect for privacy and civil liberties.

We hope this information is helpful. Please do not hesitate to contact this office if we may be of additional assistance.

Sincerely,

A handwritten signature in blue ink, appearing to read 'PJK', is positioned above the printed name.

Peter J. Kadzik  
Assistant Attorney General

**From:** Brown Lee, Erika (ODAG)  
**Subject:** Cell-site Simulator Policy  
**To:** Jain, Samir (ODAG)  
**Sent:** July 20, 2015 9:40 AM (UTC-04:00)

Hi Samir – any update on the policy in terms of timing?

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)

CHARLES E. GRASSLEY, IOWA, CHAIRMAN  
ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA  
DAVID VITTER, LOUISIANA  
DAVID A. PERDUE, GEORGIA  
THOM TILLS, NORTH CAROLINA  
PATRICK J. LEAHY, VERMONT  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KELAN L. DAVIS, Chief Counsel and Staff Director  
KRISTINE J. LORRUS, Democratic Chief Counsel and Staff Director

March 18, 2015

### VIA ELECTRONIC TRANSMISSION

The Honorable Eric H. Holder Jr.  
Attorney General  
U.S. Department of Justice

The Honorable Sally Quillian Yates  
Acting Deputy Attorney General  
U.S. Department of Justice

Dear Attorney General Holder and Acting Deputy Attorney General Yates:

In June and December, we wrote to the Department of Justice (DOJ) and other agencies raising questions about the use of cell-site simulators. Often referred to as "IMSI Catchers," "dirtboxes," or "Stingrays," these devices mimic standard cell towers and force affected cell phones to reveal their approximate location and identifying serial number. Although we understand that some versions of these devices can intercept and collect the content of communications, the Federal Bureau of Investigation ("FBI") and the United States Marshals Service ("USMS") both maintain that they do not use the devices in this way. These agencies have also reported that they purge any data collected from non-targeted telephones once an investigation is complete.

Last week, the *Wall Street Journal* reported that the USMS field-tested various versions of this technology in the United States from 2004 to 2008 on behalf of the Central Intelligence Agency ("CIA"). If this report is true, such practices raise additional concerns. In December, we asked about the full range of DOJ entities that use this technology, the policies in place to protect the privacy interests of third parties whose information might be collected by these devices, and the legal process that is sought prior to their deployment, including the information provided to courts that may authorize their use. DOJ's failure to answer these questions has heightened our concerns.

Accordingly, please provide written responses to each of the following by March 27, 2015:

1. Does DOJ policy ever permit the use of cell-site simulators to capture the content of communications domestically? If so, under what circumstances is this permitted?
2. Has DOJ or any DOJ entity tested cell-site simulators or other surveillance technology on behalf of the intelligence community, by employing the devices in

the course of domestic law enforcement operations? If so, when, to what extent, and under what legal authority?

3. What, if any, DOJ policy governs the testing and deployment of new surveillance technology?
4. Please provide written responses to Questions 1 through 7 of our December 23, 2014 letter, as requested in that letter.

Should you have any questions, please contact Jay Lim at (b) (6) or Lara Flint at (b) (6). Thank you for your cooperation in this important matter.

Sincerely,



Charles E. Grassley  
Chairman



Patrick Leahy  
Ranking Member



# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074  
MINORITY (202) 225-5051  
<http://oversight.house.gov>

April 24, 2015

The Honorable Eric H. Holder  
Attorney General  
U.S. Department of Justice  
Washington, D.C. 20530

Dear Mr. Attorney General:

In recent months, various media reports have detailed the use of cell-site simulation technology, commonly referred to as “Stingrays” or “dirtboxes,” by Department of Justice (DOJ) component agencies.<sup>1</sup> The technology allows law enforcement agents to simulate a cell phone tower, which results in nearby mobile phones and other wireless communication devices connecting to the simulated tower instead of the phone carrier’s legitimate tower. When the mobile device connects, the simulation device can see and record the mobile device’s unique ID number and approximate location.

Committee staff has received briefings from multiple DOJ component agencies, including the Federal Bureau of Investigation (FBI), the U.S. Marshals Service (USMS), and the Drug Enforcement Administration (DEA), about their use of the technology and policies governing use of the technology. While the briefings were informative, we remain concerned that DOJ component agencies are not employing uniform legal standards before deploying cell-site simulation technology. We are also concerned about a number of the policies and procedures related to the technology, including those governing the use and retention of information collected by the devices, as well as those governing the use of the devices in conjunction with joint law enforcement operations conducted at the State and local level.

In addition, we are troubled that DOJ and its component agencies may be using non-disclosure agreements to impede Congressional and Judicial oversight of the use of these devices. We understand that there may be non-disclosure agreements between the component agencies and the manufacturers of these devices, as well as non-disclosure agreements between the component agencies and State and local law enforcement agencies. Media reports indicate that these non-disclosure agreements prevent signatories from producing information about the technology, even in response to a court order.<sup>2</sup>

---

<sup>1</sup> See E.g., Devlin Barrett, *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, WALL STREET JOURNAL (Apr. 9, 2015), available at <http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>

<sup>2</sup> See Justin Fenton, *Baltimore Police used secret technology to track cellphones in thousands of cases*, BALTIMORE SUN (Apr. 9, 2015), available at <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html#page=1> (discussing court testimony in which a local police officer acknowledged that the non-disclosure agreement “instruct[s] [him] to withhold evidence from the state’s attorney and Circuit Court, even upon court order to produce.”)

So that the Committee can better understand Department-wide policies surrounding the use of cell-site simulation technology, please provide the following documents as soon as possible, but no later than 5:00 p.m. May 8, 2015:

- (1) All Department-wide and component agency policies, guidance, or memoranda on the use of cell-site simulation technology.
- (2) All Department-wide and component agency policies, guidance, or memoranda on the use and retention of information collected by cell-site simulation technology.
- (3) All Department-wide and component agency policies, guidance, or memoranda on the use of cell-site simulation technology by any component agency of DOJ in conjunction with joint law enforcement operations conducted at the State and local level.
- (4) All Department-wide or component agency policies, memoranda of understanding, or non-disclosure agreements entered into by any component agency of DOJ with State and local law enforcement agencies regarding the use of cell-site simulation technology.
- (5) All policies, guidance, or memoranda on the use of DOJ grants and the total amount of money disbursed by DOJ to State or local law enforcement agencies to purchase cell-site simulation technology.
- (6) A list of all allegations against any component agency of DOJ regarding any potential misuse of cell-site simulation technology.
- (7) All documents related to the cost and possession of cell-site simulators in the possession of the component agencies of DOJ. In lieu of documents, DOJ can provide an inventory of the cell-site simulators in the possession of the component agencies of DHS. The inventory is to show for each agency:
  - a. the total number of such devices in possession of the agency;
  - b. the name, make, and model of the devices used by or in possession of the agency;
  - c. the total number of devices in possession of the agency for each make and model of device; and,
  - d. the cost of each individual device and the total amount each agency spent in fiscal years 2010-2014 on acquiring and using cell-site simulation technology.

In addition, please contact the Committee as soon as possible to arrange a briefing on this matter by May 1, 2015.

The Committee on Oversight and Government Reform is the principal investigative committee in the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate "any matter" at "any time."

When producing documents to the Committee, please deliver production sets to the Majority staff in Room 2157 of the Rayburn House Office Building and to the Minority staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request.

Please contact Sean Brebbia or Troy D. Stock of Chairman Chaffetz's staff at (b) (6) or Brian Quinn of Ranking Member Cummings' staff at (b) (6) with any questions about this request. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz  
Chairman



Will Hurd  
Chairman  
Subcommittee on  
Information Technology



Elijah E. Cummings  
Ranking Member



Robin Kelly  
Ranking Member  
Subcommittee on  
Information Technology

cc: The Honorable Harold Rogers, Chairman  
House Committee on Appropriations

The Honorable Nita M. Lowey, Ranking Member  
House Committee on Appropriations

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

The Honorable Chaka Fattah, Ranking Member  
Subcommittee on Commerce, Justice, Science, and Related Agencies

Enclosure



### Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
  - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
  - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
  - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;  
  
BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,  
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,  
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,  
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,  
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,  
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,  
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.



7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term "employee" means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

|                                   |                                  |
|-----------------------------------|----------------------------------|
| ORRIN G. HATCH, UTAH              | PATRICK J. LEAHY, VERMONT        |
| JEFF SESSIONS, ALABAMA            | DIANNE FEINSTEIN, CALIFORNIA     |
| LINDSEY O. GRAHAM, SOUTH CAROLINA | CHARLES E. SCHUMER, NEW YORK     |
| JOHN CORNYN, TEXAS                | RICHARD J. DURBIN, ILLINOIS      |
| MICHAEL S. LEE, UTAH              | SHELDON WHITEHOUSE, RHODE ISLAND |
| TED CRUZ, TEXAS                   | AMY KLOBUCHAR, MINNESOTA         |
| JEFF FLAKE, ARIZONA               | AL FRANKEN, MINNESOTA            |
| DAVID VITTER, LOUISIANA           | CHRISTOPHER A. COONS, DELAWARE   |
| DAVID A. PERDUE, GEORGIA          | RICHARD BLUMENTHAL, CONNECTICUT  |
| THOM TILLIS, NORTH CAROLINA       |                                  |

KOLAN L. DAVIS, Chief Counsel and Staff Director  
KRISTINE J. LUCIUS, Democratic Chief Counsel and Staff Director

**United States Senate**  
COMMITTEE ON THE JUDICIARY  
WASHINGTON, DC 20510-6275

June 24, 2015

**VIA ELECTRONIC TRANSMISSION**

The Honorable Loretta Lynch  
Attorney General  
U.S. Department of Justice

Dear Attorney General Lynch:

Since last June, we have written three letters to the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) raising questions about the use of cell-site simulators. Often referred to as "IMSI Catchers," "dirtboxes," or "Stingrays," these devices mimic standard cell towers and force affected cell phones to reveal their approximate location and identifying serial number. According to the Director of the FBI, the FBI's use of these devices is not about collecting the content of communications.<sup>1</sup>

On March 18, 2015, we wrote your office a letter asking for clarification of the policy regarding the use of these devices to intercept and collect the contents of communications, but we have not received a written response specific to this question. Also in that letter, we inquired about a *Wall Street Journal* article that reported that the United States Marshals Service ("USMS") field-tested various versions of this technology in the United States from 2004 to 2008 on behalf of the Central Intelligence Agency ("CIA").<sup>2</sup> Since then, a USMS whistleblower has contacted the Committee and stated that from 2004 to 2006, the USMS tested these devices in at least three American cities. Specifically, the devices were reportedly employed from airplanes that interacted with the signals of real cell-phones and captured their serial numbers – all without seeking a court order and without targeting a fugitive. If true, this report raises additional concerns and is not consistent with the USMS' previous representations about these devices.

Accordingly, by June 26, 2015, please provide written responses to each of the questions contained in our March 18, 2015, letter and Questions 1 and 2 of our December 23, 2014, letter. Also, while we appreciate the information provided orally to our staff in response to questions previously raised about the possible use of these devices to obtain the contents of communications, we ask that you memorialize written responses to the following questions:

---

<sup>1</sup> Charlotte Observer, "FBI [D]irector James Comey on cell gathering," Feb. 13, 2015, <https://www.youtube.com/watch?v=OrkpUHGKETE#t=30>; see also Fred Clasen-Kelly, "Secrecy lifts in CMPD StingRay phone tracking," *The Charlotte Observer*, Feb. 15, 2015.

<sup>2</sup> Devlin Barrett, "CIA Aided Program to spy on U.S. Cellphones: Marshals Service uses airborne devices that mimic cell towers to scan data on thousands of cellphones," *The Wall Street Journal*, Mar. 10, 2015.



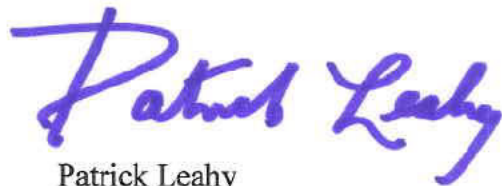
1. Does FBI policy *ever* permit the reconfiguration of cell-site simulators to intercept and collect the content of communications?
2. If the answer to Question 1 is "yes," how many times have the devices been reconfigured and used in this way?
3. If the answer to Question 1 is "yes," what level of approval within the FBI is required before the devices are reconfigured and used in this way, and how many times have this reconfiguration and use been authorized?
4. If the answer to Question 1 is "yes," what type of court order is obtained prior to using the devices in this way? What information is provided to judges when seeking these court orders?

Please number your responses according to their corresponding questions. Should you have any questions, please contact Jay Lim at (b) (6) or Lara Flint at (b) (6). Thank you for your attention to this important matter.

Sincerely,



Charles E. Grassley  
Chairman



Patrick Leahy  
Ranking Member



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

July 20, 2015

The Honorable Charles E. Grassley  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

This responds to your letter to the Attorney General dated July 9, 2015, following up on her breakfast with you and Ranking Member Leahy on June 25, 2015. The Attorney General sincerely enjoyed your conversation and asked that we convey her personal gratitude for your taking the time to join her at the Department of Justice (the Department). She looks forward to continuing to work with you and Ranking Member Leahy on the important issues you discussed. As to the specific matters raised in your letter, we appreciate the opportunity to provide more information below.

Office of Legal Counsel (OLC) Opinion on Office of Inspector General (OIG) Access

As we have discussed with your staff, we anticipate that the OLC opinion will be completed this week and available on OLC's website following the standard publication process. We will send a copy to the Committee when it becomes available. As both the Attorney General and the Deputy Attorney General (DAG) have stated repeatedly, the Department believes that the Inspector General plays a particularly critical role at the Department in helping to identify misconduct or malfeasance, as well as waste, fraud and abuse, and that he should receive all documents that he needs to complete his reviews.

FBI Whistleblower Protection Regulations

The Department believes strongly that whistleblowers play an important role in discovering and preventing waste, fraud, and abuse in the government, and we assure you that the Department takes reports of retaliation very seriously. As you know, the Department is working with the Federal Bureau of Investigation (FBI) to improve the process for adjudicating claims of retaliation. In April 2014, the Department completed a report on the process for adjudicating retaliation claims by FBI employees in response to Presidential Policy Directive 19 (PPD-19). The Department's April 2014 report was the culmination of a working group of attorneys from the FBI, the Justice Management Division (JMD), the Office of Attorney Recruitment and



Management (OARM), the Office of the Inspector General (OIG), the Office of Professional Responsibility (OPR), and the Office of the Deputy Attorney General (ODAG).

The Department has already taken a number of steps to implement the recommendations in this report, including: providing whistleblowers with access to Alternative Dispute Resolution; implementing improved training for FBI employees developed in conjunction with the OIG; employing a policy of referring any final decision that includes a finding of unlawful reprisal to the FBI Office of Professional Responsibility – copying the FBI Director; expanding resources for the office that handles appeals of FBI whistleblower cases; and committing to publicly release the OARM annual reports in the future.

The report also advocated expanding the list of persons to whom a protected disclosure may be made to the second-highest ranking tier of field office officials. The Department's review of the proposed regulations to implement this change is ongoing. As we continue this process, we will consider the April 2015 report, the Government Accountability Office's January 2015 report, and all of the testimony before the Senate Judiciary Committee regarding the appropriate category of persons to whom a protected disclosure may be made. As is the normal course, the new regulations will be subject to the requisite notice and comment process, through which we will gather more information and views on this important issue.

#### Civil Asset Forfeiture

We sincerely appreciate the productive meeting Department staff had with your office and others on July 16, 2015, in which we provided technical assistance on potential civil asset reform legislation. We look forward to continuing to work with your office to improve our system of asset forfeiture and strengthen appropriate safeguards.

#### Juvenile Justice

We appreciate your leadership in introducing the Juvenile Justice and Delinquency Prevention Reauthorization Act. The Department supports reauthorization of this important legislation, and as you know, has been in close communication with your staff about this bill. We most recently provided technical input on July 16, 2015, and are also actively working on responses to the Questions for the Record from the April 21, 2015 hearing regarding the Office of Juvenile Justice and Delinquency Prevention (OJJDP). While we need OMB approval before formally submitting responses, we are hopeful that this process can be completed in the coming weeks. We also hope that our letter of July 17, 2015, and our ongoing discussions with your staff, assists your office in its examination of these important issues.



### Nairobi Embassy Bombing

We appreciate your recent letter dated June 18, 2015, and are working to respond as expeditiously as possible. As you know, as a result of a criminal guilty plea by the BNP Paribas bank in the Southern District of New York, a large sum of money has been forfeited to the United States. In that case, the bank pleaded guilty to violating the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA), by processing billions of dollars through the U.S. financial system on behalf of Sudanese, Iranian, and Cuban entities subject to U.S. economic sanctions. The Department is currently in the process of gathering information from people who may have been harmed by these regimes. As you are likely aware, the Department has set up a website, <http://www.usvbnpp.com>, for the purpose of gathering such information. The deadline for submitting information to the Department is July 30, 2015. We have confirmed that the group about which you inquired has already submitted information. It is helpful to us to know your views on this issue and we expect the information gathered through this process will guide our next steps.

### Cell-Site Simulators

The Department has gone to great lengths to respond to the many requests from Committee staff for information regarding cell-site simulator technologies. As you are aware, earlier this year the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Drug Enforcement Administration (DEA), FBI, and U.S. Marshals Service (USMS) provided extensive law enforcement sensitive briefings on this topic, and separate in camera reviews of component-specific policies as requested. These briefings were held to provide to the Committee the requested information about certain sensitive law enforcement tools and techniques while avoiding making public the use of any specific, sensitive equipment and techniques that may be deployed in furtherance of law enforcement missions. All four components have provided additional responses to the Committee's questions through multiple e-mails and conference calls with staff. Further supplementing these efforts, on April 17, 2015, the Department responded to your letters dated December 23, 2014, and March 18, 2015. We are actively working on a response to your most recent letter dated June 24, 2015. Finally, as we have advised you and your staff, the Department is in the process of examining its policies to ensure that they reflect our continuing commitment to conducting our vital law enforcement mission while according appropriate respect for privacy and civil liberties. We expect this review to be completed soon and have committed to briefing the Committee on any resulting Departmental policy changes.

### U.S. Marshals Service

As we have stated in correspondence and conversations with your staff, the Department takes these issues seriously and sincerely appreciates that you have brought them to our attention. As you know, the Department has referred all of these allegations to the OIG and we



will take reasonable measures to accommodate your information needs to the extent we can do so without any undue interference with the pending OIG investigation.

We appreciate your staff's willingness to discuss reasonable parameters for the Department's response to your inquiries, including prioritizing certain areas among the numerous allegations in your letters. We understand that one such priority is documents related to and interviews of the two Office of General Counsel (OGC) employees you have identified. We further understand that the Committee's preference is to review relevant documents prior to scheduling these interviews and, to that end, we aim to make such documents available to your staff in the coming weeks and will schedule the noted interviews thereafter.

As discussed above, we are working diligently to respond to your requests as expeditiously as possible. As the Attorney General noted during your breakfast, the Department is sincerely committed to working cooperatively with you and your staff, and Congress as a whole. While we have made and will continue to make all reasonable efforts to meet your stated deadlines, responding to almost 80 incoming letters, containing close to 700 questions and document requests (from your office alone this year) within limited time frames, is simply not feasible in all cases. While we will continue to do everything we can to meet your information needs, please be aware that our ability to timely respond to your inquiries is impacted by the significant volume of letters we receive.

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

Sincerely,

A handwritten signature in blue ink, appearing to read 'P. J. Kadzik', with a stylized flourish at the end.

Peter J. Kadzik  
Assistant Attorney General

cc: The Honorable Patrick J. Leahy  
Ranking Member

3058587  
DA  
1

CHARLES E. GRASSLEY, IOWA, CHAIRMAN  
ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA  
DAVID VITTER, LOUISIANA  
DAVID A. PERDUE, GEORGIA  
THOMAS M. NOBLE, NORTH CAROLINA  
PATRICK J. LEAHY, VERMONT  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHARON ANGEL, ILLINOIS  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. GROSS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

## United States Senate

COMMITTEE ON THE JUDICIARY  
WASHINGTON, DC 20510-6275

2015 JUL -9 PM 4:50

DEPT. OF JUSTICE  
EXECUTIVE SECRETARIAT

Karen L. Davis, Chief Counsel and Staff Director  
Katie L. Conner, Democratic Chief Counsel and Staff Director

July 9, 2015

The Honorable Loretta Lynch  
Attorney General  
U.S. Department of Justice

Dear Attorney General Lynch:

Thank you for inviting me to breakfast on June 25<sup>th</sup>. We agreed that more communication is critical to improving the Justice Department's relationship with Congress. Effective oversight can help you lead a more effective Department. In this spirit, I write to ask for your help in obtaining responses to the following requests, some of which we did not have time to discuss in person, but which are very important. Some of these issues have been awaiting Department action for a long time, and the Department itself has acknowledged that they need to be resolved, particularly the Inspector General access issue and the FBI whistleblower protection regulations.

- 1. OLC Opinion on the OIG's Right of Access to Department Documents:** The IG and the public have been waiting for more than a year for OLC to opine on this issue. Meanwhile, the FBI has refused to provide details I asked for about the amount of time and money spent assessing which documents to withhold from the IG.
- 2. Revisions to the FBI Whistleblower Protection Regulations:** At a March 2015 hearing, all witnesses including the FBI representative agreed that existing regulations should be revised so that disclosures to Congress are explicitly protected. And, it was clear that there was widespread support to protect disclosures to immediate supervisors and others in the chain of command as well. The Department has not yet implemented its own recommendations for improving the FBI whistleblower process, even after studying the issue for years.
- 3. Civil Asset Forfeiture:** Please provide technical assistance that the Department agreed to do on bill language to have JLEO effectively replace funds that local law enforcement now obtains through equitable sharing and please provide your position on the reforms that you would accept generally.
- 4. Juvenile Justice:** Please provide responses to Questions for the Record for the April 21, 2015, hearing and also technical input on the bipartisan JJDP reauthorizing legislation.

5. **Embassy Bombings:** Victims of the 1998 Nairobi Embassy bombing have obtained a judgment that Sudan assisted the bombing and have filed a petition for remission from the Department to receive some of the recovery against the French bank that recently pled guilty to illegally funneling funds to Sudan. Please give their petition all due consideration.
6. **Cell-Site Simulators:** Please respond to my three letters, dating back to December 2014.
7. **U.S. Marshals Service Whistleblowers:** Please set a schedule for the interviews I requested of the USMS General Counsel's office staff and related document-production. And please take a leading role in ensuring that whistleblowers at the USMS are protected. Although I've received letters talking about general reminders of whistleblower rights, my office continues to receive information about USMS managers retaliating against suspected whistleblowers. These managers ultimately report to you, and a message that retaliation at the USMS specifically won't be tolerated needs to be sent down the bureaucracy, directly from you at the top, because it continues to happen.

Thank you again for your invitation to breakfast. I am grateful for our relationship and look forward to working with you.

Sincerely,



Charles E. Grassley  
Chairman  
Senate Committee on the Judiciary

*your honoring Sen. Leahy  
and me at breakfast  
is much appreciated.  
Also, I'd like to communicate  
by phone regularly like  
we did Monday!*

PATRICK J. LEAHY, VERMONT CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT  
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA  
ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA

KRISTINE J. LOGGUS, *Chief Counsel and Staff Director*  
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510 6275

December 23, 2014

The Honorable Eric H. Holder, Jr.  
Attorney General  
Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

The Honorable Jeh Johnson  
Secretary of Homeland Security  
Department of Homeland Security  
Washington, D.C. 20528

Dear Attorney General Holder and Secretary Johnson:

In recent months, media reports have detailed the use of cell-site simulators (often referred to as “IMSI Catchers” or “Stingrays”) by federal, state and local law enforcement agencies. Most recently, a November 13, 2014, Wall Street Journal article (“Americans’ Cellphones Targeted in Secret U.S. Spy Program”) reported that the United States Marshals Service regularly deploys airborne cell-site simulators (referred to as “DRT boxes” or “dirtboxes”) from five metropolitan-area airports across the United States. Like the more common Stingray devices, these “dirtboxes” mimic standard cell towers, forcing affected cell phones to reveal their approximate location and registration information. The Wall Street Journal article reports that “dirtboxes” are capable of gathering data from tens of thousands of cellphones in a single flight.

We wrote to FBI Director Comey in June seeking information about law enforcement use of cell-site simulators. Since then, our staff members have participated in two briefings with FBI officials, and at the most recent session they learned that the FBI recently changed its policy with respect to the type of legal process that it typically seeks before employing this type of technology. According to this new policy, the FBI now obtains a search warrant before deploying a cell-site simulator, although the policy contains a number of potentially broad exceptions and we continue to have questions about how it is being implemented in practice. Furthermore, it remains unclear how other agencies within the Department of Justice and Department of Homeland Security make use of cell-site simulators and what policies are in place to govern their use of that technology.

The Judiciary Committee needs a broader understanding of the full range of law enforcement agencies that use this technology, the policies in place to protect the privacy interests of those whose information might be collected using these devices, and the legal process that DOJ and DHS entities seek prior to using them.

For example, we understand that the FBI’s new policy requires FBI agents to obtain a search warrant whenever a cell-site simulator is used as part of an FBI investigation or operation, unless one of several exceptions apply, including (among others): (1) cases that pose an imminent danger to public safety, (2) cases that involve a fugitive, or (3) cases in which the



technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy.

We have concerns about the scope of the exceptions. Specifically, we are concerned about whether the FBI and other law enforcement agencies have adequately considered the privacy interests of other individuals who are not the targets of the interception, but whose information is nevertheless being collected when these devices are being used. We understand that the FBI believes that it can address these interests by maintaining that information for a short period of time and purging the information after it has been collected. But there is a question as to whether this sufficiently safeguards privacy interests.

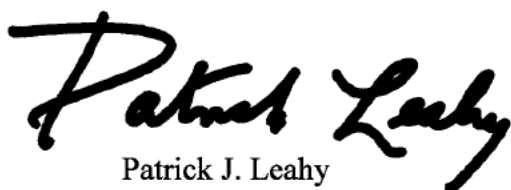
Accordingly, please provide written responses to these questions by January 30, 2015:

1. Since the effective date of the FBI's new policy:
  - a. How many times has the FBI used a cell-site simulator?
  - b. In how many of these instances was the use of the cell-site simulator authorized by a search warrant?
  - c. In how many of these instances was the use of the cell-site simulator authorized by some other form of legal process? Please identify the legal process used.
  - d. In how many of these instances was the cell-site simulator used without any legal process?
  - e. How many times has each of the exceptions to the search warrant policy, including those listed above, been used by the FBI?
2. From January 1, 2010, to the effective date of the FBI's new policy:
  - a. How many times did the FBI use a cell-site simulator?
  - b. In how many of these instances was the use of a cell-site simulator authorized by a search warrant?
  - c. In how many of these instances was the use of the cell-site simulator authorized by some other form of legal process? Please identify the legal process used.
  - d. In how many of these instances was the cell-site simulator used without any legal process?
  - e. In how many of the instances referenced in Question 2(d) did the FBI use a cell-site simulator in a public place or other location in which the FBI deemed there is no reasonable expectation of privacy?
3. What is the FBI's current policy on the retention and destruction of the information collected by cell-site simulators in all cases? How is that policy enforced?
4. What other DOJ and DHS agencies use cell-site simulators?

5. What is the policy of these agencies regarding the legal process needed for use of cell-site simulators?
  - a. Are these agencies seeking search warrants specific to the use of cell-site simulators?
  - b. If not, what legal authorities are they using?
  - c. Do these agencies make use of public place or other exceptions? If so, in what proportion of all instances in which the technology is used are exceptions relied upon?
  - d. What are these agencies' policies on the retention and destruction of the information that is collected by cell-site simulators? How are those policies enforced?
6. What is the Department of Justice's guidance to United States Attorneys' Offices regarding the legal process required for the use of cell-site simulators?
7. Across all DOJ and DHS entities, what protections exist to safeguard the privacy interests of individuals who are not the targets of interception, but whose information is nevertheless being collected by cell-site simulators?

Please number your written responses according to their corresponding questions. In addition, please arrange for knowledgeable DOJ and DHS officials to provide a briefing to Judiciary Committee staff about these issues following the provision of these written responses, but no later than February 6, 2015. Should you have any questions, please have your staff contact Lara Flint at (b) (6), or Jay Lim at (b) (6).

Sincerely,



Patrick J. Leahy  
Chairman



Charles E. Grassley  
Ranking Member

COMMITTEES:

COMMERCE, SCIENCE, AND TRANSPORTATION  
SMALL BUSINESS AND ENTREPRENEURSHIP  
FOREIGN RELATIONS

CHAIRMAN:

SUBCOMMITTEE ON INTERNATIONAL DEVELOPMENT AND  
FOREIGN ASSISTANCE, ECONOMIC AFFAIRS,  
INTERNATIONAL ENVIRONMENTAL PROTECTION, AND  
PEACE CORPS

U.S. SENATE CLIMATE CHANGE CLEARING HOUSE

## United States Senate

November 14, 2014

SUITE SR-218  
RUSSELL BUILDING  
WASHINGTON, DC 20510-2107  
202-224-2742

975 JFK FEDERAL BUILDING  
15 NEW SUDBURY STREET  
BOSTON, MA 02203  
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312  
FALL RIVER, MA 02721  
508-677-0523

1550 MAIN STREET, 4TH FLOOR  
SPRINGFIELD, MA 01101  
413-785-4610

The Honorable Eric H. Holder, Jr.  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20530

Dear Attorney General Holder:

According to a recent article in the Wall Street Journal ("Americans' Cellphones Targeted in Secret U.S. Spy Program", November 14, 2014), the Department of Justice (DOJ) has deployed equipment on aircraft to mimic the operations of cell phone towers in an effort to intercept the mobile phone information of Americans. While such data can serve as an important tool for law enforcement to detect and deter criminal or terrorist activity, the sweeping nature of this program and the likely collection of sensitive records belonging to innocent consumers raise a number of important questions about how the Department protects the privacy of Americans, particularly those with no connection to unlawful activities.

In order to better understand this program, I ask that you provide responses to the following questions:

- 1) When did this program begin operating? Do any other agencies within DOJ operate similar programs, in which airplanes, helicopters or drones with attached cellular surveillance equipment are flown over US airspace?
- 2) How many times have DOJ agencies conducted operations over US cities with cellular surveillance technology attached to an airplane, helicopter or drone? How many under this program?
- 3) What types of court order, if any, are sought and obtained to authorize searches conducted under this program? What are judges told about how the technology works and the number of innocent people whose information may be swept up? Please provide a representative sample of the applications for these court orders.
- 4) In what kind of investigations are the "dirtbox" and similar technology used to locate targets? Are there any limitations imposed on the kinds of investigations in which the dirtbox and similar technology can be used?

- 5) According to media reports, the dirtbox technology, which is similar to a so-called "stingray" technology, works by mimicking the cellular networks of U.S. wireless carriers. Upon what specific legal authority does the Department rely to mimic these cellular networks? Do the applications for court orders authorizing the use of this technology inform judges of this practice?
- 6) According to the Wall Street Journal, the dirtbox can interrupt calls. Even if such jamming is incidental and unavoidable, under what legal authority does it take place? Are judges told that the surveillance operations they are authorizing may also disrupt or jam the phone calls of innocent people?
- 7) Do the dirtbox and stingray send signals through the walls of innocent people's homes in order to communicate with and identify the phones within? If so, are judges informed of this fact in applications for court orders?
- 8) What information is collected about these phones by the surveillance technology?
- 9) What, if any, policies govern the collection, retention, use and sharing of this information?
  - a. Where is this information stored (i.e., on the device itself or transmitted to a different device)?
  - b. For how long is this information retained?
  - c. How is the information associated with consumers who are not the subject of an investigation handled?
  - d. How much of this information is retained after the conclusion of the operation?
- 10) In a typical operation, how many innocent peoples' phones are probed by the dirtbox equipment?
- 11) Are individuals – either those suspected of committing crimes or innocent individuals – provided notice that information about their phones was collected? If yes, explain how. If no, why not?

Thank you for your attention to this important matter. Please provide responses to these questions no later than December 8, 2014. If you have any questions, please have a member of your staff contact Joseph Wender at (b) (6).

Sincerely,  


Edward J. Markey  
United States Senator



## United States Senate

April 13, 2015

The Honorable Eric H. Holder, Jr.  
Attorney General of the United States  
Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

The Honorable Michele M. Leonhart  
Administrator  
Drug Enforcement Administration  
8701 Morissette Drive  
Springfield, VA 22152

Dear Attorney General Holder and Administrator Leonhart:

I write with serious concerns regarding media reports that the Department of Justice, and particularly the Drug Enforcement Agency (DEA), tracked and collected billions of international phone calls from U.S. citizens as part of a far-reaching program that began as early as 1992 and was only recently discontinued. As reported, these actions represent a troubling infringement upon the privacy rights of countless law-abiding Americans over four different Administrations. With portions of the PATRIOT Act expiring this year, these reports may only further undermine public confidence in the ability of your agencies to adequately protect the privacy rights of law-abiding Americans. Indeed, it is critical that the Justice Department comes forward in the most transparent manner possible to provide additional information to ensure the public and Congress fully understand the scope of this program and receive clear assurances that the privacy rights of Americans are no longer being compromised by this program.

These recent media reports indicate that the data collection began in 1992 under President George H.W. Bush and that the program was subsequently approved by top Justice Department officials in each of the succeeding three Administrations -- targeting Americans' phone calls to as many as 116 countries over two decades. Instead of focusing the program on individuals suspected to be involved in criminal activity, the Justice Department is said to have ordered telephone companies to turn over entire lists of all the calls placed by Americans to these various countries. This raises numerous questions about the legality of the program, and represents an unacceptable breach of privacy. Further, I am troubled by the apparent absence of independent oversight of this program, particularly as it's reported that the DEA gathered these phone records without court approval.

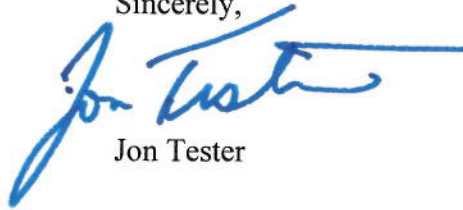
Moving forward, I would specifically like to know:

- What calendar years this program was active;
- What was the legal justification for the actions carried out through this program;
- Is the Justice Department or DEA still in possession of any call records obtained through this program;
  - If not, when was that data purged;
  - And if so, under what legal basis and why?

- How long were these records kept after the data was found to be irrelevant to ongoing investigations;
- Who was the arbiter of what records were pertinent to these investigations;
- What metrics were used to determine the relevance of the call records;
- How long were records kept before such a determination was made?

Montanans, like all Americans, are rightly concerned by these recent revelations and deserve a transparent accounting of the program's history and current status. They expect and deserve a higher level of privacy than what has been detailed in the reporting on this particular program. I appreciate your attention to this matter and await your response.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jon Tester", with a long horizontal flourish extending to the right.

Jon Tester

PATRICK J. LEAHY, VERMONT, CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT  
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA  
ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA

KRISTINE J. LUCIUS, *Chief Counsel and Staff Director*  
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

November 18, 2014

The Honorable Eric H. Holder, Jr.  
Attorney General  
Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530

Dear Attorney General Holder:

I am concerned by recent reports about the Department of Justice's collection of Americans' cellphone data from aircraft. The reports describe the Department's use of wireless surveillance systems, known as IMSI-catchers (e.g., Stingrays or DRTBoxes), that collect phone identifications, locations, and possibly communications content by impersonating cellular phone towers. While I understand that law enforcement agents need to be able to track down and catch dangerous suspects, this should not come at the expense of innocent Americans' privacy.

The reports, while alarming, lack critical details about the parameters of this program. Therefore, I request that you provide answers to the following questions:

1. Which federal agencies are currently using, or plan to use, this technology or similar technology?
2. Under what legal authority is the federal government acting? To the extent that the Department of Justice is seeking court approval, is this done on a case-by-case basis or on a wider scale? What are judges told about how the technology works, and the potential impact on innocent Americans? Please provide a representative sample of the applications for these court orders.
3. What is the frequency and duration of such flights? How many phones can be detected, tracked, and/or monitored during each flight?
4. What types of fugitives are targeted for surveillance under this technology?
5. What types of information (e.g., phone metadata, location, emails, files, and photos) are collected from phones?
6. What types of data are retained by the government using this program, both from phones of targets and innocent Americans?
7. What is the effectiveness of this program? Please be specific about the number of fugitives who have been detained as a direct result of this technology.



8. Reports indicate that the surveillance systems have the capability of blocking phone calls, including 911 and other emergency calls. What steps have been taken to ensure that phone calls of non-targeted civilians are not interrupted by this program?
9. What safeguards are in place to ensure that innocent Americans' privacy is protected to the fullest extent possible?

Thank you for your prompt attention to this important matter. If you have any questions, please contact Brent Beckert on my staff at (b) (6).

Sincerely,



Senator Al Franken  
Chairman, Subcommittee on Privacy,  
Technology, and the Law



# United States Senate

WASHINGTON, DC 20510

December 9, 2014

The Honorable Eric H. Holder, Jr.  
Attorney General  
U.S. Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530

The Honorable Jeh Johnson  
Secretary of Homeland Security  
Department of Homeland Security  
Washington, D.C. 20528

Dear Attorney General Holder and Secretary Johnson,

We are writing to express our concern about recent news reports revealing that the U.S. Marshals Service is flying airplanes over the United States equipped with surveillance devices that transmit electronic signals into the homes of thousands of Americans in order to locate individuals via their mobile phones. These International Mobile Subscriber Identity Catcher surveillance devices (IMSI-catcher), commonly known as “DRTBoxes,” “dirtboxes” or “Stingrays,” simulate legitimate cell phone towers, thus compelling all nearby phones to identify themselves. As a result, agencies that use these devices collect the information of thousands of Americans, potentially infringing on the Fourth Amendment and disrupting normal cell phone usage.

The U.S. Marshals Service is apparently not the only agency using these devices from the air—it has come to our attention that other agencies with the Department of Justice (DOJ), including the Drug Enforcement Administration (DEA), as well as the Department of Homeland Security (DHS), more specifically Immigration and Customs Enforcement (ICE), are also using airborne IMSI-catchers.

Whether used on an automobile or plane, these devices potentially violate the Fourth Amendment and represent a significant intrusion into the private lives of thousands of Americans. While we all want law enforcement agencies to use cutting-edge tools to catch criminals and protect our borders, Americans should not have to sacrifice their privacy rights in the process. Furthermore, given the extreme lengths to which federal agencies have gone to keep surveillance technologies like this a secret,<sup>1</sup> it is vital that their use be subject to strict oversight by the courts and Congress.

---

<sup>1</sup> See Martin Kaste, *Should Police Be Able To Keep Their Devices Secret?*, NPR, October 22, 2014, *available at* <http://www.npr.org/2014/10/22/358120429/should-police-be-able-to-keep-their-devices-secret>. See also Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, *Wired*, March 3, 2014, *available at* <http://www.wired.com/2014/03/stingray/>.

We would like to know if your departments, or its components, utilize these devices along the borders and in our states. Accordingly, we request the following information:

1. To what extent does your department use IMSI-catchers (Stingrays, DRTboxes, etc.) or other similar technology? Specifically:
  - a. Which components within your department use such devices? If multiple components use such devices, is there department-wide guidance governing their use?
  - b. Since FY 2010, how many times has such technology been deployed, and how many phones were identified or tracked by this technology, including devices used by the targets of the operation as well as non-targets whose information was incidentally swept up?
  - c. In what types of operations are these devices deployed?
  - d. What statutory authority permits the use of this surveillance technology?
  - e. Do DHS and/or DOJ obtain a court order prior to using such devices? If so, do DHS and/or DOJ inform the courts of the number of individuals likely to be impacted; the scope of acquisition; or the specific technology being deployed?
2. Did the DOJ Office of Privacy and Civil Liberties, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties review and/or conduct a privacy impact assessment or other review regarding the use of these technologies prior to deployment? If so, please provide copies of such reviews or assessments.
3. To what extent is your department coordinating or providing assistance to other federal agencies in order to help them purchase or otherwise obtain this type of technology?
4. The Federal Communication Commission requires that “state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) ... prior to the acquisition and use of the [IMSI-catchers or other similar] equipment/technology.”<sup>2</sup> What does the FBI require of departments and agencies as part of this coordination process?
5. To what extent does your department provide assistance to state and local agencies in order to help them purchase or otherwise obtain this type of technology?
  - a. To the extent that these devices have been purchased through DHS and DOJ grant programs, how much federal money has been used to purchase them? What, if any, limitations or requirements are imposed on agencies that receive and use federal grant money to acquire this type of surveillance technology?

---

<sup>2</sup> Muckrock, FCC and FBI disagree over NDA requirement for police StingRays, October 8, 2014, <https://www.beaconreader.com/muckrock/fcc-claims-nondisclosure-agreement-not-required-for-police-to-use-stingrays>.

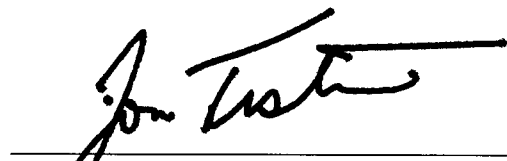
- b. What training and conditions are given to state and local agencies who receive this technology, as it relates to protecting innocent Americans' privacy?
  - c. How many times have DHS and/or DOJ loaned or otherwise permitted the use of such devices by state or local agencies?
6. Public documents reveal that the DEA has acquired airborne IMSI-catchers for use along the southwestern border.<sup>3</sup> Is this technology also being utilized by the DEA or other DOJ office along the Northern Border? How many miles inland from both borders is this technology being deployed?
7. Does DHS also deploy this or similar technology along northern and/or southern borders? If so, in what areas? What legal authority is your agency using to conduct flights whilst using such devices?
8. Are operations conducted within existing high-crime designated areas (i.e. High Intensity Drug Trafficking Area)?
9. What policies and guidance govern the use, retention, and dissemination of information collected by these devices? Specifically:
- a. What information is collected using these devices? How is the acquired information stored?
  - b. When are department personnel permitted to search through information acquired by these devices?
  - c. How long is the collected information retained? How is this information disposed of, and what timeframe is your agency using to dispose of information collected by such devices?
  - d. When is this information shared with other federal, state, or local agencies, or international partners? How much is information shared with other federal agencies, how often is information shared, and to which agencies?
  - e. Is information collected used in criminal prosecutions or immigration proceedings? If so, does DHS or DOJ have a policy in place requiring that defendants be notified of how such information was collected so they may raise relevant legal challenges?
10. Do DHS and/or DOJ have policies in place requiring that individuals who are not targets be informed when their information is inadvertently collected, reviewed, or retained?
11. What efforts are made to ascertain and minimize civilian interference?

---

<sup>3</sup> See "Prime Award Spending Data," *available at* [http://www.usaspending.gov/explore?fiscal\\_year=all&comingfrom=searchresults&piid=DJD14HQP0798&typeofview=complete](http://www.usaspending.gov/explore?fiscal_year=all&comingfrom=searchresults&piid=DJD14HQP0798&typeofview=complete)

Thank you for your attention to this important matter. We look forward to your response.

Sincerely,



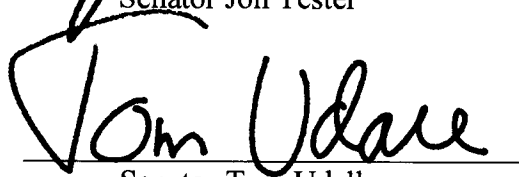
---

Senator Jon Tester



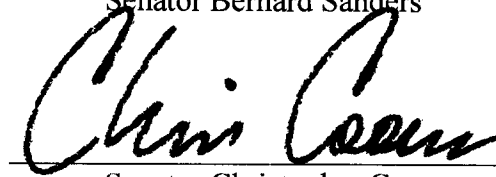
---

Senator Bernard Sanders



---

Senator Tom Udall



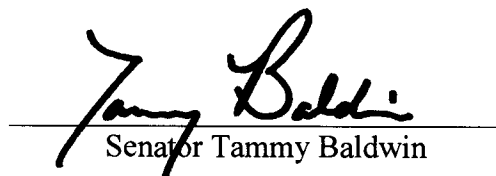
---

Senator Christopher Coons



---

Senator Mark Begich



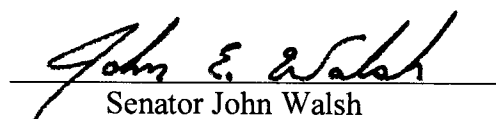
---

Senator Tammy Baldwin



---

Senator Al Franken



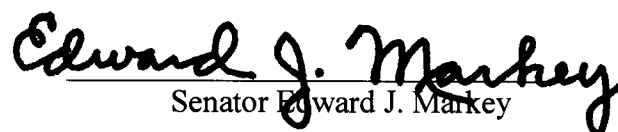
---

Senator John Walsh



---

Senator Jeff Merkley



---

Senator Edward J. Markey



---

Senator Martin Heinrich



**From:** Jain, Samir (ODAG)  
**Subject:** FW: TIME SENSITIVE RE: Stingray  
**To:** Brown Lee, Erika (ODAG)  
**Sent:** August 14, 2015 6:08 PM (UTC-04:00)  
**Attached:** DRAFT 8-12-15 - DOJ Cell-Site Simulator Policy to DAG.docx

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Wednesday, August 12, 2015 5:33 PM  
**To:** Fried, Hannah (OLP); OBrien, Paul; Bitkower, David; (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS); Auerbach, Gerald (USMS); (b)(6), (7)(C) per ATF (ATF); Evans, Stuart (NSD); (b)(6), (7)(C) per EOUSA (USACO); (b)(6), (7)(C) per EOUSA (USAALN); Stemler, Patty; Dreeben, Michael R (OSG); (b)(6) per NSD (NSD); (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); (b)(6), (7)(C) per ATF (ATF); (b)(6) per NSD (NSD); Pazur, Shannon (OLP)  
**Cc:** Jain, Samir (ODAG)  
**Subject:** RE: TIME SENSITIVE RE: Stingray

Thanks for your responses. Attached is the version that is going forward to the DAG for her review. There is one change since our dispatches yesterday – the addition of a footnote (number 9) to (b) (5)

I am unaware of any issues in dispute at this point. If I am incorrect, please contact me by 10 am tomorrow morning to identify any remaining issues of concern.

Thanks,  
Elana

**From:** Fried, Hannah (OLP)  
**Subject:** Stingray rollout materials  
**To:** Tyrangiel, Elana (OLP)  
**Sent:** August 14, 2015 7:34 PM (UTC-04:00)  
**Attached:** DAG cover memo re Stingray Policy draft v2.docx, Stingray roll-out to-do's 8 13 2014.docx, cell-site simulator Q&A draft 8 14 2015.docx, cell-site simulator Q&A draft 8 14 2015 nat sec.docx

Sending to you:

1. **rollout list:** think you want to use this version – the one you sent me yesterday, which this builds off of, was missing the section we added on (b) (5)
2. **Stingray cover memo:** edited
3. **Q&A:**
  - a. Attaching two Q&As. The one marked “nat sec” is not really for your review, but for your reference. It’s from way back, when I drafted a larger Q&A for national security. I don’t think it makes sense to have that be separate, since many of the questions duplicate the broader Q&A.
  - b. Note that I’ve included a question on (b) (5), which is drafted to reflect what the current draft says. Same goes for the way I’ve answered national security questions, especially the one about (b) (5).

Last thing – I did not hear back from Jill Tyson regarding her email. Left her a voicemail and sent her an email.

**From:** Lan, Iris (ODAG)  
**Subject:** Fwd: TIME SENSITIVE RE: Stingray  
**To:** Gauhar, Tashina (ODAG)  
**Sent:** August 20, 2015 4:13 PM (UTC-04:00)  
**Attached:** DRAFT - DOJ Cell Site Simulator Policy 8-20-15 v2.docx, ATT00001.htm, DRAFT - DOJ Cell Site Simulator Policy 8-20-15 v2 (1).docx, ATT00002.htm

FYI - and this is the first I am seeing of the draft policy.

Begin forwarded message:

**From:** "Axelrod, Matthew (ODAG)" <(b) (6)>  
**Date:** August 20, 2015 at 4:11:28 PM EDT  
**To:** "Jain, Samir (ODAG)" <(b) (6)>, "Lan, Iris (ODAG)" <(b) (6)>, "Bonilla, Armando (ODAG)" <(b) (6)>, "Grooms, Daniel (ODAG)" <(b) (6)>, "Brown Lee, Erika (ODAG)" <(b) (6)>, "Goldsmith, Andrew (ODAG)" <(b) (6)>  
**Cc:** "Childs, Heather G. (ODAG)" <(b) (6)>  
**Subject:** FW: TIME SENSITIVE RE: Stingray

I believe all of you have seen various drafts of this policy as it has progressed. Elana and I have hashed some things through and this is the final version that is now being circulated to components. If you have any significant heartburn, please call me or swing by my office to discuss. That said, I'm hopeful it won't be necessary. The goal is to finalize the text early next week.

Thanks,  
Matt

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Thursday, August 20, 2015 3:37 PM  
**To:** Axelrod, Matthew (ODAG)  
**Subject:** FW: TIME SENSITIVE RE: Stingray

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Thursday, August 20, 2015 3:37 PM  
**To:** Fried, Hannah (OLP); OBrien, Paul; Bitkower, David; (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS); Auerbach, Gerald (USMS); (b)(6), (7)(C) per ATF (ATF); Evans, Stuart (NSD); (b)(6), (7)(C) per EOUSA (USACO); (b)(6), (7)(C) per EOUSA (USAALN); Stemler, Patty; Dreeben, Michael R. (OSG); (b)(6) per NSL (NSD); (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); (b)(6), (7)(C) per ATF (ATF); (b)(6) per NSD (NSD); Pazur, Shannon (OLP)  
**Subject:** RE: TIME SENSITIVE RE: Stingray

Duplicative Information - See Document ID 0.7.12327.5653

**From:** Lan, Iris (ODAG)  
**Subject:** Fwd: TIME SENSITIVE RE: Stingray  
**To:** Gauhar, Tashina (ODAG)  
**Sent:** August 20, 2015 4:48 PM (UTC-04:00)  
**Attached:** DRAFT - DOJ Cell Site Simulator Policy 8-20-15 v3.docx, ATT00001.htm

Begin forwarded message:

**From:** "Axelrod, Matthew (ODAG)" <(b) (6)>  
**Date:** August 20, 2015 at 4:41:56 PM EDT  
**To:** "Jain, Samir (ODAG)" <(b) (6)>, "Lan, Iris (ODAG)" <(b) (6)>, "Bonilla, Armando (ODAG)" <(b) (6)>, "Grooms, Daniel (ODAG)" <(b) (6)>, "Brown Lee, Erika (ODAG)" <(b) (6)>, "Goldsmith, Andrew (ODAG)" <(b) (6)>  
**Cc:** "Childs, Heather G. (ODAG)" <(b) (6)>  
**Subject:** FW: TIME SENSITIVE RE: Stingray

Duplicative Information - See Document ID 0.7.12327.5779





**From:** Goldsmith, Andrew (ODAG)  
**Subject:** Re: TIME SENSITIVE RE: Stingray  
**To:** Axelrod, Matthew (ODAG)  
**Cc:** Jain, Samir (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Grooms, Daniel (ODAG); Brown Lee, Erika (ODAG); Childs, Heather G. (ODAG)  
**Sent:** August 24, 2015 4:23 PM (UTC-04:00)

FYI - Elana stopped by this afternoon to discuss a discovery-related aspect of the policy. I was unable to talk and we've tentatively scheduled to meet on Wednesday.

Sent from my iPhone

On Aug 20, 2015, at 4:41 PM, Axelrod, Matthew (ODAG) <(b) (6)> wrote:

Please use this version instead. Thx.

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Thursday, August 20, 2015 4:17 PM  
**To:** Axelrod, Matthew (ODAG)  
**Subject:** RE: TIME SENSITIVE RE: Stingray

Matt, please use this version.

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Thursday, August 20, 2015 3:37 PM  
**To:** Axelrod, Matthew (ODAG)  
**Subject:** FW: TIME SENSITIVE RE: Stingray

---

**From:** Tyrangiel, Elana (OLP)  
**Sent:** Thursday, August 20, 2015 3:37 PM  
**To:** Fried, Hannah (OLP); O'Brien, Paul; Bitkower, David; (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI); Goggin, Wendy H. (DEA); Quinn, Maura F. (DEA); Driscoll, Derrick (USMS); Auerbach, Gerald (USMS); (b)(6), (7)(C) per ATF (ATF); Evans, Stuart (NSD); (b)(6), (7)(C) per EOUSA (USACO); (b)(6), (7)(C) per EOUSA (USAALN); Stemler, Patty; Dreeben, Michael R. (OSG); (b)(6) per NSD (NSD); (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per ATF (ATF); (b)(6), (7)(C) per ATF (ATF); (b)(6) per NSD (NSD); Pazur, Shannon (OLP)  
**Subject:** RE: TIME SENSITIVE RE: Stingray

All --

Attached are ODAG edits to the draft Stingray policy. If any of them give rise to significant concern, please let us know by **3 pm on Tuesday**.

The document is in redline. Two things of note: 1) the applications section has been relocated, but that re-location does not appear in redline; and 2) most, but not all, of the changes to the background section reflect a re-ordering of the sentences, rather than brand new text.

Thanks for your attention to this.

Elana

**From:** Proia, Andrew (OPCL)  
**Subject:** RE: DOJ To Release Cell Phone Tracking Records to ACLU  
**To:** Brown Lee, Erika (ODAG)  
**Cc:** Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)  
**Sent:** August 26, 2015 3:17 PM (UTC-04:00)  
**Attached:** Stipulation Order--ACLU v DOJ (8-21-2015).pdf, Complaint--ACLU v DOJ (7-30-2015).pdf, Cross-Motion For Summary Judgment Order--ACLU v DOJ (12-30-2015).pdf

Erika,

Just to follow-up with you on our phone call about the Law360 article below, I've attached a few documents to this e-mail:

- [Stipulation Order--ACLU v DOJ \(8-21-2015\)](#): This is the settlement order issued in which the Law360 article is based. Under the Order, DOJ will agree to provide ACLU all responsive documents related to its request for "requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008." Note that the three other FOIA requests not settled deal specifically with information on cell-site simulators, other location tracking technologies, and documents related to Department procedures since the *Jones* decision.
- [Cross-Motion For Summary Judgment Order--ACLU v DOJ \(12-30-2015\)](#): The article discusses DOJ's intent to appeal a summary judgment order concerning parts of a "strategy handbook" and other sealed records. I believe this is the summary judgment order. It provides a bit more background about ACLU's request, and the other responsive documents at issue in this case.
- [Complaint--ACLU v DOJ \(8-21-2015\)](#): Just in case you were interested in viewing the original complaint filed by ACLU.

Overall, it appears that this case does deal with records related to the Department's use of cell-site simulators and other location tracking technologies.

Let me know if you have any additional questions or comments.

Thanks, Erika!

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)

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:** Wednesday, August 26, 2015 1:58 PM

**To:** Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL); Wood, Alexander W (OPCL)

**Subject:** DOJ To Release Cell Phone Tracking Records to ACLU

All,

Here is an interesting article on a recent DOJ FOIA case settlement with the ACLU on cell phone tracking records:

"The U.S. Department of Justice will provide a host of documents surrounding warrants and subpoenas for cellphone tracking efforts, to settle part of a Freedom of Information Act suit by the American Civil Liberties Union, according to a recent California federal court filing.

. . . .

Friday's settlement gives the ACLU access to summaries of applications for subpoenas, court orders and warrants from January 2008 onward, according to court records. Linda Lye, in-house counsel at the ACLU, said the documents they have obtained give a greater insight into the US attorney's office's use of statutory letters over search warrants when obtaining cellphone location data."

<http://www.law360.com/articles/694772/doj-cedes-cellphone-tracking-docs-to-aclu>

Let me know if you have any questions.

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)

JS 44 CAND (Rev. 12/11)

## CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

## I. (a) PLAINTIFFS

American Civil Liberties Union of Northern California  
San Francisco Bay Guardian

(b) County of Residence of First Listed Plaintiff San Francisco  
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)  
Michael T. Risher (CA Bar No. 191627), Linda Lye (CA Bar No. 215584)  
American Civil Liberties Union of Northern California, INC.  
39 Drumm St., San Francisco, CA 94111. Ph. 415-621-2493

## DEFENDANTS

Department Of Justice  
450 Golden Gate Avenue, 13th Floor  
San Francisco, CA 94102-9523  
County of Residence of First Listed Defendant

(IN U.S. PLAINTIFF CASES ONLY)

NOTE:

IN LAND CONDEMNATION CASES, USE THE LOCATION OF  
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)  
U.S. Attorney's Office  
450 Golden Gate Avenue  
San Francisco, CA 94102

CV 12 4008

MEJ

## II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☒ 2 U.S. Government Defendant
- ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

## III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- |                                         | PTF                        | DEF                        |                                                               | PTF                        | DEF                        |
|-----------------------------------------|----------------------------|----------------------------|---------------------------------------------------------------|----------------------------|----------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State     | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State                | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation                                                | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

## IV. NATURE OF SUIT (Place an "X" in One Box Only)

| CONTRACT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | TORTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | FORFEITURE/PENALTY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | BANKRUPTCY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | OTHER STATUTES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> 110 Insurance<br><input type="checkbox"/> 120 Marine<br><input type="checkbox"/> 130 Miller Act<br><input type="checkbox"/> 140 Negotiable Instrument<br><input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment<br><input type="checkbox"/> 151 Medicare Act<br><input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excl. Veterans)<br><input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits<br><input type="checkbox"/> 160 Stockholders' Suits<br><input type="checkbox"/> 190 Other Contract<br><input type="checkbox"/> 195 Contract Product Liability<br><input type="checkbox"/> 196 Franchise | <b>PERSONAL INJURY</b><br><input type="checkbox"/> 310 Airplane<br><input type="checkbox"/> 315 Airplane Product Liability<br><input type="checkbox"/> 320 Assault, Libel & Slander<br><input type="checkbox"/> 330 Federal Employers' Liability<br><input type="checkbox"/> 340 Marine<br><input type="checkbox"/> 345 Marine Product Liability<br><input type="checkbox"/> 350 Motor Vehicle<br><input type="checkbox"/> 355 Motor Vehicle Product Liability<br><input type="checkbox"/> 360 Other Personal Injury<br><input type="checkbox"/> 362 Personal Injury - Med. Malpractice | <b>PERSONAL INJURY</b><br><input type="checkbox"/> 365 Personal Injury - Product Liability<br><input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability<br><input type="checkbox"/> 368 Asbestos Personal Injury Product Liability<br><b>PERSONAL PROPERTY</b><br><input type="checkbox"/> 370 Other Fraud<br><input type="checkbox"/> 371 Truth in Lending<br><input type="checkbox"/> 380 Other Personal Property Damage<br><input type="checkbox"/> 385 Property Damage Product Liability | <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881<br><input type="checkbox"/> 690 Other<br><b>LABOR</b><br><input type="checkbox"/> 710 Fair Labor Standards Act<br><input type="checkbox"/> 720 Labor/Mgmt. Relations<br><input type="checkbox"/> 740 Railway Labor Act<br><input type="checkbox"/> 751 Family and Medical Leave Act<br><input type="checkbox"/> 790 Other Labor Litigation<br><input type="checkbox"/> 791 Empl. Ret. Inc. Security Act<br><b>IMMIGRATION</b><br><input type="checkbox"/> 462 Naturalization Application<br><input type="checkbox"/> 463 Habeas Corpus - Alien Detainee (Prisoner Petition)<br><input type="checkbox"/> 465 Other Immigration Actions | <input type="checkbox"/> 422 Appeal 28 USC 158<br><input type="checkbox"/> 423 Withdrawal 28 USC 157<br><b>PROPERTY RIGHTS</b><br><input type="checkbox"/> 820 Copyrights<br><input type="checkbox"/> 830 Patent<br><input type="checkbox"/> 840 Trademark<br><b>SOCIAL SECURITY</b><br><input type="checkbox"/> 861 HIA (1395ff)<br><input type="checkbox"/> 862 Black Lung (923)<br><input type="checkbox"/> 863 DIWC/DIWW (405(g))<br><input type="checkbox"/> 864 SSID Title XVI<br><input type="checkbox"/> 865 RSI (405(g))<br><b>FEDERAL TAX SUITS</b><br><input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)<br><input type="checkbox"/> 871 IRS—Third Party 26 USC 7609 | <input type="checkbox"/> 375 False Claims Act<br><input type="checkbox"/> 400 State Reapportionment<br><input type="checkbox"/> 410 Antitrust<br><input type="checkbox"/> 430 Banks and Banking<br><input type="checkbox"/> 450 Commerce<br><input type="checkbox"/> 460 Deportation<br><input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations<br><input type="checkbox"/> 480 Consumer Credit<br><input type="checkbox"/> 490 Cable/Sat TV<br><input type="checkbox"/> 850 Securities/Commodities/Exchange<br><input type="checkbox"/> 890 Other Statutory Actions<br><input type="checkbox"/> 891 Agricultural Acts<br><input type="checkbox"/> 893 Environmental Matters<br><input checked="" type="checkbox"/> 895 Freedom of Information Act<br><input type="checkbox"/> 896 Arbitration<br><input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision<br><input type="checkbox"/> 950 Constitutionality of State Statutes |

## V. ORIGIN

(Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from another district (specify)
- ☐ 6 Multidistrict Litigation

## VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):  
5 U.S.C. § 552

Brief description of cause:

Action to compel timely and complete production of records under FOIA

## VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☐ Yes ☒ No

## VIII. RELATED CASE(S) IF ANY

(See Instructions):

JUDGE

DOCKET NUMBER

## IX. DIVISIONAL ASSIGNMENT (Civil L.R. 3-2)

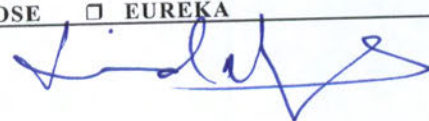
(Place an "X" in One Box Only)

☒ SAN FRANCISCO/OAKLAND☐ SAN JOSE☐ EUREKA

DATE

7/30/12

SIGNATURE OF ATTORNEY OF RECORD





E-filing

FILED  
JUL 31 2012  
RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

Michael Risher (CA SBN 191627)  
mrisher@aclunc.org  
Linda Lye (CA SBN 215584)  
llye@aclunc.org  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF NORTHERN CALIFORNIA, INC.  
39 Drumm Street  
San Francisco, CA 94111  
Tel: (415) 621-2493  
Fax: (415) 255-8437

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

**Cv 12 4008**

AMERICAN CIVIL LIBERTIES UNION OF  
NORTHERN CALIFORNIA;  
*SAN FRANCISCO BAY GUARDIAN*,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE,

Defendant.

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

COMPLAINT FOR DECLARATORY  
AND INJUNCTIVE RELIEF

**MEJ**

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

American Civil Liberties Union of Northern California and *San Francisco Bay Guardian* v. DOJ, Case No. \_\_\_\_\_

## INTRODUCTION

1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. §552, to enforce the public’s right to information about the federal government’s use of location tracking technology. Recent revelations have made clear that government agencies are engaged in seeking and acquiring the location information of individuals for tracking and surveillance purposes, utilizing varying technologies and varying legal standards that frequently fall short of constitutional protections designed to protect the public from intrusive government searches.

2. There has been widespread media interest and public concern related to government tracking and surveillance of location information. There is also great urgency to inform the public about governmental efforts to track and surveil individuals because members of Congress and California state legislators are currently weighing new laws related to location tracking – and information shedding lights on the government’s current practices would inform those pending legislative debates. It is imperative that Northern California community members and policymakers representing this region immediately gain a full and complete understanding of how the United States Attorneys for the Northern District are seeking or obtaining location information and whether these activities comport with constitutional rights. Access to this information is necessary for a meaningful and informed public debate over these pressing public policy issues and pending legislative debates.

3. Over three months ago, on April 13, 2012, Plaintiffs American Civil Liberties Union of Northern California, a non-profit civil rights organization, and *San Francisco Bay Guardian*, an independent newspaper, submitted a FOIA request to Defendant Department of Justice (“DOJ”) seeking information about the federal government’s use of location tracking technology to monitor and surveil suspects. Plaintiffs also requested expedited processing, pursuant to 5 U.S.C. §522(a)(6)(E), on the grounds that there is an “urgency to inform the public about actual or alleged federal government activity” and also that this is “a matter of widespread and exceptional media interest in which there exists possible questions about the government’s integrity which affect public confidence.” 28 C.F.R. §16.5(d)(1)(ii) & (iv). Acknowledging the

1 import and urgency of this request, the DOJ granted Plaintiffs' request for expedited processing  
2 by letter dated April 23, 2012. Since that time, however, the agency has provided Plaintiffs with  
3 no records or any information regarding the status of its search.

4 4. Plaintiffs now bring this action to obtain the information and the expedited  
5 processing to which are statutorily entitled.

#### 6 PARTIES

7 5. Plaintiff American Civil Liberties Union of Northern California ("ACLU-NC") is  
8 an affiliate of the American Civil Liberties Union, a national, non-profit, non-partisan  
9 organization with the mission of protecting civil liberties from government incursions,  
10 safeguarding basic constitutional rights, and advocating for open government. The ACLU-NC is  
11 established under the laws of the state of California and is headquartered in San Francisco,  
12 California. The ACLU-NC has approximately 50,000 members. In support of its mission, the  
13 ACLU-NC uses its communications department to disseminate to the public information relating  
14 to its mission, through its website, newsletters, and other publications.

15 6. Plaintiff *San Francisco Bay Guardian* ("*The Bay Guardian*") is a corporation  
16 organized in the state of California and headquartered in San Francisco, California. It is a  
17 newspaper of general circulation and has the largest circulation of a newsweekly in Northern  
18 California, with an audited weekly distribution of 65,000. *The Bay Guardian* has been published  
19 continuously since 1966, and its primary activity is publishing or otherwise disseminating  
20 information to the public. In 2011, *The Bay Guardian* received the California Newspaper  
21 Publishers Association's General Excellence award for a weekly newspaper. In 2012, Tim  
22 Redmond, the executive editor of *The Bay Guardian*, received the Professional Journalist award  
23 from the Society of Professional Journalists, Northern California chapter.

24 7. Defendant Department of Justice is an agency within the meaning of 5 U.S.C.  
25 §552(f). The agency has its headquarters in Washington, D.C., and field offices all over the  
26 country, including San Francisco, California.

## JURISDICTION

8. This Court has subject matter jurisdiction and personal jurisdiction over the parties pursuant to 5 U.S.C. §§552(a)(4)(B) and 552(a)(6)(C)(i). This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1331 and 1346.

## VENUE AND INTRADISTRICT ASSIGNMENT

9. Venue is proper in this district pursuant to 5 U.S.C. §552(a)(4)(B) and 28 U.S.C. §§1391(e) and §1402. The plaintiffs have their principle places of business in this district.

10. Pursuant to Local Rule 3-2(c) and (d), assignment to the San Francisco division is proper because a substantial portion of the events giving rise to this action occurred in this district and division and because both Plaintiffs are headquartered in San Francisco.

## FACTUAL ALLEGATIONS

### **The Federal Government's Use of Location Tracking Technology Is a Matter of Significant Public Interest**

11. Location tracking technology enables law enforcement to capture intimate details of an individual's life, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, the synagogue or church, the gay bar and on and on." *United States v. Jones*, \_U.S.\_, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. 2009)).

12. New technology dramatically reduces the normal barriers of cost and officer resources to mount comprehensive surveillance. While an individual's trip along a public road to the doctor is visible to the public (and police), the expenditure of resources to surveil an individual around the clock wherever she goes serves as a deterrent to abuse. When, by contrast, one technician can sit at the police station and monitor hundreds or even thousands of targets continuously and for indefinite periods, judicial oversight is essential to protect privacy and ensure that invasive surveillance is only conducted of those as to whom there is probable cause of criminal activity.



1           13.     Technological developments have expanded the mechanisms by which the  
2 government can track an individual's location. GPS (global positioning system) devices can be  
3 affixed to a vehicle. Cell phones can reveal historic and real-time location information through  
4 cell site location information (which refers to the identity of the nearest cell tower), triangulation  
5 data (which involves analysis of the time and angle at which a cell phone's signal arrives at  
6 multiple cell towers), and GPS receiver hardware that may be built into the device. Other  
7 location tracking devices have come to light, such as "stingrays," which mimic a cellphone tower  
8 and convince a target cellphone to connect to it and thereby transmit information about the  
9 location of the cellphone, even if its owner is not placing a call.

10           14.     The media has extensively covered the government's use of location tracking  
11 devices, and its efforts to do so without obtaining a warrant based on probable cause. *See, e.g.,*  
12 Robert Barnes, "Supreme Court: Warrants needed in GPS tracking," *Washington Post*, January  
13 23, 2012; Rebecca J. Rosen, "Why the Jones Supreme Court Ruling on GPS Tracking Is Worse  
14 Than It Sounds," *The Atlantic*, January 23, 2012; Barry Friedman, "Privacy, Technology and  
15 Law," *New York Times*, January 29, 2012; Greg Stohr, "Police Use of GPS Devices to Track  
16 People Limited by U.S. Supreme Court," *Bloomberg*, January 23, 2012; Jess Bravin, "Justices  
17 Rein In Police on GPS Trackers," *Wall Street Journal*, January 24, 2012; Editorial, "Navigating  
18 the Supreme Court's GPS ruling," *Los Angeles Times*, January 25, 2012; Bob Egelko, "U.S.  
19 Supreme Court to decide major legal issues," *San Francisco Chronicle*, September 30, 2011;  
20 Editorial, "The Court's GPS Test," *New York Times*, November 5, 2011; David G. Savage,  
21 "Supreme Court: warrant required for GPS tracking," *San Francisco Chronicle*, January 24,  
22 2012; Adam Liptak, "Court Case Asks if 'Big Brother' Is Spelled GPS," *New York Times*,  
23 September 10, 2011; Editorial, "A court test of privacy in the digital age," *San Francisco*  
24 *Chronicle*, January 29, 2012; Adam Liptak, "Justices Say GPS Tracker Violated Privacy Rights,"  
25 *New York Times*, January 24, 2012; Julia Angwin, "FBI Turns Off Thousands of GPS Devices  
26 After Supreme Court Ruling," *Wall Street Journal*, February 25, 2012.

1           15.     The government's efforts to use GPS devices to engage in location tracking  
2 without a warrant were recently rebuffed by the United States Supreme Court in *United States v.*  
3 *Jones, supra*.

4           16.     Following that decision, the media continued to report on the issue extensively,  
5 including the implications of the *Jones* decision for law enforcement and the fact that the *Jones*  
6 decision prompted an increased reliance by law enforcement on cell site location information.  
7 *See, e.g.*, David Kravets, "After Car-Tracking Smackdown, Feds Turn to Warrantless Phone  
8 Tracking," *Wired*, March 31, 2012; Editorial, "GPS and the Right to Privacy," *New York Times*,  
9 January 25, 2012; David Kravets, "Supreme Court Court Rejects Willy-Nilly GPS Tracking,"  
10 *Wired*, January 23, 2012; Dave Bohon, "More Police Agencies Using Warrantless Cell Phone  
11 Tracking in Surveillance," *The New American*, April 5, 2012; Thomas Peracchio, "Supreme  
12 court ruling exposes many digital privacy issues," *The Examiner*, April 2, 2012; Thomas  
13 Claburn, "Supreme Court Tackles GPS Tracking Vs. Privacy," *Information Week*, January 23,  
14 2012; Editorial, "EDITORIAL: Obama wants to track you," *Washington Times*, March 20, 2012;  
15 Emily Babay, "After GPS tracking banned by court, privacy fight turns to cell phone data,"  
16 *Washington Examiner*, April 1, 2012.

17           17.     The American Civil Liberties Union released a report shedding light on a  
18 disturbing trend across the country of law enforcement agencies obtaining cell phone location  
19 information without probable cause warrants. The ACLU report was the subject of a front page  
20 *New York Times* article, and a flurry of subsequent news articles and editorials emphasizing the  
21 importance of a warrant requirement for cell phone location information. *See* Eric Lichtblau,  
22 "Police Are Using Phone Tracking as a Routine Tool," *New York Times*, March 31, 2012;  
23 Cristian Salazar, "ACLU demands police disclose cell phone tracking," *San Francisco*  
24 *Chronicle*, August 4, 2011; James Temple, "How California cops grab phone data from Apple,  
25 Google, carriers," *San Francisco Chronicle*, April 3, 2012; Suzy Khimm, "ACLU: Local police  
26 departments tracking cellphones without warrants," *Washington Post*, April 2, 2012; Declan  
27 McCullagh, "How Apple and Google help police bypass iPhone, Android lock screens," *CNET*,  
28

1 April 2, 2012; Athima Chansanchai, "ACLU: Police track cellphones, too," *MSNBC*  
 2 *Technology*, April 2, 2012 (Tab 53); Bob Sullivan, "Pricey 'stingray' gadget lets cops track  
 3 cellphones without telco help," *MSNBC Red Tape*, April 3, 2012; Peter Doocy, "Law  
 4 enforcement under scrutiny by ACLU for tracking cell phones," *Fox News*, April 4, 2012.

5 18. Members of Congress representing Northern California, including  
 6 Representatives Zoe Lofgren and Barbara Lee, are currently working on bipartisan efforts to pass  
 7 a federal location privacy bill, the GPS Act (H.R. 2168), and state lawmakers, including State  
 8 Senator Mark Leno, are working on state location privacy laws (SB 1434).

9 19. The information sought in Plaintiffs' FOIA request would inform the on-going  
 10 societal debate as well as specific legislative debates over the government's use of location  
 11 tracking technology.

12 **Plaintiffs Submitted A FOIA Request and DOJ Granted Expedited Processing But**  
 13 **Has Failed to Produce Any Records**

14 20. On April 13, 2012, Plaintiffs submitted a FOIA request to the DOJ seeking  
 15 information about its surveillance of the Occupy movement. A copy of Plaintiffs FOIA request  
 16 (without exhibits) is appended hereto as Exhibit 1.

17 21. In particular, Plaintiffs FOIA request seeks:

- 18 (a) All requests, subpoenas, and applications for court orders or warrants  
 19 seeking location information since January 1, 2008.
- 20 (b) Any template applications or orders that have been utilized by United  
 21 States Attorneys in the Northern District to seek or acquire location  
 22 information since January 1, 2008.
- 23 (c) Any documents since January 1, 2008, related to the use or policies of  
 24 utilizing any location tracking technology, including but not limited to  
 25 cell-site simulators or digital analyzers such as devices known as Stingray,  
 26 Triggerfish, AmberJack, KingFish or Loggerhead.

(d) Any records related to the Supreme Court's holding in *United States v. Jones*, excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below

22. Plaintiffs also requested expedited processing, pursuant to 5 U.S.C. §522(a)(6)(E), on the grounds that there is an "urgency to inform the public about actual or alleged federal government activity" and also that this is "a matter of widespread and exceptional media interest in which there exists possible questions about the government's integrity which affect public confidence." 28 C.F.R. §16.5(d)(1)(ii) & (iv).

23. By letter dated April 17, 2012, DOJ acknowledged receipt of Plaintiffs' FOIA request. A copy of this letter is appended hereto as Exhibit 2.

24. By letter dated April 23, 2012, DOJ granted Plaintiffs' request for expedited processing. A copy of this letter is appended hereto as Exhibit 3.

25. On July 6, 2012, Plaintiffs sent a letter to the DOJ inquiring as to the status of its search. A copy of this letter is appended hereto as Exhibit 4.

26. As of the date of the filing of this complaint, Plaintiffs have not received any response to their July 6, 2012 status inquiry.

27. More than 20 working days have passed since the DOJ received Plaintiffs' FOIA request.

28. As of the date of the filing of this complaint, Plaintiffs have not received any responsive documents from the DOJ or any correspondence indicating when the DOJ might provide any documents.

29. Plaintiffs have exhausted all applicable administrative remedies.

30. DOJ has wrongfully withheld the requested records from Plaintiffs.

//

//

//

//



**FIRST CLAIM FOR RELIEF**  
**Violation of Freedom of Information Act For**  
**Wrongful Withholding Of Agency Records**

31. Plaintiffs incorporate paragraphs 1 through 30 above as if fully set forth herein.

32. Defendant DOJ has wrongfully withheld agency records requested by Plaintiffs under FOIA and has failed to comply with the statutory time for the processing of FOIA requests.

33. Plaintiffs have exhausted the applicable administrative remedies with respect to DOJ's wrongful withholding of the requested records.

34. Plaintiffs are entitled to injunctive relief with respect to the release and disclosure of the requested documents because Defendant DOJ continues to improperly withhold agency records in violation of FOIA. The Plaintiffs will suffer irreparable injury from, and have no adequate legal remedy for, the DOJ's illegal withholding of government documents pertaining to the subject of Plaintiffs' FOIA request.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs prays that this Court:

A. Order Defendant DOJ to process immediately the requested records in their entirety;

B. Order Defendant DOJ to make the requested records in their entirety available to Plaintiffs promptly upon completion of its processing of such records;

C. Provide for expeditious proceedings in this action;

D. Enter a preliminary and permanent injunction against the DOJ ordering the relief requested herein;

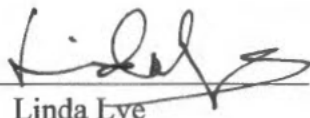
E. Declare that DOJ's failure to disclose the records requested by Plaintiffs is unlawful;

F. Award Plaintiffs' their litigation costs and reasonable attorney's fees incurred in this action;

//

1 G. Grant such other relief as the Court may deem just and proper.

2  
3 Dated: July 31, 2012

4 By: 

Linda Lye

5 Michael Risher  
6 Linda Lye  
7 AMERICAN CIVIL LIBERTIES UNION  
8 FOUNDATION OF NORTHERN CALIFORNIA  
9 39 Drumm Street  
10 San Francisco, CA 94111  
11 Tel: (415) 621-2493  
12 Fax: (415) 255-8437

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28 Attorneys for Plaintiffs

# Exhibit 1



April 13, 2012

Via Certified Mail

Melinda Haag  
United States Attorney  
Northern District of California  
Federal Courthouse  
450 Golden Gate Avenue, 11<sup>th</sup> Floor  
San Francisco, CA 94102

Office of Public Affairs  
United States Department of Justice  
950 Pennsylvania Ave, NW, Room 1128  
Washington, DC 20530

Re: Freedom of Information Act Request regarding location tracking  
*Expedited Processing Requested*

Dear Ms. Haag,

The American Civil Liberties Union of Northern California (ACLU-NC) and *San Francisco Bay Guardian* (*Bay Guardian*) submit this expedited Freedom of Information Act (FOIA) request for records in the possession of the United States Attorneys' Office for the Northern District of California pertaining to efforts to seek or obtain location information. We submit this request pursuant to the FOIA, 5 U.S.C. § 552, implementing regulations 28 CFR §16.1 *et seq.*, and any other applicable regulations.

Recent revelations have made clear that government agencies are engaged in seeking and acquiring the location information of individuals for tracking and surveillance purposes, utilizing varying technologies and varying legal standards that frequently fall short of constitutional protections designed to protect the public from intrusive government searches. Previous ACLU Freedom of Information Act requests have revealed that the Department of Justice has maintained since at least 2007 that the government need not obtain a warrant and show probable cause to track people's location with only one exception: real-time GPS and triangulation data, and that U.S. Attorneys around the country are only encouraged to obtain a warrant based on probable cause prior to engaging in precise cell phone tracking.<sup>1</sup> FOIA requests have also revealed that some U.S. Attorney offices do not even comply even with this set of guidelines.<sup>2</sup>

<sup>1</sup> Email from Brian Klebba, *GPS or "E-911-data" Warrants*, November 17, 2009, available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_dojrecommendation.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf).

<sup>2</sup> Letter from William G. Stewart II, to Catherine Crump, *Mobile Phone Tracking (Items 3-5)/DNJ*, Dec. 31, 2008, available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_released\\_074132\\_12312008.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf); Letter from William G. Stewart II to Catherine Crump, *Mobile Phone Tracking (Items 3-5)/FLS*, Dec. 31, 2008, available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_released\\_074135\\_12312008.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf).

MICHELLE A. WELSH, CHAIRPERSON | DENNIS McNALLY, AJAY KRISHNAN, FARAH BRELYI, ALLEN ASCH, VICE CHAIRPERSONS | KENNETH SUGARMAN, SECRETARY/TREASURER  
ABDI SOLTANI, EXECUTIVE DIRECTOR | KELLI EVANS, ASSOCIATE DIRECTOR | CHERI BRYANT, DEVELOPMENT DIRECTOR | SHAYNA GELENDER, ORGANIZING & COMMUNITY ENGAGEMENT DIRECTOR  
LAURA SAPONARA, COMMUNICATIONS DIRECTOR | ALAN SCHLOSSER, LEGAL DIRECTOR | MARGARET C. CROSBY, ELIZABETH GILL, LINDA LYE, JULIA HARUMI MASS, MICHAEL RISHER, JORY STEELE, STAFF ATTORNEYS  
PHYLLIDA BURLINGAME, ALLEN HOPPER, NATASHA MINSKER, NICOLE A. OZER, DIANA TATE VERMEIRE, POLICY DIRECTORS | STEPHEN V. BOMSE, GENERAL COUNSEL

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA  
39 DRUMM STREET, SAN FRANCISCO, CA 94111 | T/415.621.2493 | F/415.255.1470 | TTY/415.863.7832 | WWW.ACLUNC.ORG

①



April 13, 2012

Page 2

In December 2009, it was revealed that telecommunications provider, Sprint Nextel, received over 8 million demands from government agencies for access to customer location information between September 2008 and October 2009.<sup>3</sup> In September 2011, it was also revealed that federal authorities had utilized a "stingray" device to track a mobile device and locate an individual in a California home.<sup>4</sup>

Following the Supreme Court's January 23, 2012 decision in *United States v. Jones*, U.S., 132 S.Ct. 945 (2012), in which the Court unanimously held that it was unconstitutional to install a global positioning device (GPS) on an individual's car and utilize it to track the individual for 28 days without a warrant, the FBI was forced to turn off nearly 3,000 active GPS devices in the field.<sup>5</sup> On April 4, 2012, the American Civil Liberties Union released findings from a 32-state coordinated public records act request seeking the policies, procedures, and practices of state and local law enforcement agencies related to cell tracking, revealing that many government entities were violating the privacy rights of Americans by obtaining location information without a probable cause warrant.<sup>6</sup>

There has been widespread media interest and public concern related to government tracking and surveillance of location information. There is also great urgency to inform the public about governmental efforts to track and surveil individuals because members of Congress and California state legislators are currently weighing new laws related to location tracking – and information shedding lights on the government's current practices would inform those pending legislative debates. It is imperative that Northern California community members and policymakers representing this region immediately gain a full and complete understanding of how the United States Attorneys for the Northern District are seeking or obtaining location information and whether these activities comport with constitutional rights. Access to this information is necessary for a meaningful and informed public debate over these pressing public policy issues and pending legislative debates.

## I. REQUEST FOR INFORMATION

We request disclosure of agency records<sup>7</sup> in your possession created since January 1, 2008,<sup>8</sup> pertaining to efforts to seek or obtain location information utilizing any means.

<sup>3</sup> <http://www.wired.com/threatlevel/2009/12/gps-data/>

<sup>4</sup> See Jennifer Valentino-Devries, "Stingray" Phone Tracker Fuels Constitutional Clash," *Wall Street Journal*, September 21, 2011 (Tab 35).

<sup>5</sup> FBI General Counsel Andrew Weissmann. <http://news.yahoo.com/supreme-court-ruling-prompts-fbi-turn-off-3-154046722--abc-news.html>

<sup>6</sup> <http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>

<sup>7</sup> The term "records" as used herein includes all records preserved in written or electronic form, including but not limited to: court filings, correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training materials, manuals, studies, text messages, social networking posts or messages. To the extent the agency chooses to redact identifying information of individuals, we request that individuals be identified with an alphanumeric code so that multiple records related to the same individual can be recognized as such.

April 13, 2012  
Page 3

“Location information” as used in this request means any information that helps to ascertain the location of an individual or particular electronic device that, in whole or in part, is generated or derived from the operation of an electronic device, including but not limited to a cell phone, smartphone, cell site, global positioning system, cell-site simulator, digital analyzer, stingray, triggerfish, amberjack, kingfish loggerhead, or other electronic device, including both historical and real-time information.

In particular, we seek the following:

- 1) All requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008.
- 2) Any template applications or orders that have been utilized by United States Attorneys in the Northern District to seek or acquire location information since January 1, 2008.
- 3) Any documents since January 1, 2008, related to the use or policies of utilizing any location tracking technology, including but not limited to cell-site simulators or digital analyzers such as devices known as Stingray, Triggerfish, AmberJack, KingFish or Loggerhead.
- 4) Any records related to the Supreme Court’s holding in *United States v. Jones*, excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below.

## II. REQUEST FOR EXPEDITED PROCESSING

Requesters seek expedited processing. This request should be granted because there is widespread media interest in government surveillance methods using new technology to collect detailed, sensitive, personal information, and there is urgency to inform the public about the scope of the government’s practices because of pending legislation on these very issues. The information sought in this request is necessary to contribute to that pending legislative debate.

Title 5 U.S.C. §552(a)(6)(E) provides for expedited processing of requests for information in cases in which the person requesting the records demonstrates a compelling need. Department of Justice regulations state that FOIA requests are entitled to expedited processing when information requested involves “[a] matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence.” 28 CFR §16.5(d)(1)(iv). In addition, for requests by persons primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged federal government activity constitutes a “compelling need.” 5 U.S.C. §552(a)(6)(E)(v)(II); 28 CFR §16.5(d)(1)(ii).

### A. Widespread and exceptional media interest

---

<sup>8</sup> Requestors seek records located either at the United State Attorneys’ Northern District San Francisco, Oakland or San Jose offices, or at any other location where records are stored.

April 13, 2012

Page 4

The federal government's surveillance and tracking of individuals using invasive new technologies but without satisfying the Fourth Amendment's requirements for obtaining warrants based on probable cause is a matter of great public concern. Whether and to what extent the United States Attorney for the Northern District of California is seeking or obtaining location information without a probable cause warrant are matters of great public concern. There are dramatic implications for core democratic values when the federal government engage in location surveillance to spy on ordinary members of the public, critics, dissidents, and those who espouse unpopular views, without adequate judicial oversight. As demonstrated by the extensive coverage of this issue, there is widespread media interest regarding governmental collection of location information.

Location information is very sensitive information and can reveal far more than just an individual's latitude and longitude. As the United States Court of Appeals for the D.C. Circuit explained in 2010 in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010):

"A person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts." *Id.* at 562.

As a result, the media has extensively covered the government's use of location tracking devices, and its efforts to do so without obtaining a warrant based on probable cause. *See, e.g.*, Robert Barnes, "Supreme Court: Warrants needed in GPS tracking," *Washington Post*, January 23, 2012 (Tab 1); Rebecca J. Rosen, "Why the Jones Supreme Court Ruling on GPS Tracking Is Worse Than It Sounds," *The Atlantic*, January 23, 2012 (Tab 2); Ariane de Vogue, "GPS Tracking Requires Warrant, Supreme Court Rules," *ABC*, January 23, 2012 (Tab 3); Barry Friedman, "Privacy, Technology and Law," *New York Times*, January 29, 2012 (Tab 4); Greg Stohr, "Police Use of GPS Devices to Track People Limited by U.S. Supreme Court," *Bloomberg*, January 23, 2012 (Tab 5); Jess Bravin, "Justices Rein In Police on GPS Trackers," *Wall Street Journal*, January 24, 2012 (Tab 6); Editorial, "Navigating the Supreme Court's GPS ruling," *Los Angeles Times*, January 25, 2012 (Tab 7); Bob Egelko, "U.S. Supreme Court to decide major legal issues," *San Francisco Chronicle*, September 30, 2011 (Tab 8); Editorial, "The Court's GPS Test," *New York Times*, November 5, 2011 (Tab 9); David G. Savage, "Supreme Court: warrant required for GPS tracking," *San Francisco Chronicle*, January 24, 2012 (Tab 10); Cristian Salazar, "ACLU demands police disclose cell phone tracking," *San Francisco Chronicle*, August 4, 2011 (Tab 11); Adam Liptak, "Court Case Asks if 'Big Brother' Is Spelled GPS," *New York Times*, September 10, 2011 (Tab 12); Editorial, "A court test of privacy in the digital age," *San Francisco Chronicle*, January 29, 2012 (Tab 13); Adam Liptak, "Justices Say GPS Tracker Violated Privacy Rights," *New York Times*, January 24, 2012 (Tab 14); Julia Angwin, "FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling," *Wall Street Journal*, February 25, 2012 (Tab 15); Joan Biskupic, "Supreme Court rules warrant needed for GPS tracking," *USA Today*, January 24, 2012 (Tab 16); Kashmir Hill, "Supreme Court Deals Blow To Government Surveillance, Saying Warrant Needed For GPS Tracking," *Forbes*, January 23, 2012 (Tab 17); Timothy B. Lee, "GPS ruling is 'hard' on the FBI—and that's a feature, not a bug," *Ars Technica*, March 23, 2012 (Tab 18); Renee Hutchins, "A step



April 13, 2012  
Page 5

back for rights," *Baltimore Sun*, January 29, 2012 (Tab 19); Debra Cassens Weiss, "Jones Decision Spurs FBI to Disable 3,000 GPS Devices and to Consider Legality of Trash Can Trespass," *ABA Journal*, February 28, 2012 (Tab 20); Nina Totenberg, "High Court: Warrant Needed For GPS Tracking Device," *NPR*, January 23, 2012 (Tab 21); Carl Franzen, "What Does The Supreme Court Ruling Against Warrantless GPS Tracking Mean?," *Talking Points Memo*, January 23, 2012 (Tab 22); James Vicini, "Supreme Court rules police need warrant for GPS tracking," *Reuters*, January 24, 2012 (Tab 23); Bill Mears, "Justices rule against police, say GPS surveillance requires search warrant," *CNN*, January 23, 2012 (Tab 24); Mark Sherman, "Supreme Court questions warrantless GPS tracking," *Business Week*, November 8, 2012 (Tab 25); Alex Fitzpatrick, "Supreme Court: GPS Tracking Is Illegal Without Warrant," *Mashable*, January 23, 2012 (Tab 26); Kashmir Hill, "How Many GPS Trackers Is The FBI Actually Using?," *Forbes*, March 27, 2012 (Tab 27); Jim McElhatton, "Supreme Court says police need warrant for GPS tracking," *The Washington Times*, January 23, 2012 (Tab 28); Jessie J. Holland and Pete Yost, "Warrant needed for GPS tracking, high court says," *The Washington Times*, January 23, 2012 (Tab 29); Catherine Crump, "How GPS tracking threatens our privacy," *CNN*, November 7, 2011 (Tab 30); Adam Cohen, "The Government Can Use GPS to Track Your Moves," *Time*, November 25, 2010 (Tab 31); Timothy B. Lee, "Supreme Court ponders constitutionality of 24/7 GPS tracking," *Ars Technica*, November 1, 2011 (Tab 32); Joshua A. Engel, "In 'U.S. v. Jones,' Supreme Court Rules No Warrantless GPS Tracking," *Law.com*, January 23, 2012 (Tab 33); Dahlia Lithwick, "U.S. v. Jones: Supreme Court Justices Alito and Scalia brwl over technology and privacy," *Slate*, January 26, 2012 (Tab 34); Jennifer Valentino-Devries, "Stingray' Phone Tracker Fuels Constitutional Clash," *Wall Street Journal*, November 21, 2011 (Tab 35); Lior J. Strailevitz, "Can the police keep up with Jones?," *Chicago Tribune*, January 27, 2012 (Tab 36); "Want to Use a GPS-Tracking Device? Get a Warrant, Supreme Court Tells Police," *PBS*, January 23, 2012 (Tab 37); "Can Feds track the GPS of every American?," *RT*, November 9, 2011 (Tab 38).

The government's efforts to use GPS devices to engage in location tracking without a warrant were recently rebuffed by the United States Supreme Court in *United States v. Jones*, *supra*. Following that decision, the media continued to report on the issue extensively, including the implications of the *Jones* decision for law enforcement and the fact that the *Jones* decision prompted an increased reliance by law enforcement on cell site location information. *See, e.g.*, David Kravets, "After Car-Tracking Smackdown, Feds Turn to Warrantless Phone Tracking," *Wired*, March 31, 2012 (Tab 39); Editorial, "GPS and the Right to Privacy," *New York Times*, January 25, 2012 (Tab 40); John W. Whitehead, "U.S. v. Jones: The Battle for the Fourth Amendment Continues," *Huffington Post*, January 24, 2012 (Tab 41); Mike Sacks, "Warrantless GPS Tracking Unconstitutional, Supreme Court Rules," *Huffington Post*, January 23, 2012 (Tab 42); David Kravets, "Supreme Court Court Rejects Willy-Nilly GPS Tracking," *Wired*, January 23, 2012 (Tab 43); Dave Bohon, "More Police Agencies Using Warrantless Cell Phone Tracking in Surveillance," *The New American*, April 5, 2012 (Tab 44); Thomas Peracchio, "Supreme court ruling exposes many digital privacy issues," *The Examiner*, April 2, 2012 (Tab 45); Thomas Claburn, "Supreme Court Tackles GPS Tracking Vs. Privacy," *Information Week*, January 23, 2012 (Tab 46); Editorial, "EDITORIAL: Obama wants to track you," *Washington Times*, March 20, 2012 (Tab 47); Emily Babay, "After GPS tracking banned by court, privacy fight turns to cell phone data," *Washington Examiner*, April 1, 2012 (Tab 48).



April 13, 2012  
Page 6

Most recently, the ACLU released a report shedding light on disturbing trend across the country of law enforcement agencies obtaining cell phone location information without probable cause warrants. The ACLU report was initially the subject of a front page *New York Times* article. See Eric Lichtblau, "Police Are Using Phone Tracking as a Routine Tool," *New York Times*, March 31, 2012 (Tab 102).

After the *New York Times* piece appeared, a flurry of news articles on the subject followed, as well as numerous editorials emphasizing the importance of a warrant requirement for cell phone location information. See, e.g., Cristian Salazar, "ACLU demands police disclose cell phone tracking," *San Francisco Chronicle*, August 4, 2011 (Tab 49); James Temple, "How California cops grab phone data from Apple, Google, carriers," *San Francisco Chronicle*, April 3, 2012 (Tab 50); Suzy Khimm, "ACLU: Local police departments tracking cellphones without warrants," *Washington Post*, April 2, 2012 (Tab 51); Declan McCullagh, "How Apple and Google help police bypass iPhone, Android lock screens," *CNET*, April 2, 2012 (Tab 52); Athima Chansanchai, "ACLU: Police track cellphones, too," *MSNBC Technology*, April 2, 2012 (Tab 53); Bob Sullivan, "Pricey 'stingray' gadget lets cops track cellphones without telco help," *MSNBC Red Tape*, April 3, 2012 (Tab 54); Peter Doocy, "Law enforcement under scrutiny by ACLU for tracking cell phones," *Fox News*, April 4, 2012 (Tab 55); American Foreign Press, "Many US police use cell phones to track: study," *American Foreign Press*, April 2, 2012 (Tab 56); Gary Johnson, "Privacy: Ditch the Cell Phone or Prepare to Disrobe," *Huffington Post*, April 5, 2012 (Tab 57); Adam Levine, "The New American Pie: Breached, Tracked and Strip Searched," *Huffington Post*, April 5, 2012 (Tab 58); Josh Gerstein, "Key Patriot Act opinions may not be classified," *Politico*, March 16, 2012 (Tab 59); Editorial, "EDITORIAL: Individual cell phone privacy is compromised," *Fresno Bee*, April 11, 2012 (Tab 60); Brendan Sasso, "ACLU report: Warrantless tracking of cellphones 'pervasive and frequent'," *The Hill*, April 2, 2012 (Tab 61); James Temple, "Why cell-phone tracking should require a warrant," *San Francisco Chronicle*, April 2, 2012 (Tab 62); John Moe, "Warrantless cell phone tracking is everywhere," *Marketplace*, April 4, 2012 (Tab 63); Grant Gross, "ACLU: Most US Police Don't Seek Warrants Before Tracking Cell Phones," *PC World*, April 2, 2012 (Tab 64); Josh Smith, "ACLU: Most Police Departments Track Cellphones Without Warrants," *National Journal*, April 2, 2012 (Tab 65); Timothy B. Lee, "Documents show cops making up the rules on mobile surveillance," *Ars Technica*, April 3, 2012 (Tab 66); Jay Bookman, "The dangerous nexus of privacy, liberty and government," *Atlanta Journal Constitution*, April 2, 2012 (Tab 67); Anne Blythe, "Police scrutiny of mobile device data raises concerns," *News & Observer*, April 3, 2012 (Tab 68); Andy Greenberg, "These Are The Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps," *Forbes*, April 3, 2012 (Tab 69); Julian Sanchez, "Cell Phone Location Surveillance: Now at a Police Dept. Near You!," *Cato*, April 2, 2012 (Tab 70); Darlene Storm, "ACLU: Cops often violate Americans' privacy by warrantless cell phone tracking," *Computerworld*, April 2, 2012 (Tab 71); Debra Cassens Weiss, "Local Police Increasingly Use Cellphone Tracking, Sometimes Without a Warrant," *ABA Journal*, April 2, 2012 (Tab 72); David Dayen, "Pervasive Cell Phone Tracking Performed Even By Local Law Enforcement," *Firedoglake*, April 2, 2012 (Tab 73); Kevin Gosztoła, "ACLU: US Law Enforcement Often Track Cell Phones Without a Warrant," *Firedoglake*, April 2, 2012 (Tab 74); Jacob Sullum, "ACLU Says Police Often Obtain Cellphone Location Data Without Warrants," *Reason*, April 2,

April 13, 2012  
Page 7

2012 (Tab 75); Andrew Jones, "ACLU: Many local police tracking cell phones without warrants," *Raw Story*, April 2, 2012 (Tab 76); Tiffany Kaiser, "ACLU Finds U.S. Police Departments Using Cell Phone Tracking, Sometimes Warrantless," *Daily Tech*, April 4, 2012 (Tab 77); James Gaskin, "Cell phone tracking now routine police action," *IT World*, April 2, 2012 (Tab 78); Scott Daniels, "APD admits to tracking cell phones," *KRQE*, April 2, 2012 (Tab 79); Amy Gahrn, "ACLU: Most police track phones' locations without warrants," *CNN*, April 3, 2012 (Tab 80); Jennifer Waters, "Your cell phone is telling your secrets," *Market Watch*, April 6, 2012 (Tab 81); Helen A.S. Popkin, "Carriers charge cops for cellphone information," *MSNBC Technology*, April 4, 2012 (Tab 82); Jeff Homan, "Technology outpaces laws, raises concerns," *Collegiate Times*, April 5, 2012 (Tab 83); Mike Fossum, "How Cops Get Into Locked iPhone," *Web Pro News*, April 4, 2012 (Tab 84); Scott Schwebke, "ACLU questions cellphone tracking policies of law enforcement," *Standard*, April 4, 2012 (Tab 85); Viviane Vo-Duc, "ACLU: Many law enforcement agencies obtain cellphone tracking information without a warrant," *Deseret News*, April 5, 2012 (Tab 86); Robert Siegel, "Phone Tracking Big Business For Cell Companies," *NPR*, April 5, 2012 (Tab 87); Fox Report, "ACLU Claims Police are Tracking Cell Phones Without a Warrant," *Fox News Insider*, April 4, 2012 (Tab 88); Michael Santo, "ACLU-obtained documents show police use of cell phone tracking becoming routine," *Examiner*, April 1, 2012 (Tab 89); Editorial, "Editorial: Cell phone privacy is on the line," *Sacramento Bee*, April 8, 2012 (Tab 90); Jill Redhage, "Cellphone data draws scrutiny," *Daily Journal*, March 30, 2012 (Tab 91); Levi Sumagaysay, "Watching Big Brother: The cops and cell phones in the U.S., the U.K.'s monitoring plans," *Silicon Valley*, April 2, 2012 (Tab 92); Jack A. Smith, "BIG BROTHER'S GETTING BIGGER," *The People's Voice*, April 10, 2012 (Tab 93); Editorial, "Who's listening? Authorities engaging in cellphone tracking," *Las Vegas Review-Journal*, April 10, 2012 (Tab 94); Brian Duggan, "ACLU: Police using cellphone tracking, including RPD; Reno says court approval always obtained," *Montgomery Advertiser*, April 6, 2012 (Tab 95); Associated Press, "ACLU finds Nevada police use cellphone tracking," *Las Vegas Sun*, April 8, 2012 (Tab 96); "ACLU finds widespread warrantless cell phone tracking by local police," *Info Security*, April 3, 2012 (Tab 97); "Cop's 'ear' in your pocket: Cell phone tracking routine with US police," *RT*, April 1, 2012 (Tab 98); "ACLU: Many local police track cell phones without warrants," *Press TV*, April 2, 2012 (Tab 99); "ACLU: Cell phone tracking by police widespread," *Homeland Security News Wire*, April 4, 2012 (Tab 100); "Cell Phone Tracking Raises Eyebrows," *Fox News*, August 4, 2011 (Tab 101);

#### B. Urgency to inform the public

There is great urgency in shedding light on location tracking by the government. The information sought in this FOIA request would contribute to the ongoing national debate on this topic generally, as well as specific legislative debates over the legal standard that should apply when the government seeks location information.

Justice Alito in his concurring opinion in *Jones* urges legislative action, noting that "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way. To date,



April 13, 2012  
Page 8

however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes.” 132 S.Ct. at 964.

Members of Congress representing Northern California, including Representatives Zoe Lofgren and Barbara Lee, are currently working on bipartisan efforts to pass a federal location privacy bill, the GPS Act,<sup>9</sup> and state lawmakers, including State Senator Mark Leno, are working on state location privacy laws.<sup>10</sup> There is great urgency in shedding light on whether the Department of Justice is adhering to constitutional standards: The information sought herein would contribute to ongoing societal and legislative debates and help the public and Bay Area policymakers assess what new laws should be implemented to better protect the public from “warrantless surveillance.” *Elec. Priv. Info. Ctr. V. Dept. of Justice*, 416 F.Supp.2d 30, 41 (D.D.C. 2006) (granting preliminary injunction requiring agency to produce information where FOIA request sought information “vital to the current and ongoing debate surrounding the legality of the Administration’s warrantless surveillance program”); *see also Elec. Frontier Fdn. V. Ofc. Of Dir. Of Natl. Intelligence*, 542 F.Supp.2d 1181, 1187 (N.D. Cal. 2008) (granting preliminary injunction requiring agency to produce information where “Congress is considering legislation that would amend the FISA and the records may enable the public to participate meaningfully in the debate over such pending legislation.”).

Further, requesters ACLU-NC and *Bay Guardian* are primarily engaged in disseminating information. The ACLU-NC is an affiliate of the ACLU, a national organization that works to protect the civil liberties of all people, including the safeguarding of the basic constitutional rights to privacy, free expression, and due process of law. The ACLU-NC is responsible for serving the population of northern California. The communications department of the ACLU-NC is the division of the ACLU-NC that is responsible for disseminating information to the public about issues of concern to the ACLU-NC and to the general public.

The *Bay Guardian* is the largest circulation newsweekly in northern California, with an audited weekly distribution of 100,000. Its website (sfbg.com) receives about 350,000 page views per month. The paper is locally owned, independent, and has been published continuously since 1966.

In short, expedited processing is warranted here because there is an urgency to inform the public about actual or alleged location tracking surveillance and requesters are primarily engaged in disseminating information. *See* 5 U.S.C. §552(a)(6)(E)(v)(II); 28 CFR §16.5(d)(1)(ii). Moreover, location tracking by the government is a matter of widespread and exceptional media interest. When the government utilizes technology to spy on citizens without adequate judicial oversight, the public confidence is deeply affected. *See* 28 CFR §16.5(d)(1)(iv). In this regard, this request is very similar other FOIA requests by ACLU-NC and *Bay Guardian*, seeking information about federal government surveillance practices and as to which the Department of

<sup>9</sup> <http://www.govtrack.us/congress/bills/112/hr2168>

<sup>10</sup> [http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb\\_1401-1450/sb\\_1434\\_bill\\_20120409\\_amended\\_sen\\_v98.html](http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_bill_20120409_amended_sen_v98.html)

April 13, 2012  
Page 9

Justice (Federal Bureau of Investigation) granted expedited processing. *See* FOIA Request Nos. 1144839-00 & 1184877-000.<sup>11</sup>

### III. REQUEST FOR WAIVER OF PROCESSING FEES

We request a waiver of process fees. In a recent request by requesters ACLU-NC and *Bay Guardian*, the FBI granted the fee waiver. *See* FOIA Request No. 1144839-000. Such a waiver is appropriate here for two reasons.

First, the *Bay Guardian* and communications department of the ACLU-NC are “representative[s] of the news media.” Fees associated with the processing of this request should therefore be “limited to reasonable standard charges for document duplication.” 5 U.S.C. §552(a)(4)(A)(ii)(II).

As noted above, the *Bay Guardian*, is the largest circulation newsweekly in northern California, with an audited weekly distribution of 100,000. Its website receives about 350,000 page views per month. The paper is locally owned, independent, and has been continuously published since 1966. The paper covers breaking news, does detailed investigative reporting, publishes editorials and covers arts, entertainment and lifestyle issues. The *Bay Guardian* has received more than 100 state, local, and national awards for journalistic excellence. Executive Editor Tim Redmond, for example, is the recipient of the 2012 Professional Journalist award from the Society of Professional Journalists, Northern California Chapter, for his investigation of state agencies’ legally questionable acquisitions of a drug used for lethal injections that is no longer produced in the United States, an investigative series based in part on documents uncovered by the *Bay Guardian* and ACLU-NC in FOIA requests to various federal agencies. The *Bay Guardian* is a member of the California Newspaper Publishers Association and the Association of Alternative Newsweeklies.

Similarly, the ACLU-NC’s communication department publishes newsletters, news briefings, right to know materials, and other materials that are disseminated to the public. Its material is widely available to everyone, including tax-exempt organizations, not-for-profit groups, law students and faculty, for no cost or for a nominal fee. The ACLU-NC’s communications department also disseminates information through the website <http://www.aclunc.org>, which had 127,475 visitors in 2011. This website addresses civil liberties issues in depth and provides features on civil liberties issues on which the ACLU-NC is focused. ACLU-NC staff persons are frequent spokespersons in television and print media and make frequent public presentations at meetings and events. Finally, the ACLU-NC’s communications department disseminates information through newsletters which are distributed

---

<sup>11</sup> *See also* *ACLU-NC, et al. v. Dept. of Defense*, 2006 WL 1469418, Case No. 06-01698 (N.D. Cal. May 25, 2006) (ordering Department of Defense to comply with request for expedited processing by ACLU-NC and *Bay Guardian*).



April 13, 2012  
Page 10

to subscribers by mail. Due to these extensive publication activities, the ACLU-NC is a “representative of the news media” under the FOIA and agency regulations.<sup>12</sup>

The records requested are not sought for commercial use.

Second, a fee waiver for duplication costs should be granted for the independent reason that disclosure of the requested information is in the public interest. *See* 5 U.S.C. §552(a)(4)(ii)(II)-(iii). It will further public understanding of government conduct, in particular, the Department of Justice’s policies, practices, and methods of surveillance. The ACLU-NC’s communications department is a division of a nonprofit 501(c)(3) organization, and both the ACLU-NC’s communications department and the *Bay Guardian* are “representative[s] of the news media.” They are well situated to disseminate information gained through this request to the public, to affected communities and to political and religious organizations.

If the fee waivers are denied, the requesters are prepared to pay fees up to \$25 and request to be informed of further fees that may be charged, but reserve the right to appeal a denial of fee waivers.

\* \* \*

If this request for information is denied in whole or in part, we ask that you justify all deletions by reference to specific provisions of the Freedom of Information Act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information.

Thank you for your prompt attention to this matter. Please furnish all applicable records to Nicole Ozer, American Civil Liberties Union of Northern California, 39 Drumm Street, San Francisco, California, 94111, telephone 415 621 2493.

I affirm that the information provided supporting the request for expedited processing and the fee waiver is true and correct to the best of our knowledge and belief.

Sincerely,



Nicole A. Ozer  
Technology and Civil Liberties Policy Director  
ACLU of Northern California

Also on behalf of  
*San Francisco Bay Guardian*

---

<sup>12</sup> Courts have found that organizations with missions similar to that of the ACLU and that engage in similar information dissemination activities are “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F.Supp.2d 246, 260 (D.D.C. 2005).

# Exhibit 2



U.S. Department of Justice

United States Attorney  
Northern District of California

APR 23 2012

11th Floor, Federal Building  
450 Golden Gate Avenue, Box 36055  
San Francisco, California 94102-3495

(415) 436-7200  
FAX: (415) 436-7234

April 17, 2012

VIA U.S. MAIL

Nicole A. Ozer  
Technology and Civil Liberties Policy Director  
ACLU of Northern California  
39 Drumm Street  
San Francisco, CA 94111

Freedom of Information Request

Dear Ms. Ozer:

This letter acknowledges receipt of your request for information under the Freedom of Information Act, sent to the United States Attorney's Office of the Northern District of California, dated April 13, 2012.

We are forwarding your request to the U.S. Department of Justice, Freedom of Information/Privacy Act Unit for processing, as all Freedom of Information requests to the U.S. Attorney's Office are handled by that unit.

Very truly yours,

MELINDA HAAG  
United States Attorney

  
LILIBETH MARGEN  
Paralegal Specialist

cc: Shirley Botts  
U.S. Department of Justice  
Freedom of Information /Privacy Act Unit  
(With Enclosure)

# Exhibit 3





## U.S. Department of Justice

Executive Office for United States Attorneys  
 Freedom of Information & Privacy Staff  
 600 E Street, N.W., Suite 7300, Bicentennial Building  
 Washington, DC 20530-0001  
 (202) 252-6020 FAX: 252-6047 (www.usdoj.gov/usao)

Requester: Nicole A. OzerRequest No.: 12-1293

APR 23 2012

Subject: Location Tracking/CAN

The Executive Office for United States Attorneys (EOUSA) has received your Freedom of Information Act/Privacy Act (FOIA/PA) request. It has been assigned the above number. Please give us this number if you write about your request. If we need additional information, we will contact you within two weeks.

Your request will be placed in the order in which it was received for processing, unless it is a very large request (Project Request). Then, it will be placed in a separate group of Project Requests, which are also processed in the order received.

EOUSA makes every effort to process most requests within a month (20 working days). There are some exceptions, for example, Project Requests take approximately nine months to process. Requests for "all information about myself in criminal case files" are usually Project Requests. If you have made such a request, you may either write us and narrow your request for specific items, or you may expect that the processing of your request may take nine months from the date of this letter.

By making a FOIA/PA request, you have agreed to pay fees up to \$25, as stated in 28 CFR § 16.3(c), unless you have requested a fee waiver. Although you appear to qualify as a requester who is not subject to search fees, please note that pursuant to 28 CFR § 16.11, if you have not been granted a fee waiver, we are required to charge duplication fees at \$0.10 per page after the first 100 pages which are free. Please do not send any payment at this time! If we anticipate that fees will exceed \$25 or the amount you have stated in your letter (if greater than \$25), we will normally notify you of our estimate of fees. After we have received your agreement to pay for the expected fees (or you have narrowed your request to reduce fees) and we have processed your request, we will require payment for the accumulated charges before we release documents to you. Without such payment, your request file will be closed without further action.

If you wish to revise your request to try to reduce fees, you may use the attached form. If you do not wish to incur fees for your request as it is now stated, please submit this form (or your letter revising your request) to us immediately so that your request, and fees, can be limited.

Sincerely,

  
 Susan B. Gerson  
 Acting Assistant Director

Form No. 001B -4/11

Requester: Nicole A. Ozer Request Number: 12-1293

**CHOOSE ONE**

       I understand that I am entitled to the first 100 pages free. Please process only up to 100 pages that can be released to me.

       I wish to withdraw my request.

       I wish to revise my request to try to reduce fees. Please limit my request to the following documents:

---

---

---

---

\_\_\_\_\_  
Name

\_\_\_\_\_  
Date

Please return to:

EOUSA  
FOIA/PA Staff  
600 E. Street, N.W., Room 7300  
Washington D.C., 20530

Nicole Ozer  
#12-1293

Note: Your request is being expedited. This does not guarantee that records will be released within the statutory time limits.

# Exhibit 4





July 6, 2012

Via United States mail

Susan B Gerson  
Acting Assistant Director  
United States Department of Justice  
EOUSA  
FOIA/PA STAFF  
600 E. Street, N.W., Room 7300  
Washington D.C., 20530

Re: Request Number 12-1293

Dear Ms. Gerson:

I write in regard to the above-referenced Freedom of Information Act request, dated April 13, 2012, on which expedited processing has been granted. Almost three months have passed from the date of our request and we have not yet received an indication as to when we can anticipate receiving any records. This delay exceeds the twenty working day period under FOIA within which the FBI is required to notify us of a determination whether it intends to comply with our request. *See* 5 U.S.C. §552(a)(6)(A)(i). We request a response at your earliest convenience. Please feel free to call me or my assistant Nishtha Jolly at 415 621 2493 if you have any questions or have any information you can provide as to the status of our request. Your assistance is greatly appreciated.

Sincerely,

Linda Lye  
Staff Attorney

MICHELLE A. WELSH, CHAIRPERSON | DENNIS McNALLY, AJAY KRISHNAN, FARAH BRELVI, ALLEN ASCH, VICE CHAIRPERSONS | KENNETH SUGARMAN, SECRETARY/TREASURER  
ABDI SOLTANI, EXECUTIVE DIRECTOR | KELLI EVANS, ASSOCIATE DIRECTOR | CHERI DRYANT, DEVELOPMENT DIRECTOR | SHAYNA GELENDER, ORGANIZING & COMMUNITY ENGAGEMENT DIRECTOR  
LAURA SAPONARA, COMMUNICATIONS DIRECTOR | ALAN SCHLOSSER, LEGAL DIRECTOR | MARGARET C. CROSBY, ELIZABETH GILL, LINDA LYE, JULIA HARUMI MASS, MICHAEL RISHER, JORY STEELE, STAFF ATTORNEYS  
PHYLLIDA BURLINGAME, ALLEN HOPPER, NATASHA MINSKER, NICOLE A. OZER, DIANA TATE VERMEIRE, POLICY DIRECTORS | STEPHEN V. BOMSE, GENERAL COUNSEL

70 F.Supp.3d 1018  
United States District Court,  
N.D. California.

American Civil Liberties Union of  
Northern California, et al., Plaintiffs,  
v.  
Department of Justice, Defendant.

Case No. 12-cv-04008-MEJ  
| Signed September 30, 2014

### Synopsis

**Background:** Requesters brought action against Department of Justice (DOJ) under Freedom of Information Act (FOIA) to compel release of documents regarding use of location tracking technology to monitor and surveil suspects. Parties moved for partial summary judgment.

**Holdings:** The District Court, [Maria-Elena James](#), United States Magistrate Judge, held that:

[1] documents on use of location tracking technology did not constitute working law subject to disclosure as exception to deliberative process exemption;

[2] template for federal prosecutor's application and order for use of pen register and trap and trace device was not attorney work product subject to deliberative process exemption;

[3] pages from federal prosecutors' presentation on use of location tracking devices was attorney work product that was exempt from disclosure pursuant to deliberative process exemption;

[4] memoranda for federal prosecutors regarding use of location tracking devices were attorney work product that was exempt from disclosure pursuant to deliberative process exemption;

[5] portions of federal prosecutors' legal resource book and reference guide that dealt with location tracking devices were not attorney work product; and

[6] discussion of location tracking technology in legal resource book and reference guide was not exempt from disclosure as information that would reveal law enforcement

investigative techniques and procedures that were not publicly known.

Motions granted in part and denied in part.

West Headnotes (31)

### [1] Records

#### Evidence and burden of proof

Strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any documents requested under Freedom of Information Act (FOIA). [5 U.S.C.A. § 552](#).

[Cases that cite this headnote](#)

### [2] Federal Civil Procedure

#### Records, disclosure, and privacy, cases involving

On a motion for summary judgment in a case under Freedom of Information Act (FOIA), underlying facts and possible inferences are construed in favor of the requester. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

### [3] Federal Civil Procedure

#### Records, disclosure, and privacy, cases involving

To carry its burden on summary judgment in case under Freedom of Information Act (FOIA), agency may be required to submit a “*Vaughn* index,” including detailed public affidavits, that identifies the documents withheld, the FOIA exemptions claimed, and a particularized explanation of why each document falls within the claimed exemption. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

### [4] Federal Civil Procedure

🔑 [Records, disclosure, and privacy, cases involving](#)

To carry its burden on summary judgment in case under Freedom of Information Act (FOIA), affidavits in agency's [Vaughn](#) index must be from affiants who are knowledgeable about the information sought and detailed enough to allow court to make an independent assessment of the government's claim of exemption. [5 U.S.C.A. § 552\(a\)\(4\)\(B\)](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

[5] **Federal Civil Procedure**

🔑 [Records, disclosure, and privacy, cases involving](#)

On motion for summary judgment in case under Freedom of Information Act (FOIA), first step of the inquiry requires the court to determine whether the agency has met its burden of proving that it fully discharged its obligations under FOIA, and in the second stage of the inquiry, the court examines whether the agency has proven that the information that it withheld falls within one of the nine FOIA exemptions. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

[6] **Federal Civil Procedure**

🔑 [Records, disclosure, and privacy, cases involving](#)

On motion for summary judgment in case under Freedom of Information Act (FOIA), agency may submit affidavits to satisfy its burden of proving that the information that it withheld falls within one of the nine FOIA exemptions, but agency may not rely upon conclusory and generalized allegations of exemptions. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

[7] **Federal Civil Procedure**

🔑 [Records, disclosure, and privacy, cases involving](#)

On motion for summary judgment in case under Freedom of Information Act (FOIA),

agency's affidavits must contain reasonably detailed descriptions of withheld documents and allege facts sufficient to establish an exemption. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

[8] **Federal Civil Procedure**

🔑 [Records, disclosure, and privacy, cases involving](#)

On motion for summary judgment in case under Freedom of Information Act (FOIA), court accords substantial weight to an agency's declarations regarding the application of a FOIA exemption. [5 U.S.C.A. § 552](#); [Fed. R. Civ. P. 56](#).

[Cases that cite this headnote](#)

[9] **Records**

🔑 [In general; freedom of information laws in general](#)

Freedom of Information Act's (FOIA) core purpose is to inform citizens about what their government is up to. [5 U.S.C.A. § 552](#).

[Cases that cite this headnote](#)

[10] **Records**

🔑 [Matters Subject to Disclosure; Exemptions](#)

Use of exemptions under Freedom of Information Act (FOIA) is within agency's discretion. [5 U.S.C.A. § 552\(b\)\(1\)-\(9\)](#).

[Cases that cite this headnote](#)

[11] **Records**

🔑 [Matters Subject to Disclosure; Exemptions](#)

Exemptions under Freedom of Information Act (FOIA) are exclusive, and thus information not falling within the scope of an exemption must be disclosed. [5 U.S.C.A. § 552\(b\)\(1\)-\(9\)](#).

[Cases that cite this headnote](#)

[12] **Records**

🔑 [Matters Subject to Disclosure; Exemptions](#)

Exemptions under Freedom of Information Act (FOIA) are narrowly construed. 5 U.S.C.A. § 552(b)(1)-(9).

[Cases that cite this headnote](#)

### [13] Records

🔑 Internal memoranda or letters; executive privilege

Pursuant to “secret law exception” or “working law exception” to deliberative process exemption under Freedom of Information Act (FOIA), if an agency’s memorandum or other document has become its effective law and policy it will be subject to disclosure as the working law of the agency. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)

### [14] Records

🔑 Internal memoranda or letters; executive privilege

Agency documents may be properly characterized as “working law” subject to disclosure under Freedom of Information Act (FOIA) as exception to deliberative process exemption when the documents resemble final opinions, statements of policy, and interpretations which have been adopted by the agency, and instructions to staff that affect a member of the public. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)

### [15] Records

🔑 Internal memoranda or letters; executive privilege

Department of Justice (DOJ) documents on use of location tracking technology did not constitute working law subject to disclosure as exception to deliberative process exemption under Freedom of Information Act (FOIA); documents did not represent final agency opinions or statements of policy and interpretations that had been adopted by DOJ and had force and effect of law, rather, documents reflected DOJ’s interpretation of recent case law and would affect only the

strategies used to obtain court permission to use location tracking techniques by law enforcement officers in criminal prosecutions. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)

### [16] Records

🔑 Internal memoranda or letters; executive privilege

Secret law exception to deliberative process exemption under Freedom of Information Act (FOIA) generally applies when agencies are rendering decisions based on non-public analyses. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)

### [17] Records

🔑 Internal memoranda or letters; executive privilege

Department of Justice (DOJ) documents discussing litigation strategies with respect to use of location tracking technology did not constitute working law subject to disclosure as exception to deliberative process exemption under Freedom of Information Act (FOIA); documents were neither directives, nor interpretations of DOJ regulations, nor part of a body of law promulgated by DOJ, rather, documents presented arguments and litigating positions that federal prosecutors could pursue on case-by-case basis, and documents did not require prosecutors to make any particular arguments. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)

### [18] Records

🔑 Internal memoranda or letters; executive privilege

“Deliberative process exemption” to disclosure under Freedom of Information Act (FOIA) essentially grants an agency the same power to withhold documents as it would have in the civil discovery context. 5 U.S.C.A. § 552(b)(5).

[Cases that cite this headnote](#)



**[19] Federal Civil Procedure**

🔑 [Work Product Privilege; Trial Preparation Materials](#)

To be withheld as attorney work-product, document must have been prepared by an attorney or his or her agent “in anticipation of litigation,” which extends beyond an attorney’s preparation for a case in existing litigation and includes documents prepared in anticipation of foreseeable litigation, even if no specific claim is contemplated. [Fed. R. Civ. P. 26\(b\)\(3\)](#).

[Cases that cite this headnote](#)

**[20] Records**

🔑 [Internal memoranda or letters; executive privilege](#)

Template for federal prosecutor’s application and order for use of pen register and trap and trace device was not attorney work product subject to deliberative process exemption from withholding under Freedom of Information Act (FOIA); template did not provide legal theories or strategies for use in specific criminal litigation, rather, template consisted of general instructions to government attorneys on how to apply for an order for location tracking information. [5 U.S.C.A. § 552\(b\)\(5\); Fed. R. Civ. P. 26\(b\)\(3\)](#).

[1 Cases that cite this headnote](#)

**[21] Federal Civil Procedure**

🔑 [Work Product Privilege; Trial Preparation Materials](#)

Work-product rule does not protect from disclosure every written document generated by an attorney, rather, the documents must at least have been prepared with a specific claim supported by concrete facts which would likely lead to litigation. [Fed. R. Civ. P. 26\(b\)\(3\)](#).

[Cases that cite this headnote](#)

**[22] Records**

🔑 [Internal memoranda or letters; executive privilege](#)

Department of Justice (DOJ) guidelines and manuals that set forth general standards for United States Attorneys are not attorney work product that may be withheld from disclosure under Freedom of Information Act (FOIA) pursuant to deliberative process exemption; such documents are not prepared in anticipation of a particular trial, even though they might be prepared literally in anticipation of litigation. [5 U.S.C.A. § 552\(b\)\(5\); Fed. R. Civ. P. 26\(b\)\(3\)](#).

[Cases that cite this headnote](#)

**[23] Federal Civil Procedure**

🔑 [Work Product Privilege; Trial Preparation Materials](#)

Where government lawyers act as legal advisors protecting their agency clients from the possibility of future litigation, the work product privilege can apply to documents advising the agency as to potential legal challenges. [Fed. R. Civ. P. 26\(b\)\(3\)](#).

[Cases that cite this headnote](#)

**[24] Federal Civil Procedure**

🔑 [Work Product Privilege; Trial Preparation Materials](#)

When government lawyers are clearly acting as prosecutors, and not as attorneys advising an agency client on potential liability, the work product privilege only attaches to documents prepared in the course of an active investigation focusing upon specific events and a specific possible violation by a specific party. [Fed. R. Civ. P. 26\(b\)\(3\)](#).

[Cases that cite this headnote](#)

**[25] Records**

🔑 [Internal memoranda or letters; executive privilege](#)

Pages from federal prosecutors’ presentation on use of location tracking devices was attorney work product that was exempt from disclosure under Freedom of Information Act (FOIA) pursuant to deliberative process exemption; pages’ content was not merely general agency

policy or instructions on how to apply for orders authorizing use of location tracking devices, rather, pages contained legal analysis of issues that could arise in connection with use of location tracking devices in foreseeable litigation arising out of federal government's criminal investigations. 5 U.S.C.A. § 552(b)(5); Fed. R. Civ. P. 26(b)(3).

Cases that cite this headnote

#### [26] Records

🔑 Internal memoranda or letters; executive privilege

Memoranda for federal prosecutors regarding use of location tracking devices were attorney work product that was exempt from disclosure under Freedom of Information Act (FOIA) pursuant to deliberative process exemption; memoranda were not intended to function as agency manual or provide neutral analysis of the law, rather, memoranda were prepared in response to recent federal court decisions on tracking technology and discussed potential legal strategies, defenses, and arguments that might be considered by federal prosecutors in future litigation. 5 U.S.C.A. § 552(b)(5); Fed. R. Civ. P. 26(b)(3).

Cases that cite this headnote

#### [27] Federal Civil Procedure

🔑 Work Product Privilege; Trial Preparation Materials

Where the purpose of government attorney's documents is to convey litigation strategy, rather than convey routine agency policy, they are entitled to work product protection. Fed. R. Civ. P. 26(b)(3).

1 Cases that cite this headnote

#### [28] Records

🔑 Internal memoranda or letters; executive privilege

Portions of federal prosecutors' legal resource book and reference guide that dealt with location tracking devices were not attorney work

product that was exempt from disclosure under Freedom of Information Act (FOIA) pursuant to deliberative process exemption; documents were not litigation specific, but rather fit general description of guidance and included templates for use in obtaining location tracking information or devices. 5 U.S.C.A. § 552(b)(5); Fed. R. Civ. P. 26(b)(3).

Cases that cite this headnote

#### [29] Records

🔑 Personal privacy considerations in general; personnel matters

##### Records

🔑 Discretion and equitable considerations; balancing interests

Freedom of Information Act (FOIA) privacy exemption requires court to protect, in the proper degree, the personal privacy of citizens against the uncontrolled release of information, and thus the usual rule that the requester need not offer a reason for requesting the information is inapplicable and court must instead balance the public interest in disclosure against the privacy interest Congress intended the exemption to protect. 5 U.S.C.A. § 552(b)(6).

Cases that cite this headnote

#### [30] Records

🔑 Investigatory or law enforcement records

Freedom of Information Act (FOIA) exemption from disclosure for law enforcement techniques and procedures applies only to investigative techniques not generally known to the public or to detailed information regarding a publicly known technique where the public disclosure did not provide a technical analysis of the techniques and procedures used to conduct law enforcement investigations. 5 U.S.C.A. § 552(b)(7)(E).

1 Cases that cite this headnote

#### [31] Records

🔑 Investigatory or law enforcement records

Discussion of location tracking technology in legal resource book and reference guide

for federal prosecutors was not exempt from disclosure under Freedom of Information Act (FOIA) as information that would reveal law enforcement investigative techniques and procedures that were not publicly known; requested information dealt with publicly well-known tracking technology, including use of location information from wireless carriers, global position systems (GPS), and cell site simulators, although government contended public was not aware of specifics of how or when technology was used. 5 U.S.C.A. § 552(b)(7).

[Cases that cite this headnote](#)

#### Attorneys and Law Firms

**\*1022** [Linda Lye](#), [Michael Temple Risher](#), ACLU Foundation of Northern California, Inc., San Francisco, CA, for Plaintiffs.

[Brad Prescott Rosenberg](#), U.S. Department of Justice, Washington, DC, for Defendant.

### ORDER ON CROSS MOTIONS FOR PARTIAL SUMMARY JUDGMENT

**Re: Dkt. Nos. 23, 25**

[MARIA-ELENA JAMES](#), United States Magistrate Judge

#### INTRODUCTION

On July 31, 2012, Plaintiffs American Civil Liberties Union and San Francisco Bay Guardian filed this lawsuit under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, seeking to compel the release of documents of the United State Attorney’s Office for the Northern District of California regarding use of location tracking technology in Northern California. Compl., Dkt. No. 1 at ¶ 1. Pending before the Court are Plaintiffs’ and Defendant United States Department of Justice’s (the “DOJ” or the “Government”) cross-motions for partial summary judgment. Dkt. Nos. 23 (Gov.Mot.), 25 (Pl.Mot.). On September 5, 2013, the Court held a hearing on the motions. Having considered the parties’ positions, relevant legal authority, and the record in this case, the Court

GRANTS IN PART and DENIES IN PART the DOJ’s Motion for Partial Summary Judgment, and GRANTS IN PART and DENIES IN PART Plaintiffs’ Cross-Motion for Partial Summary Judgment for the reasons set forth below.

#### BACKGROUND

On April 13, 2012, Plaintiffs submitted to the DOJ a FOIA request seeking information about the federal government’s use of **\*1023** location tracking technology to monitor and surveil suspects. Compl. ¶ 3 & Ex. 1; Decl. of John W. Kornmeier (“Kornmeier Decl.”) ¶ 4 & Ex. A, Dkt. No. 23–1. Specifically, Plaintiffs’ FOIA request sought the following materials:

- 1) All requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008.
- 2) Any template applications or orders that have been utilized by United States Attorneys in the Northern District to seek or acquire location information since January 1, 2008.
- 3) Any documents since January 1, 2008, related to the use or policies of utilizing any location tracking technology, including but not limited to cellsite simulators or digital analyzers such as devices known as Stingray, Triggerfish, AmberJack, KingFish or Loggerhead.
- 4) Any records related to the Supreme Court’s holding in [United States v. Jones](#), excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below.

Kornmeier Decl., Ex. A.

Plaintiffs requested expedited processing pursuant to 5 U.S.C. § 522(a)(6)(E), on the grounds that there is an “urgency to inform the public about actual or alleged federal government activity,” and also that this is “a matter of widespread and exceptional media interest in which there exists possible questions about the government’s integrity which affect public confidence.” Compl. ¶ 3 (quoting 28 C.F.R. § 1.6.5(d)(l)(ii) & (iv)). On April 23, 2012, the DOJ granted Plaintiffs’ request for expedited processing. Compl. ¶ 24 & Ex. 3. However, after the DOJ failed to produce responsive documents and did not respond to Plaintiffs’ inquiry regarding the status of the FOIA request, Plaintiffs initiated this lawsuit.

Compl. ¶¶ 25–28. In their Complaint, Plaintiffs assert a claim for wrongful withholding of agency records under FOIA, and seek injunctive relief ordering the DOJ to immediately process the requested records and make them available to Plaintiffs. *Id.* ¶¶ 32–24.

Subsequently, after this lawsuit was filed, counsel for the Government and Plaintiffs conferred numerous times regarding the scope and processing of Plaintiffs' FOIA request. As a result of those discussions, on January 3, 2013, the parties negotiated a Stipulation regarding the processing of Parts 2–4 of Plaintiffs' FOIA request. *See* Dkt. No. 17, Ex. 1 (Appendix); Kornmeier Decl. ¶ 4. That Stipulation clarified the scope of Parts 2–4 of Plaintiffs' FOIA request and defined the steps that DOJ would take to search for records responsive to those parts of the FOIA request. Dkt. No. 17. There is no dispute that DOJ complied with the requirements of the Stipulation regarding the adequacy of its search for responsive records. *Id.*

In processing the FOIA request, the Executive Office for United States Attorneys (“EOUSA”) identified some potentially responsive records that it referred to the DOJ's FOIA/Privacy Act (“FOIA/PA”) Unit of the Office of Enforcement Operations in the Criminal Division, as those records were authored and maintained by that Division. Kornmeier Decl. ¶ 4; Declaration of John E. Cunningham III (“First Cunningham Decl.”) ¶ 8, Dkt. No. 23–2. EOUSA processed the remaining records. Kornmeier Decl. ¶ 5. With respect to the records referred, on February 27, 2013, the EOUSA, in a two-part referral, referred a total of 535 pages of records to the Criminal Division. First Cunningham Decl. ¶ 8. Part one of EOUSA's referral to the Criminal Division consisted of three documents: the Memo of February 27, 2012 (“CRM One”), the Memo of July 5, 2012 (“CRM Two”), and an Electronic \*1024 Communication (“EC”), including the Memo of September 12, 2008, as an attachment thereto (“CRM Three”). *Id.* & Ex. 2. Part two of EOUSA's referral to the Criminal Division consisted of records maintained at USA Book, a DOJ intranet site (“CRM Four” and “CRM Five”). *Id.* EOUSA requested that the Criminal Division review the documents referred and directly respond to the Northern California ACLU (“ACLU–NC”). *Id.* ¶ 8. EOUSA further advised the Criminal Division that a response to ACLU–NC was required by March 23, 2013. *Id.*

The FOIA/PA Unit received EOUSA's referral and began processing the three memoranda and the sections of USABook that had been referred to it. *Id.* FOIA/PA Unit

personnel conducted a line by line review of the CRM One, CRM Two, CRM Three, and the sections of USA Book (CRM Four and CRM Five), to determine whether any FOIA exemptions were applicable to the information contained therein and, if so, whether any nonexempt information could be segregated and released to the requester. *Id.* ¶ 9.

Based on the FOIA/PA Unit's review, it determined that CRM One could be released in part, with 2 pages released in full, 2 pages released with certain redactions pursuant to FOIA Exemptions 5 and 7(E) <sup>1</sup>, and 53 pages withheld in full pursuant to FOIA Exemptions 5 and 7(E). *Id.* ¶ 10.

The FOIA/PA Unit determined that CRM Two could be released in part, with 1 page released with certain redactions pursuant to FOIA Exemptions 5 and 7(E), and 53 pages withheld in full pursuant to Exemptions 5 and 7(E). *Id.*

The FOIA/PA Unit concluded that one-hundred and sixteen pages of records comprising CRM Three, CRM Four, and CRM Five needed to be withheld in full pursuant to FOIA Exemptions 5, (b) 6, 7(C) and 7(E). *Id.* Finally, it determined that 304 pages of records are nonresponsive, because they relate to such matters as electronic surveillance, pen register, and trap and trace applications generally. *Id.*

On March 22, 2013, EOUSA and the Criminal Division separately released what they characterized as responsive, non-exempt records to Plaintiffs. Kornmeier Decl. ¶ 5 & Ex. B; First Cunningham Decl. ¶ 11 & Ex. 3. Specifically, EOUSA indicated that 41 pages were being released in full, and 18 pages were being withheld in full pursuant to FOIA Exemption 5. Kornmeier Decl. Ex. B.

By letter dated March 22, 2013, the Criminal Division notified Plaintiffs of the Criminal Division's disclosure determinations. First Cunningham Decl. ¶ 11 & Ex. 3. Specifically, it notified Plaintiffs that 2 pages were released in full, 3 pages were released in part, and 530 pages were withheld in full pursuant to FOIA exemptions 5, 6, 7(C), and 7(E). *Id.* ¶ 11 & Ex. 3. Concomitantly, it provided Plaintiffs with copies of the redacted CRM One and the redacted CRM Two. *Id.*

The parties have now filed motions for partial summary judgment with respect to the documents produced and withheld in response to Parts 2, 3, and 4 of Plaintiffs' FOIA request. Dkt. Nos. 23, 25. In their Motion, Plaintiffs assert that the DOJ has unlawfully withheld documents and challenge

its assertion of privileges as to the documents withheld. The Government, however, maintains that in processing Plaintiffs' FOIA request, the DOJ properly \*1025 withheld, in whole or in part, records except from disclosure under FOIA.

## LEGAL STANDARD

### A. The FOIA Statutory Scheme

[1] Congress enacted FOIA to “clos[e] the loopholes which allow agencies to deny legitimate information to the public.” *U.S. Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 150, 109 S.Ct. 2841, 106 L.Ed.2d 112 (1989) (citations and quotations omitted). The FOIA's “core purpose” is to inform citizens about “what their government is up to.” *Yonemoto v. Dep't of Veterans Affairs*, 686 F.3d 681, 687 (9th Cir.2012) (citing *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. at 775, 109 S.Ct. 1468 (citation omitted)). “Consistently with this purpose, as well as the plain language of the Act, the strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any requested documents.” *United States Dep't of State v. Ray*, 502 U.S. 164, 173, 112 S.Ct. 541, 116 L.Ed.2d 526 (1991).

### B. Summary Judgment Standard in FOIA Cases

[2] “Summary judgment is the procedural vehicle by which nearly all FOIA cases are resolved.” *Nat'l Res. Def. Council v. U.S. Dep't of Def.*, 388 F.Supp.2d 1086, 1094 (C.D.Cal.2005) (quoting *Mace v. EEOC*, 37 F.Supp.2d 1144, 1146 (E.D.Mo.1999)) (internal quotations omitted). The underlying facts and possible inferences are construed in favor of the FOIA requester. *Id.* at 1095 (citing *Weisberg v. U.S. Dep't of Justice*, 705 F.2d 1344, 1350 (D.C.Cir.1983)). Because the facts are rarely in dispute in a FOIA case, the Court need not ask whether there is a genuine issue of material fact. *Minier v. Cent. Intelligence Agency*, 88 F.3d 796, 800 (9th Cir.1996). The standard for summary judgment in a FOIA case generally requires a two-stage inquiry. See *Animal Legal Def. Fund. v. U.S. Food & Drug Admin.*, 2013 WL 4511936, at \*3 (N.D.Cal. Aug. 23, 2013).

[3] [4] To carry their burden on summary judgment, “agencies are typically required to submit an index and ‘detailed public affidavits’ that, together, ‘identify[ ] the documents withheld, the FOIA exemptions claimed, and a particularized explanation of why each document falls within the claimed exemption.’ ” *Yonemoto*, 686 F.3d at

688 (quoting *Lion Raisins v. Dep't of Agric.*, 354 F.3d 1072, 1082 (9th Cir.2004)) (modification in original). These submissions—commonly referred to as a *Vaughn* index—must be from “affiants [who] are knowledgeable about the information sought” and “detailed enough to allow court to make an independent assessment of the government's claim [of exemption].” *Id.* (citing *Lion Raisins*, 354 F.3d at 1079; 5 U.S.C. § 552(a)(4)(B)).

[5] Under the first step of the inquiry, the Court must determine whether the agency has met its burden of proving that it fully discharged its obligations under FOIA. *Zemansky v. EPA*, 767 F.2d 569, 571 (9th Cir.1985) (citing *Weisberg*, 705 F.2d at 1350–51). In the second stage of the inquiry, the Court examines whether the agency has proven that the information that it withheld falls within one of the nine FOIA exemptions. 5 U.S.C. § 552(a)(4)(B); *U.S. Dep't of State v. Ray*, 502 U.S. 164, 173, 112 S.Ct. 541, 116 L.Ed.2d 526 (1991) (“The burden remains with the agency when it seeks to justify the redaction of identifying information in a particular document as well as when it seeks to withhold an entire document.”); *Dobronski v. FCC*, 17 F.3d 275, 277 (9th Cir.1994).

[6] [7] The government may submit affidavits to satisfy its burden, but “the government \*1026 ‘may not rely upon conclusory and generalized allegations of exemptions.’ ” *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir.1995) (quoting *Church of Scientology v. Dep't of the Army*, 611 F.2d 738, 742 (9th Cir.1980)). The government's “affidavits must contain ‘reasonably detailed descriptions of the documents and allege facts sufficient to establish an exemption.’ ” *Id.* (quoting *Lewis v. IRS*, 823 F.2d 375, 378 (9th Cir.1987)).

[8] Courts “accord substantial weight to an agency's declarations regarding the application of a FOIA exemption.” *Shannahan v. I.R.S.*, 672 F.3d 1142, 1148 (9th Cir.2012) (citing *Hunt v. CIA*, 981 F.2d 1116, 1119–20 (9th Cir.1992)).

Here, the parties do not dispute that the DOJ has fully discharged its search obligations under FOIA, and the Government has submitted testimony from John Kornmeier from the Executive Office for United States Attorneys (“EOUSA”), and John Cunningham, a trial attorney in the FOIA/Privacy Act Unit of the Office of Enforcement Operations in the Criminal Division of the DOJ, attesting that the agencies conducted searches that were reasonably calculated to uncover all relevant documents. The issue in this case is whether the EOUSA properly withheld templates



and certain pages of a power point presentation as attorney work product under Exemption (b)(5), and whether the Criminal Division properly withheld memoranda and records maintained on a DOJ intranet site pursuant to Exemption 5, (attorney work product) and 7(E) (release would risk circumvention of the law). The Government argues that it has properly withheld the documents under these Exemptions, and that there are no non-segregable portions to release. Gov. Mot. at 4–13.

Plaintiffs' position is that the documents withheld by the DOJ are not exempt from disclosure. Pl. Mot. at 1. Plaintiffs first argue that the deliberative process privilege does not apply because the documents set forth the Government's policy on location tracking. Pl. Mot. at 4–11. Further, Exemption 5 does not apply because none of the documents are attorney work product, but rather set forth general legal standards and are conceptually indistinguishable from legal manuals and guidelines not entitled to work product protection. *Id.* at 11–15. Plaintiffs also contend that the materials withheld by the Criminal Division are not protected under Exemption 7(E), which permits the withholding of investigative techniques which would risk circumvention if disclosed, is inapplicable because the documents pertain to well-known technologies used to track individuals through cell phones and vehicles. *Id.* at 15–20.

## DISCUSSION

### A. Overview of FOIA and Exemptions

[9] FOIA's "core purpose" is to inform citizens about "what their government is up to." *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773, 775, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989) (citation omitted). This purpose is accomplished by "permit[ing] access to official information long shielded unnecessarily from public view and attempt[ing] to create a judicially enforceable public right to secure such information from possibly unwilling official hands." *EPA v. Mink*, 410 U.S. 73, 80, 93 S.Ct. 827, 35 L.Ed.2d 119 (1973). Such access will "ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152, 110 S.Ct. 471, 107 L.Ed.2d 462 (1989) (citation omitted).

[10] [11] [12] At the same time, FOIA contemplates that some information can legitimately \*1027 be kept

from the public through the invocation of nine exemptions to disclosure. See 5 U.S.C. § 552(b)(1)–(9). Use of the exemptions is within the agency's discretion, see *Chrysler Corp. v. Brown*, 441 U.S. 281, 293, 99 S.Ct. 1705, 60 L.Ed.2d 208 (1979); " 'exclusive,' " *Milner v. Dep't of Navy*, 562 U.S. 562, 131 S.Ct. 1259, 1262, 179 L.Ed.2d 268 (2011) (quoting *Mink*, 410 U.S. at 79, 93 S.Ct. 827) i.e., information not falling within the scope of an exemption must be disclosed; and " 'narrowly construed.' " *Id.* (quoting *FBI v. Abramson*, 456 U.S. 615, 630, 102 S.Ct. 2054, 72 L.Ed.2d 376 (1982)). "These limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 7–8, 121 S.Ct. 1060, 149 L.Ed.2d 87 (2001) (citation omitted). When an agency chooses to invoke an exemption to shield information from disclosure, it bears the burden of proving the applicability of the exemption. See *Reporters Comm.*, 489 U.S. at 755, 109 S.Ct. 1468. An agency may withhold only that information to which the exemption applies, and must provide all "reasonably segregable" portions of that record to the requester. 5 U.S.C. § 552(b)(9); see *Mead Data Cent., Inc. v. Dep't of Air Force*, 566 F.2d 242, 260 (D.C.Cir.1977).

### B. Deliberative Process Privilege

[13] [14] Federal courts have recognized an exception to Exemption 5 of FOIA for documents which constitute an agency's "secret law" or "working law." See *New York Times Co. v. Dep't of Justice*, 872 F.Supp.2d 309, 317 (S.D.N.Y.2012). Under this principle, "[i]f an agency's memorandum or other document has become its 'effective law and policy,' it will be subject to disclosure as the 'working law' of the agency...." *Brennan Ctr. for Justice at N.Y. Univ. Sch. of Law v. U.S. Dep't of Justice*, 697 F.3d 184, 199 (2d Cir.2012) (quoting *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 153, 95 S.Ct. 1504, 44 L.Ed.2d 29 (1975)). Documents may be properly characterized as working law when they resemble "final opinions, statements of policy and interpretations which have been adopted by the agency, and instructions to staff that affect a member of the public." *Id.* at 201 (internal quotation marks omitted).

[15] Plaintiffs argue that each of the documents the DOJ seeks to withhold constitutes the agency's working law on location tracking technology. Pl. Mot. at 9. Particularly, Plaintiffs maintain that all of the documents are instructions or guidelines issued by the U.S. Attorney and directed at his subordinates which express the settled and established policy of the U.S. Attorney's Office with respect to the legal

prerequisites for obtaining location tracking orders. Pl. Mot. at 9.<sup>2</sup> The Government, however, contends that Plaintiffs attempt to characterize the documents as working law is misplaced because the documents are not final decisions or policy **\*1028** statements: they discuss or otherwise reflect strategies, defenses, risks, and arguments that may arise in litigation. Gov. Reply at 2, Dkt. No. 33. The Government points out that “any final decisions or law with respect to the issues addressed in the documents will be generated in the course of the adjudicative process, not by an agency decision.” *Id.*

In *Jordan v. U.S. Dep't of Justice*, 591 F.2d 753 (D.C.Cir.1978), the D.C. Circuit rejected the DOJ's effort to withhold documents “relating to the exercise of prosecutorial discretion by the United States Attorney for the District of Columbia and his assistants” on Exemption 5 deliberative process and attorney work product grounds.<sup>3</sup> *Id.* at 755, 772. The court found the documents were “instructions or guidelines issued by the U.S. Attorney and directed at his subordinates” and thus “constitute[d] [the agency's] ‘effective policy.’ ” *Id.* at 774. These documents consisted of charging manuals which set forth “rules, and guidelines used by the Office of the United States Attorney for the District of Columbia in deciding whether to exercise prosecutorial discretion. *Id.* at 757.

[16] In contrast, the materials here provide legal strategy or guidelines for obtaining location tracking orders from a court, or discuss strategies, defenses, risks, and arguments that may arise in litigation. See Kornmeier Decl. Ex. C; First Cunningham Decl. ¶¶ 15, 16; Second Declaration of John E. Cunningham III (“Second Cunningham Decl.”) ¶ 19, Dkt. No. 33–1. They do not set forth the DOJ's policy on which members of the public prosecutors should target to obtain location tracking information. See *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 137–38, 95 S.Ct. 1504, 44 L.Ed.2d 29 (1975) (one of the purposes of FOIA is the avoidance of undisclosed written rules of decision for administrative action); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 869 (D.C.Cir.1980) (memoranda used “routinely” by DOE agency staff “as guidance in conducting their audits,” and “retained and referred to as precedent” in its dealings with the public constituted official agency policy). “[T]he secret law doctrine in FOIA cases generally arises in which agencies are *rendering decisions* based on non-public analyses.” (emphasis in original). *Families for Freedom v. U.S. Customs & Border Prot.*, 797 F.Supp.2d 375, 396 (S.D.N.Y.2011)

The Court agrees with the Government that both of the documents here do not represent final agency opinions or statements of policy and interpretations that have been adopted by the DOJ which have the “force and effect of law.” *Jordan*, 591 F.2d at 787. They involve legal issues that will ultimately be decided by the Court, not the DOJ. For instance, the 16–page template document (EOUSA No. 1), provides the format for AUSAs in the Northern District to use when filing applications for use of a pen register and trap and trace devices. The two slides withheld from the PowerPoint presentation (EOUSA No. 2) analyze legal issues that may arise in connection with the use of location tracking devices. Unlike the precedential effect of the DOE memoranda in *Coastal States*, 617 F.2d at 869, which interpreted **\*1029** the agency's own regulations and how to apply them while conducting audits, the DOJ's interpretation of recent case law affects only the strategies government lawyers will use to obtain permission from the court to use location tracking techniques by law enforcement officers in criminal prosecutions. See *Families for Freedom*, 797 F.Supp.2d at 396<sup>4</sup> (“[T]he secret law doctrine in FOIA cases generally arises in which agencies are *rendering decisions* based on non-public analyses.” (emphasis in original)).

[17] As to the Criminal Division documents, CRM One through Five discuss potential legal strategies, defenses, and arguments that might be considered by federal prosecutors. First Cunningham Decl. ¶¶ 15–16. They are not directives, not interpretations of any of the DOJ's regulations, and are not part of a body of law promulgated by the DOJ. Rather, they present arguments and litigating positions that federal prosecutors may pursue on a case-by-case basis. CRM One through CRM Five provide federal prosecutors with guidelines, recommendations and suggested best practices, not directives, to consider in litigating their cases. Second Cunningham Decl. ¶ 19. CRM One through CRM Five also do not require DOJ attorneys to make any particular arguments or follow any particular course of conduct. *Id.* ¶ 20. CRM One through CRM Five do not contain reasoning or conclusions that have been adopted as official DOJ policy or opinions and do not provide any official interpretation of DOJ's Fourth Amendment obligations. *Id.* ¶ 21.

For these reasons, the Court rejects Plaintiffs' argument that the documents at issue constitute the DOJ's working law. The Court therefore turns to the specific FOIA exemptions asserted.

### C. Exemption 5

[18] [19] Exemption 5 protects documents which “would not be available by law to a party ... in litigation with the agency.” 5 U.S.C. § 552(b)(5). This provision essentially grants an agency the same power to withhold documents as it would have in the civil discovery context. *NLRB*, 421 U.S. at 149, 95 S.Ct. 1504. To be withheld under attorney work-product, a document must have been prepared by an attorney or his or her agent in anticipation of litigation. *Delaney, Migdail & Young, Chartered v. I.R.S.*, 826 F.2d 124, 126 (D.C.Cir.1987). Attorney work-product protects documents prepared in anticipation of litigation, specifically memoranda, letters, and e-mails. Fed. R. Civ. P. 26(b)(3). The purpose of this protection is to “protect the attorney’s thought processes and legal recommendations from the prying eyes of his or her opponent.” *In re EchoStar Commc’ns Corp.*, 448 F.3d 1294, 1301 (Fed.Cir.2006); see also *Hickman v. Taylor*, 329 U.S. 495, 508, 67 S.Ct. 385, 91 L.Ed. 451 (1947). The phrase “in anticipation of litigation” extends beyond an attorney’s \*1030 preparation for a case in existing litigation, and includes “documents prepared in anticipation of foreseeable litigation, even if no specific claim is contemplated.” *Feshbach v. Sec. and Exch. Comm’n*, 5 F.Supp.2d 774, 782 (N.D.Cal.1997) (citing *Schiller v. NLRB*, 964 F.2d 1205, 1208 (D.C.Cir.1992)), *abrogated on other grounds* by *Milner*, 131 S.Ct. at 1259.

### D. Documents Withheld by the EOUSA

The Government asserts that the two sets of documents being withheld by EOUSA constitute protected work product that are exempt from disclosure pursuant to FOIA Exemption 5. Gov. Mot. at 6. Plaintiffs argue that the documents the DOJ seeks to withhold are not exempt work-product, but are neutral, objective analyses of the law and they do not analyze any particular matter. Pl. Mot. at 11.

#### 1. EOUSA Vaughn Index Document No. 1

[20] The Government’s *Vaughn* Index of EOUSA Records identifies document number 1 as being 16 pages in length and describes it as follows:

These 16 pages were created by the U.S. Attorney’s Office for the Northern District of California. The 16 pages are templates for an application and order for the use of a pen register and trap and trace device. The templates

incorporate the interpretation of the law by the U.S. Attorney’s Office and give advice on what information to include in particular situations. These templates represent the opinions of attorneys for the U.S. Attorney’s Office on the applicable law and are prepared to provide legal advice and in anticipation of litigation.

Kornmeier Decl., Ex. C, EOUSA *Vaughn* Index (“Index”), p. 1. The Index indicates that the templates are withheld in full pursuant to FOIA Exemption (b)(5) as Attorney Work Product and provides the following justification:

Exemption b(5) protects the U.S. Attorney’s Office legal opinions and recommendations for action under the attorney work product privilege. This document was prepared in anticipation of litigation involving the use of location tracking devices.

This information is attorney work product, which contains no nonexempt material. Therefore, there is nothing to segregate.

*Id.*

The Government argues that the template is work product because it was prepared in anticipation of litigation. Gov. Mot. at 6. Plaintiffs argue that the template does not qualify as attorney work product because it is not case-specific and merely sets forth general agency policies and instructions regarding how attorneys should apply for location tracking orders. Pl. Mot. at 12–13. (citing *Judicial Watch v. U.S. Dep’t of Homeland Sec.*, 926 F.Supp.2d 121, 143–44 (D.D.C.2013)). As in *Jordan*, Plaintiffs argue, these documents set forth “general standards to guide the Government lawyers” in applying for orders seeking location tracking information and do not contain “factual information, mental impressions,” or “legal theories” relating to any “particular” matter. Pl. Mot. 11–12 (citing *Jordan*, 591 F.2d at 775–76).

In *Jordan*, the D.C. Circuit rejected the DOJ’s effort to withhold documents “relating to the exercise of prosecutorial discretion by the United States Attorney for the District of Columbia and his assistants” on Exemption 5 deliberative process and attorney work product grounds. 591 F.2d at 755, 772. The court found the documents were “instructions or guidelines issued by the U.S. Attorney and directed at his subordinates” and thus “constitute[d] [the \*1031

agency's] 'effective policy.' ” *Id.* at 774. The *Jordan* court also found that the documents were not protected work product because they were “promulgated as general standards to guide the Government lawyers” in the exercise of prosecutorial discretion; they did not contain the type of “factual information, mental impressions” and “legal strategies relevant” to a “particular trial” or even “prepared in anticipation of trials in general.” *Id.* at 775–76.

In *Judicial Watch*, the court found that a memorandum that was authored to “convey agency policies and instructions regarding the exercise of prosecutorial discretion in civil immigration enforcement” was not protected work product because its purpose was to provide “general standards” to “instruct ICE staff attorneys in determining whether to exercise prosecutorial discretion in specific categories of cases.” 926 F.Supp.2d at 143. As in *Jordan*, the court found the documents were promulgated as “general standards” to instruct ICE staff attorneys in determining whether to exercise prosecutorial discretion in specific categories of cases. *Id.* at 142. The evident purpose of the memorandum was to convey agency policies and instructions regarding the exercise of prosecutorial discretion in civil immigration enforcement. *Id.* at 143. Thus, the court found that it “simply [did] not anticipate litigation in the way the work-product doctrine demands, as there [was] no indication that the document include[d] the mental impressions, conclusions, opinions, or legal theories of ... any ... agency attorney, relevant to any specific, ongoing or prospective case or cases.” *Id.* (citing *Am. Immigration Council v. U.S. Dep't of Homeland Sec.*, 905 F.Supp.2d 206, 221–23 (D.D.C.2012) (finding that PowerPoint slides that the Office of the Chief Counsel used to teach United States Citizenship and Immigration Services employees about interacting with private attorneys during proceedings before adjudicators did not merit work-product protection because the “lawyers prepared the slides to convey routine agency policies.”)).

In both *Jordan* and *Judicial Watch*, the purpose of the memorandum was “to convey agency policies and instructions,” not to provide legal theories or strategies for use in agency litigation. *Judicial Watch*, 926 F.Supp.2d at 143. Here, by contrast, the template does not provide legal theories or strategies for use in criminal litigation. Rather, they instruct government attorneys on how to apply for an order for location tracking information.

[21] Moreover, “[t]he work-product rule does not extend to every written document generated by an attorney.” *Coastal*

*States*, 617 F.2d at 864 (internal quotation marks, citation omitted). “The documents must at least have been prepared with a specific claim supported by concrete facts which would likely lead to litigation.” *Id.* at 865; see also *QST Energy, Inc. v. Mervyn's*, 2001 WL 777489, at \*5 (N.D.Cal. May 14, 2001) (“The protection applies ‘if the prospect of litigation is identifiable because of specific claims that have already arisen’ ”) (citation omitted); *Fox v. Cal. Sierra Fin. Servs.*, 120 F.R.D. 520, 525 (N.D.Cal.1988) (“in order for documents to qualify as attorney work-product, there must be an identifiable prospect of litigation (i.e., specific claims that have already arisen) at the time the documents were prepared”).

[22] “While it may be true that the prospect of future litigation touches virtually any object of a DOJ attorney's attention, if the agency were allowed ‘to withhold any document prepared by any person in the Government with a law degree simply because litigation might someday occur, the policies of the FOIA would be largely defeated.’ ” *Senate of Puerto Rico v. U.S. Dep't of Justice*, 823 F.2d 574, 586–87 (D.C.Cir.1987) (citation \*1032 omitted) (affidavits too conclusory to justify withholding as work product documents prepared in the course of investigation into homicide of political activists). As the D.C. Circuit held in *Jordan*, guidelines and manuals for U.S. Attorneys are not work product because they set forth “general standards to guide the Government lawyers.” 591 F.2d at 775. They are not “prepared in anticipation of a particular trial.” *Id.* Even though documents might be prepared “literally ‘in anticipation of litigation,’ ” “they do not anticipate litigation in the manner that the privilege requires” if they do not “ensu[e] from any ‘particular transaction.’ ” *Am. Immig. Council*, 905 F.Supp.2d at 222.

[23] The DOJ argues that the template falls within the privilege “even if no specific claim is contemplated.” Gov. Reply at 4. This assertion is correct in some contexts, but not the context of this case. Where government lawyers act “as legal advisors protecting their agency clients from the possibility of future litigation,” the work product privilege can apply to documents advising the agency as to potential legal challenges. *In re Sealed Case*, 146 F.3d 881, 885 (D.C.Cir.1998) (citing *Schiller*, 964 F.2d at 1208, and *Delaney, Migdail & Young*, 826 F.2d at 127). But when government lawyers are acting as “prosecutors or investigators of suspected wrongdoers,” the specific-claim test applies. *Id.* (citing *Coastal States*, 617 F.2d at 864–66, and *SafeCard Servs. Inc. v. SEC*, 926 F.2d 1197, 1202–



03 (D.C.Cir.1991)). Thus, *Schiller* and *Delaney* are “not in conflict” with cases requiring “a specific claim” to justify the privilege; they simply apply in “very different situations.” *Id.*

[24] Here, with respect to the template, the U.S. Attorneys are clearly acting as prosecutors, and not as attorneys advising an agency client on the agency's potential liability. As a result, the work product privilege only attaches to documents prepared “in the course of an active investigation focusing upon specific events and a specific possible violation by a specific party.” *Id.* (quoting *Safecard Serv. Inc.*, 926 F.2d at 1203); see also *Judicial Watch*, 926 F.Supp.2d at 139–142 (rejecting DHS' argument that *Schiller* extends work product extension to documents providing “guidance on how to handle specific classes of cases”).<sup>5</sup> The DOJ has failed to establish that the template pertains to a specific claim or consists of more than general instructions to its attorneys with regard to applying for location tracking orders. Accordingly, the template is not work product.

#### **\*1033 2. EOUSA Vaughn Index Document No. 2: Power Point Presentation**

[25] The Vaughn Index identifies document number 2 as being two pages in length and proffers the following description:

These two pages are the last part of a power point presentation by attorneys in the U.S. Attorney's Office for the Northern District of California of which the first part has been released to the ACLU. The two pages are a legal analysis of issues that may arise in connection with the use of location tracking devices. This analysis represents the opinions of attorneys for U.S. Attorneys Office on the interpretation of the law and was prepared to provide legal advice and in anticipation of litigation.

*Id.* The EOUSA asserts that the two pages are withheld in full pursuant to FOIA Exemption (b)(5) as Attorney Work Product, and provides the same justification as that offered for document no 1. Kornmeier Decl. ¶¶ 7–9. The Court agrees that these pages constitute the USAO's legal analysis of issues that may arise in connection with the use of location tracking devices. See, *id.* The withheld pages do not convey general agency policy regarding the use of location tracking

devices, nor do they provide instructions for how the DOJ desires its attorneys to apply for orders authorizing their use. See, *id.* Here, the legal strategies and issues addressed in the withheld documents are protected because they relate to foreseeable litigation arising out of the government's criminal investigations. The Index thus provides sufficient information from which the Court may conclude that the withheld pages are attorney work product. Accordingly, the attorney work product privilege applies to this document.

*Am. Immig. Council*, on which Plaintiffs rely, is distinguishable. There, the court held non-exempt a “legal opinion” addressing “whether an INS regulation create[d] a right to counsel for people seeking admission as refugees.” 905 F.Supp.2d at 222. The court found that the memo, as described in the Vaughn index, provided a “neutral, objective analysis of agency regulations.” *Id.* (citing *Delaney, Migdail & Young*, 826 F.2d at 127). The court distinguished this memo, which sought “the best interpretation of a regulation,” and was not entitled to work product protection, with one “considering whether a court is likely to uphold a proposed agency interpretation of a statute,” which was influenced by litigation. *Id.* (citing *In re Sealed Case*, 146 F.3d at 884). Here, the withheld portions of the power point presentation offer the DOJ's legal opinion on issues that may arise in connection with the use of location tracking devices in current litigation.

#### **E. Documents Withheld By the Criminal Division**

The Government asserts that the five sets of documents being withheld by the Criminal Division constitute protected work product that are exempt from disclosure pursuant to FOIA Exemption 5. Gov. Mot. at 13. Plaintiffs argue that none of these documents qualify as work product because: (1) the memoranda (CRM 1–3) provide neutral analysis of the implications of recent case law; and (2) the portions of the USA Book (CRM 4–5) function as an agency manual rather than provide case-specific litigation strategy. Pl. Mot. at 12–13. The Court will discuss each in turn.

##### **1. Criminal Division Vaughn Index Nos 1–3: CRM Memoranda**

[26] The Government's Vaughn Index of EOUSA Records identifies document number 1 (“CRM One”) as being pages 57 in length and describes it as follows: “Guidance Regarding the Application of \*1034 *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) to GPS Tracking.” Cunningham Decl., Ex. 2 (DOJ Vaughn Index).



The Index identifies document number 2 (“CRM Two”) as being 54 pages and describes it as follows: “Guidance Regarding the Application of *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) to Additional Investigative Techniques.” *Id.*

The Index identifies document number 3 (“CRM Three”) as a two-page memorandum, and describes it as follows: a final memorandum of law from DOJ–OEO to all USAO Criminal Chiefs re: “guidance concerning requests for historical cellular telephone location equipment.” *Id.*

“CRM One and CRM Two discuss potential legal strategies, defenses, and arguments that might be considered by federal prosecutors in light of the Supreme Court’s decision in *United States v. Jones*, — U.S. —, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (“*Jones*”).” Second Cunningham Decl. ¶ 8, Ex. 1. “CRM Three discusses potential legal strategies, defenses, and arguments that might be considered by federal prosecutors in light of a Western District of Pennsylvania decision entitled *In re Application*, 534 F.Supp.2d 585 (W.D.Pa.2008) (“*In re Application*”).” *Id.*

“CRM One, CRM Two and CRM Three are intended to outline possible arguments or litigation risks that prosecutors could encounter following the *Jones* and the *In re Application* decisions in the context of defendants’ motions to exclude or suppress evidence in cases involving GPS tracking devices, historical cellular telephone location information and other investigative techniques.” *Id.* “CRM One, CRM Two and CRM Three assess the strengths and weaknesses of alternative litigating positions and offer prosecutors guidance, recommendations and best practices going forward.” *Id.*

[27] Here, the DOJ properly withheld these memoranda as attorney work product. The Second Cunningham Declaration states that CRM One, Two, and Three “are intended to outline possible arguments and or litigation risks prosecutors could encounter” and “assess the strengths and weaknesses of alternative litigating positions.” Second Cunningham Decl. ¶ 8. Moreover, these documents were “prepared because of ongoing litigation and the prospect of future litigation.” *Id.* ¶ 9. Plaintiffs’ argument that the memoranda are not case-specific, and are thus “conceptually indistinguishable from the legal documents in *Jordan*, *Judicial Watch*, and *Am. Immig. Council* is unpersuasive. Pl. Reply at 11–12. There is no indication that these memoranda were intended to function as an agency manual, or that they offer neutral analysis of the law. Rather, they appear to be the “more pointed” documents

referred to by the *Delaney* court, which were prepared in anticipation of litigation. See *Delaney*, *Migdale & Young*, 826 F.2d at 127. The memoranda at issue here were created to assist AUSAs with recurring litigation issues related to the *Jones* and the *In re Application* decisions that have arisen in current litigation, and thus are protected as work product. See Kornmeier Decl. Ex. C; First Cunningham Decl. ¶¶ 15, 16; Second Cunningham Decl. ¶¶ 8–10. Where, as here, the purpose of the documents is to convey litigation strategy, rather than convey routine agency policy, they are entitled to work product protection. *Am. Immigration Council*, 905 F.Supp.2d at 221.

## 2. Criminal Division Vaughn Index Nos. 4–5: Portions of USA Book

[28] CRM Four and Five constitute relevant portions of the USABook, which functions as a legal resource book and reference guide for federal prosecutors. \*1035 See Cunningham Decl. ¶ 16. The Index identifies document number 4 (“CRM Four”) as portions of the USABook Manual titled “Electronic Surveillance and Tracking Devices,” and describes it as follows: “Provides guidance to federal prosecutors/case agents re: electronic surveillance and tracking devices. Text covers the following: Preface; Roadmap/FAQs; Part I—Obtaining Location Information from Wireless Carriers; Part II—Mobile Tracking Devices; Part III—Telematics Providers (OnStar, etc ...)” Cunningham Decl., Ex. 2 (DOJ Vaughn Index). CRM 4 also contains sample warrants, affidavits, and letters offering guidance on applications for authorization to obtain location data concerning the targeted wireless phone; two model sealed warrants. *Id.*

The Index identifies document number 5 (“CRM Five”) as portions of the USABook Federal Narcotics Manual titled “Electronic Surveillance Non–Wiretap,” and describes it as follows: “Provides guidance to federal prosecutors/case agents re: electronic surveillance and tracking devices. Text discusses electronic tracking devices generally and cellular telephone location information.” *Id.*

These documents present a more difficult question. After careful consideration of the Index and the parties’ arguments, the Court disagrees with the Government’s characterization of CRM Four and Five as work product. The DOJ asserts that CRM Four and Five “discusse[ ] potential legal strategies, defenses, and arguments that might be considered by federal prosecutors.” Gov. Reply at 5–6 (citing Cunningham Dec.

¶ 10). However, the general description of the materials as guidance, coupled with the templates for use in obtaining location tracking information or devices, strongly suggest that these documents function like an agency manual, providing instructions to prosecutors on how to obtain location tracking information. See Cunningham Decl. ¶ 16 (these documents function as a legal resource book and reference guide for federal prosecutors). For this reason, the Court does not find the DOJ's argument that these documents are litigation-specific to be persuasive, and thus does not agree that they function like the documents in *Delaney, Migdail & Young*, to advise the agency of the "legal vulnerabilities" or a particular program. 826 F.2d at 127.

#### F. Exemption 6 and 7(C)

[29] Exemption 6 concerns documents whose disclosure could result in the "unwarranted invasion of privacy." 5 U.S.C. § 552(b)(6). The Court is thus required "to protect, in the proper degree, the personal privacy of citizens against the uncontrolled release of information." *Lane v. Dep't of the Interior*, 523 F.3d 1128, 1137 (9th Cir.2008). Under this test, "the usual rule that the citizen need not offer a reason for requesting the information must be inapplicable." *Id.* (citing *Natl. Archives & Records Admin. v. Favish*, 541 U.S. 157, 172, 124 S.Ct. 1570, 158 L.Ed.2d 319 (2004)). Instead, the Court must "balance the public interest in disclosure against the [privacy] interest Congress intended the Exemption to protect." *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 776, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989); *Forest Servs. Emps. for Envtl. Ethics v. U.S. Forest Serv.*, 524 F.3d 1021, 1025 n. 2 (9th Cir.2008). Here, Exemptions 6 and 7(C) were applied to the names and identifying information of DOJ attorneys involved in the creation of CRM Three, CRM Four, and CRM Five. Gov. Mot. at 11. Plaintiffs do not oppose the application of these exemptions.

#### G. Exemption 7(E)

[30] Exemption 7 under FOIA permits the government to withhold "records or \*1036 information compiled for law enforcement purposes" under certain enumerated conditions. 5 U.S.C. § 552(b)(7). Particularly, Exemption 7(E) provides that "records or information compiled for law enforcement purposes" may be withheld if they "would disclose techniques and procedures for law enforcement investigations or prosecutions." *Id.* However, "Exemption 7(E) only exempts investigative techniques not generally known to the public." *Rosenfeld v. Dep't of Justice*, 57 F.3d

803, 815 (9th Cir.1995). The government may also withhold detailed information regarding a publicly known technique where the public disclosure did not provide "a technical analysis of the techniques and procedures used to conduct law enforcement investigations." See *Bowen v. U.S. Food & Drug Admin.*, 925 F.2d 1225, 1228–29 (9th Cir.1991); see also *Elec. Frontier Found. v. Dep't of Defense*, 2012 WL 4364532, at \*4 (N.D. Cal., Sep. 24, 2012).

[31] The Government asserts Exemption 7(E) for its investigative techniques and procedures, as well as guidelines for law enforcement investigations and prosecutions that are not publicly known. Cunningham Decl. ¶ 21–24. CRM One discusses how GPS tracking devices are used in federal criminal investigations, including "[t]he specific techniques available to prosecutors, the circumstances in which such techniques might be employed, and the legal considerations related to such techniques." *Id.* ¶ 21. CRM Two is similar to CRM One, except that it involves investigative techniques apart from GPS tracking devices. *Id.* ¶ 22. CRM Two "discloses techniques and procedures related to approximately a dozen investigative techniques apart from GPS tracking devices that are employed in federal criminal investigations." Second Cunningham Decl. ¶ 13. CRM Three discusses these same topics as they relate to historical cellular telephone location information. First Cunningham Decl. ¶ 23. Moreover, "[a]ll three memoranda discuss techniques and procedures that are not publicly known, and disclosure of this information could provide individuals with information that would allow them to violate the law while evading law enforcement." *Id.* ¶¶ 21–23.

The responsive portions of USABook contained in CRM Four and CRM Five address specific issues relating to electronic surveillance, tracking devices, and non-wiretap electronic surveillance in the context of prospective federal criminal prosecutions and investigations. *Id.* ¶ 24. "The specific techniques available to prosecutors, the circumstances in which such techniques might be employed, and the legal considerations related to such techniques are reflected through the documents." Second. Cunningham Decl. ¶ 15.

The Government asserts that these portions "are not publicly known, and disclosure of this information could provide individuals with information that would allow them to violate the law while evading law enforcement." *Id.* Specifically

If would-be wrongdoers have access to the information contained in CRM One through CRM Five regarding

where, when, how, and under what circumstances GPS tracking devices, historical cellular telephone location information, electronic surveillance, nonwiretap electronic surveillance and other investigative techniques are used by federal investigators, they will also learn when and where certain investigatory techniques are not employed, and would be able to conform their activities to times, places, and situations where they know that unlawful conduct will not be detected.

*Id.* ¶ 16

Plaintiffs argue that the DOJ has not met its burden of establishing that the \*1037 Criminal Division documents are covered under FOIA's Exemption 7(E) because they provide only a more specific application of techniques that are well known to the public. Opp'n at 17. Plaintiffs maintain that the Government's rationale for withholding the documents is also too conclusory, and should not be accorded much weight. *Id.* at 18.

With respect to CRM Four, this document discusses a number of techniques for tracking a person's location by cellular phone or vehicle. Plaintiffs point to the Government's *Vaughn* Index, which identifies the specific location tracking technologies discussed: "Obtaining Location Information from Wireless Carriers," "Mobile Tracking Devices," and "Telematics Providers (OnStar, etc.)." Cunningham Decl., Ex. 2. Plaintiffs contend that the Government's technique of obtaining location information from wireless carriers is already well known, including efforts to obtain location information of individual subscribers, as well as all subscribers who were close to one or more targeted cell towers ("cell tower dumps"). Pl. Mot. at 15–16. This is also evidenced by a number of news articles and judicial opinions addressing these techniques. Pl. Mot. at 16.

Plaintiffs next assert that CRM Five, which describes "electronic tracking devices—generally and cellular telephone information," also covers well-known techniques. *Id.* The Government's use of mobile tracking devices such as GPS and cell site simulators (also called "IMSI catchers," "digital analyzers," or "triggerfish") is well known to the public, and is discussed in the DOJ's own publicly available guides and manuals, as well as having been the

subject of extensive media coverage. *Id.* (citing "Electronic Surveillance Issues" (Lye Decl., Ex. 6, p. 151, 153, Dkt. No. 26); "Electronic Surveillance Manual" (Lye Decl., Ex. 7, p. 40; Lye Decl. ¶ 19; and Lye Decl. Ex. 10 (24 news articles about the Government's use of IMSI catchers)). Plaintiffs also note that the public is already well aware that the Government can obtain location information from telematics providers such as OnStar. Lye Decl. ¶ 18 and Ex. 9 (collecting news articles on Government access to telematics data such as OnStar).

The Government argues that the documents discuss "the specific techniques available to prosecutors," and "the circumstances in which such techniques might be employed." Cunningham Decl. ¶¶ 21, 23, 24. Plaintiffs contend that this argument is foreclosed by the Ninth Circuit's decision in *Rosenfeld*, which rejected the claim that a "more precise" application of a well-known technique falls under Exemption 7(E) simply because the more precise application \*1038 is not generally known. *Rosenfeld v. U.S. Dept. of Justice*, 57 F.3d 803, 815 (9th Cir.1995). Moreover, Plaintiffs argue, the DOJ has not met its burden by providing non-conclusory reasons establishing that disclosure of the documents would risk circumvention of the law. Pl. Mot. at 18 (citing *Am. Civil Liberties Union of N. Cal. v. FBI*, 2013 WL 3346845, \*9 (N.D.Cal. July 1, 2013)). Plaintiff points out that these are essentially memoranda discussing the legal standards governing the use of location tracking technology. *Id.* (citing *PHE, Inc. v. Dep't of Justice*, 983 F.2d 248, 251 (D.C.Cir.1993)). The Government counters that it may withhold detailed information regarding a publicly known technique where the public disclosure did not provide technical analysis of the techniques and procedures used to conduct law enforcement investigations. Gov. Reply at 11–12.

The Court finds inadequate the Government's assertion that, even though the techniques described in CRM Four and CRM Five are generally known, the specifics on how and when the technique is used is not generally known. The Government's attempt to distinguish *Rosenfeld* on the grounds that the non-public details regarding the circumstances in which the location tracking techniques are used is not merely a more precise application is not persuasive. Further, the Government's reliance on *Soghoian v. Dep't of Justice*, 885 F.Supp.2d 62, 75 (D.D.C.2012) is also not persuasive based on applicable Ninth Circuit authority. See *Rosenfeld*, 57 F.3d at 815 (holding the government cannot simply say that the investigative technique at issue "is not the practice, but the

application of the practice to the particular facts underlying that FOIA request” cannot be adequate under Exemption 7(E) because otherwise it would prove too much).

Here, the DOJ's declaration asserts that information about the specifics of when various investigatory techniques are used could alert law violators to the circumstances under which they are not used without addressing the fact that the public is already aware that minimizing vehicular or cell phone usage will allow them to evade detection. Second Cunningham Decl. ¶ 16. To the extent that potential law violators can evade detection by the government's location tracking technologies, that risk already exists. The documents at issue here are thus distinguishable from *Morley v. CIA*, 508 F.3d 1108, 1129 (D.C.Cir.2009), in which the court found that information pertaining to CIA security clearance procedures should be withheld under Exemption 7(E) because disclosure could render those procedures vulnerable and weaken their effectiveness at uncovering background information on potential candidates. There was no suggestion in *Morley* that information about how to evade CIA security clearance procedures was already available; disclosure in that case therefore gave rise to a risk of circumvention that did not pre-exist.

Recently, in *Am. Civil Liberties Union of N. Cal. v. FBI*, 2013 WL 3346845, at \* 9 (N.D.Cal. July 1, 2013), Judge Illston rejected the same argument advanced by the Government in a case where the FBI offered an affidavit that used similar conclusory language to support its entitlement to withhold documents pursuant to Exemption 7(E). There, in response to a FOIA request seeking information regarding the FBI's investigation of the Occupy movement, the FBI submitted a declaration stating that “[d]isclosure of this information could enable subjects to circumvent similar currently used techniques and procedures by law enforcement,” and explained that “[w]hile these techniques may be known by the public in a general sense, the technical analysis of these sensitive law enforcement techniques, to include the specifics of how and in what setting they are employed, is not generally known to the public.” *Id.*

Judge Ilston held that while the FBI is entitled to withhold technical analysis” of the techniques and procedures used to conduct law enforcement investigations that are not generally known, it cannot withhold investigatory procedures. *Id.* (citing *Bowen*, 925 F.2d at 1228). Similar to the declaration in this case, the court found the FBI's conclusory assertion that, “even though the technique is generally known, the specifics

on how and when the technique is used is not generally known,” to be inadequate. *Id.* (citing *Rosenfeld*, 57 F.3d at 815). The Court concluded that the FBI's assertion that “the public is unaware of the specifics of how and when a technique is employed is not enough to sustain a withholding under Exemption 7(E).” *Id.* The same is true in this case. The declarations here set forth only conclusory statements that the public is not aware of the specifics of how or when the techniques are used, but do not state that the techniques are not generally known to \*1039 the public See Second Cunningham Decl. ¶¶ 12–15.

For these reasons, the Court finds that the Government's assertion that the public is unaware of the specifics of how and when the techniques listed in CRM Four and CRM Five are employed is not enough to sustain a withholding under Exemption 7(E).

#### H. Segregability

FOIA requires that “[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.” 5 U.S.C. § 552(b).

Plaintiffs argue that FOIA does not permit agencies to withhold non-exempt portions of responsive records (although they may withhold non-responsive documents). At issue are portions of CRM Two, Four, and Five, withheld by the Criminal Division. (See Cunningham Decl. Ex. 2:23, 24 & 31.) The Ninth Circuit only permits withholding if documents, or portions thereof, fall within the enumerated exceptions. Pl. Mot. at 22 (citing *Church of Scientology v. Dep't of Army*, 611 F.2d 738, 741–42 (9th Cir.1979)). Plaintiffs further argue that *Dettmann v. U.S. Department of Justice* ) mandates that the DOJ not narrowly read the FOIA request so as to excise information to which Plaintiffs are entitled. 802 F.2d 1472 (D.C.Cir.1986).

The DOJ counters that it has produced all reasonably segregable documents responsive to the request. Specifically, it maintains that FOIA does not require disclosure of records in which the non-exempt information that remains is meaningless. Gov. Mot. at 13. (citing *Nat'l Sec. Archive Fund, Inc. v. CIA*, 402 F.Supp.2d 211, 220–21 (D.D.C.2005), in which the court concluded that no reasonably segregable information exists because “the non-exempt information would produce only incomplete, fragmented, unintelligible sentences composed of isolated, meaningless words.”) Moreover, segregability is not required if a document is



fully protected as work-product. Gov. Mot. at 13 (citing *Judicial Watch, Inc. v. Dep't of Justice*, 432 F.3d 366, 370–72 (D.C.Cir.2005)).

As discussed above, the DOJ properly withheld EOUSA No. Two and CRM Nos. One—Three. However, the DOJ must release EOUSA One, and CRM Four and Five in full, as they have not established that they are work product, or that redactions pursuant to Exemption 7(E) are warranted.

DENIED in part. The Government properly withheld EOUSA 2 and CRM 1–3 under Exemption 5. The Government must produce EOUSA 1 and CRM 4 and 5, as these documents were not properly withheld under Exemption 5 or 7(E). Plaintiffs' Cross-Motion for Partial Summary Judgment is GRANTED in part and DENIED in Part. Exemption 5 applies to EOUSA 2 and CRM 1–3. The Government did not meet its burden to establish that the remaining documents were properly withheld pursuant to Exemption 7(E).

**IT IS SO ORDERED.**

## CONCLUSION

For the foregoing reasons, the Government's Motion for Partial Summary Judgment is GRANTED in part and

## All Citations

70 F.Supp.3d 1018

## Footnotes

- 1 FOIA Exemption 5 covers “inter-agency or intra-agency memorandums or letters” protected by the deliberative process and attorney work product/attorney-client privileges. 5 U.S.C. § 552(b)(5). FOIA Exemption 7(E) exempts law enforcement techniques and procedures, disclosure of which “risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E).
- 2 Plaintiffs cite to *Jordan*, in which charging manuals that set forth “rules, and guidelines used by the Office of the United States Attorney for the District of Columbia in deciding (1) ‘which persons should be prosecuted for suspected violations of criminal laws in the District of Columbia, and/or the manner in which prosecutorial discretion will be exercised’, and (2) ‘which persons suspected of violations of criminal laws will be eligible for rehabilitation programs which divert such individuals from criminal prosecution’ ” were considered to be policy documents that were not exempt from disclosure. 591 F.2d at 757. In other words, these manuals set forth the agency’s policy on who would be prosecuted and who would be eligible for diversion. In contrast, the DOJ manuals here provide legal strategy or guidelines for obtaining location tracking orders from a court. They do not set forth the DOJ’s policy on who prosecutors should target for location tracking.
- 3 *Jordan* also held that the disputed documents were not exempt under Exemption 2, for “personnel rules and practices.” *Id.* at 763 (quoting 5 U.S.C. § 552(b)(2)). The D.C. Circuit subsequently rejected *Jordan’s* analysis of Exemption 2. See *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051, 1073 (D.C.Cir.1981) (finding exempt Bureau of Alcohol, Tobacco and Firearms training manual prescribing investigative techniques). But *Crooker* left undisturbed *Jordan’s* Exemption 5 analysis. Moreover, *Crooker* was subsequently abrogated by the Supreme Court’s decision in *Milner*, 562 U.S. 562, 131 S.Ct. 1259, 179 L.Ed.2d 268.
- 4 Plaintiffs’ attempt to distinguish this case with *Nat’l Council of La Raza v. Dep’t of Justice*, 411 F.3d 350 (2nd Cir.2005) is unavailing. There, a memo on the authority of state and local police to enforce immigration laws was being “used by the DOJ in its dealings with the public, as the sole legal authority for the agency’s claim that its new policy had a basis in the law.” *Id.* at 358. The DOJ repeatedly invoked the memo to “assure those outside of the agency that its policy was lawful and to encourage states and localities to take actions that the Department desired.” *Id.* The court found that the DOJ relied on the memo not only to justify what the DOJ, would do as a result of its deliberations, but also to justify what a third party—“state and local law enforcement”—should and could lawfully do. *Id.* It was this latter use of the memo by agency personnel that served as “powerful evidence that the Department explicitly adopted the OLC Memorandum as part of its policy.” *Id.* at 360.
- 5 The DOJ relies on a number of inapposite cases. *Feshbach v. SEC*, 5 F.Supp.2d 774, 782–83 (N.D.Cal.1997), is distinguishable. There, Judge Illston held that documents generated in the course of the SEC’s examination of a particular company were work product, even though at the time the documents were generated, the agency had not decided to litigate. The court’s work product conclusion rested on the fact that the documents were generated in the course of an investigation “based upon a suspicion of specific wrongdoing and represent[ed] an effort to obtain evidence and to build a case against the suspected wrongdoer.” *Id.* at 782. Similarly, *Heggstad v. United Dep’t of Justice*, 182 F.Supp.2d 1, 8 (D.D.C.2000), involved memos prepared by prosecutors about the decision to prosecute in particular criminal investigations. *Raytheon Aircraft Co. v. U.S. Army Corps of Eng’rs*, 183 F.Supp.2d 1280, 1289 (D.Kan.2001) is also



distinguishable as there, the court held that certain reports discussing the production, use and disposal of certain chemical compounds were created in anticipation of specific and pending litigation. The documents DOJ seeks to withhold, by contrast, set forth general legal standards, not an analysis of issues arising in “identified litigation” or strategic decisions regarding any particular investigation. *Id.*

---

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

AMERICAN CIVIL LIBERTIES UNION )  
OF NORTHERN CALIFORNIA, )

Plaintiff, )

v. )

DEPARTMENT OF JUSTICE, )

Defendant. )

No. 12-CV-4008-MEJ

STIPULATION OF PARTIAL  
DISMISSAL WITH PREJUDICE

This action arises under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, and pertains to a FOIA request that consists of four parts. *See* Compl. ¶ 21 (Dkt. No. 1). Part 1 of Plaintiff’s FOIA request sought “[a]ll requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008” (hereinafter, “Part 1”). *See id.* This case has proceeded on two tracks, with this Court entering an order on the parties’ cross-motions for summary judgment regarding Part 1 of Plaintiff’s FOIA request, *see* Dkt. No. 62 (09/30/2014), and a separate order on the parties’ cross-motions for summary judgment regarding Parts 2-4 of Plaintiff’s FOIA request, *see* Dkt. No. 61 (09/30/2014). The government has filed a Notice of Appeal of this Court’s Order regarding Parts 2-4 of Plaintiff’s FOIA request. *See* Notice of Appeal, Dkt. No. 66 (11/26/2014).

The parties have recently executed a Settlement Agreement that resolves all of Plaintiff’s claims regarding Part 1 of the FOIA request, as well as all of Plaintiff’s claims regarding attorney’s fees and costs in this litigation generally (regardless of the claims or proceedings to which those fees or costs may relate). Pursuant to that Settlement Agreement, defendant recently filed with the Court a declaration that discharges its obligation to process Part 1 of Plaintiff’s FOIA request. Accordingly, the parties hereby stipulate to the dismissal, with prejudice, of the following:

Stipulation of Partial Dismissal with Prejudice  
Case No. 12-CV-4008-MEJ

- All of Plaintiff's claims against defendant Department of Justice relating to Part 1 of Plaintiff's FOIA request.
- Any and all claims that Plaintiff may have for attorney's fees and costs in this litigation, regardless of the claims or proceedings to which those fees or costs may relate.

This stipulation of dismissal is not intended to, and does not, dismiss this entire action, as it does not affect the pending appeal to the United States Court of Appeals for the Ninth Circuit. That appeal, which relates to Parts 2-4 of the FOIA request, remains pending and is not dismissed herein.

WE ASK FOR THIS:

/s/Linda Lye  
LINDA LYE  
American Civil Liberties Union  
Foundation of Northern California  
39 Drumm Street  
San Francisco, CA 94111  
Telephone: (415) 621-2493  
Facsimile: (415) 255-8437  
E-mail: [llye@aclunc.org](mailto:llye@aclunc.org)

*Attorney for Plaintiff*

BENJAMIN C. MIZER  
Principal Deputy Assistant Attorney General  
Civil Division

ELIZABETH J. SHAPIRO  
Deputy Branch Director

/s/ Brad P. Rosenberg  
BRAD P. ROSENBERG (D.C. Bar No. 467513)  
Trial Attorney  
U.S. Department of Justice,  
Civil Division, Federal Programs Branch  
P.O. Box 883  
Washington, D.C. 20044  
Telephone: (202) 514-3374  
Facsimile: (202) 616-8460  
E-mail: [brad.rosenberg@usdoj.gov](mailto:brad.rosenberg@usdoj.gov)

*Attorneys for Defendant*

IT IS SO ORDERED that Plaintiff's claims regarding Part 1 of its FOIA request, as well as any and all claims for attorney's fees and costs in this litigation generally, shall be, and hereby are, DISMISSED WITH PREJUDICE.

MARIA-ELENA JAMES  
United States Magistrate Judge

Date

Stipulation of Partial Dismissal with Prejudice  
Case No. 12-CV-4008-MEJ

ATTESTATION PURSUANT TO LOCAL RULE 5-1(i)(3)

I, Linda Lye, hereby attest, in accordance with Local Rule 5-1(i)(3), that the concurrence in the filing of this document has been obtained from the other signatory listed here.

Dated: August 20, 2015

/s/ Linda Lye  
Linda Lye

**From:** Brown Lee, Erika (ODAG)  
**Subject:** Article re Cellphone Tracking Technology Lawsuit  
**To:** Axelrod, Matthew (ODAG); Ferber, Scott (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Jain, Samir (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG)  
**Cc:** Childs, Heather G. (ODAG)  
**Sent:** August 26, 2015 3:53 PM (UTC-04:00)

In case you aren't already aware, per the article below, DOJ will be releasing responsive documents related to requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008. The Department is continuing to litigate the release of documents related to policies cell-site simulators and other tracking technologies.

## CORRECTED: DOJ Cedes Cellphone Tracking Docs To ACLU

Share us on: By **Michael Macagnone**

Law360, Washington (August 25, 2015, 1:40 PM ET) -- The [U.S. Department of Justice](#) will provide a host of documents surrounding warrants and subpoenas for cellphone tracking efforts, to settle part of a Freedom of Information Act suit by the [American Civil Liberties Union](#), according to a recent California federal court filing.

Though the agency has appealed a decision requiring the disclosure of parts of a strategy handbook and denying summary judgment on providing hundreds of sealed records, the DOJ agreed Friday to provide summaries of warrant and subpoena applications to settle part of the suit brought by the ACLU of Northern California. The ACLU and the DOJ have been locked in a yearslong fight over the documents, which the government maintains could help bad actors escape detection and compromise investigations.

But, the ACLU has maintained there is a strong public interest in disclosing the use of cellphone location tracking methods, especially in light of police forces' greater use of them in the wake of the [U.S. Supreme Court](#)'s decision barring warrantless GPS tracking in *U.S. v. Jones*. The group filed its suit after not receiving responsive records from the DOJ to a 2012 FOIA request.

"Recent revelations have made clear that government agencies are engaged in seeking and acquiring the location information of individuals for tracking and surveillance purposes, utilizing varying technologies and varying legal standards that frequently fall short of constitutional protections designed to protect the public from intrusive government searches," the ACLU's 2012 complaint said.

Friday's settlement gives the ACLU access to summaries of applications for subpoenas, court orders and warrants from January 2008 onward, according to court records. Linda Lye, in-house counsel at the ACLU, said the documents they have obtained give a greater insight into the US attorney's office's use of statutory letters over search warrants when obtaining cellphone location data.

"It's unfortunate that we had to litigate to get it, but it is very important that we have finally obtained this information," Lye said.

But that does not end the matter, as both sides are currently fighting over other portions of the ACLU's FOIA request in the Ninth Circuit. After various motions on summary judgment over the course of two years, U.S. Magistrate Judge Maria-Elena James in September 2014 denied both sides' motions for summary judgment on specific investigation records that used location-tracking, but ordered the DOJ to continue searching for responsive records.

In addition, Judge James ordered the release of two documents related to location-tracking techniques from USABook, an internal guide for government attorneys, and said once the search was complete, she may be able to rule on further issues surrounding the disclosure of investigative records. The DOJ appealed in November, saying the release could frustrate law enforcement efforts nationwide.



Representatives for the ACLU and the DOJ could not be immediately reached for comment Wednesday.

The ACLU is represented in-house by Linda Lye and Michael Temple Risher.

The DOJ is represented in-house by Brad Prescott Rosenberg.

The case is American Civil Liberties Union of Northern California et al. v. Department of Justice, case number is [3:12-cv-04008](#), in the U.S. District Court for the Northern District of California.

The appeal is American Civil Liberties Union et al. v. Department of Justice, case number [14-17339](#), in the U.S. Court of Appeals for the Ninth Circuit.

--Editing by Edrienne Su.

-- Correction: A previous version of this story misidentified the substance of the documents disclosed to the ACLU. This error has since been corrected.

**From:** Axelrod, Matthew (ODAG)  
**Subject:** RE: Article re Cellphone Tracking Technology Lawsuit  
**To:** Brown Lee, Erika (ODAG); Ferber, Scott (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Jain, Samir (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG)  
**Cc:** Childs, Heather G. (ODAG)  
**Sent:** August 26, 2015 8:04 PM (UTC-04:00)

Great. Thanks, Erika.

---

**From:** Brown Lee, Erika (ODAG)  
**Sent:** Wednesday, August 26, 2015 7:48 PM  
**To:** Axelrod, Matthew (ODAG); Ferber, Scott (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Jain, Samir (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG)  
**Cc:** Childs, Heather G. (ODAG)  
**Subject:** RE: Article re Cellphone Tracking Technology Lawsuit

I agree that the process can be improved. As I understand, there is at least one other case involving current ACLU litigation against the Department for the release of cell-site simulator documents (order on cross-motions for summary judgment attached).

I have an upcoming call with Melanie Pustay, OIP Director, and can find out whether they are tracking the release of documents pursuant to FOIA litigation. Also on the CIV side, I'll check with Betsy Shapiro, who heads Fed Programs, on the status of FOIA cases involving DOJ technologies litigated by privacy/civil liberties advocates.

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:** Axelrod, Matthew (ODAG)  
**Sent:** Wednesday, August 26, 2015 4:02 PM  
**To:** Brown Lee, Erika (ODAG); Ferber, Scott (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Jain, Samir (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG)  
**Cc:** Childs, Heather G. (ODAG)  
**Subject:** RE: Article re Cellphone Tracking Technology Lawsuit

Thanks, Erika. How do we improve our internal communications process so that at least someone in ODAG gets a heads up before something like this gets publicly announced?

---

**From:** Brown Lee, Erika (ODAG)  
**Sent:** Wednesday, August 26, 2015 3:53 PM  
**To:** Axelrod, Matthew (ODAG); Ferber, Scott (ODAG); Lan, Iris (ODAG); Bonilla, Armando (ODAG); Jain, Samir (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG)  
**Cc:** Childs, Heather G. (ODAG)  
**Subject:** Article re Cellphone Tracking Technology Lawsuit

Duplicative Information - See Document ID 0.7.12327.5792

**From:** Lan, Iris (ODAG)  
**Subject:** From CRM weekly report  
**To:** Jain, Samir (ODAG); Brown Lee, Erika (ODAG); Gauhar, Tashina (ODAG)  
**Sent:** August 29, 2015 2:17 PM (UTC-04:00)

*Congressional Staff Briefing on Cell Phone Location Issues:* On September 3, Computer Crime and Intellectual Property Section (CCIPS) representatives will brief staff of Representative Jason Chaffetz (R-Utah), chair of the House Committee on Oversight and Government Reform, about techniques and legal processes used to obtain cell phone location information from providers, as well as an overview of the Department's forthcoming policy on law enforcement use of cell site simulators.



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

September 3, 2015

MEMORANDUM FOR HEADS OF LAW ENFORCEMENT COMPONENTS

ALL UNITED STATES ATTORNEYS

FROM:

Sally Quillian Yates   
Deputy Attorney General

SUBJECT:

Department Policy Regarding the  
Use of Cell-Site Simulator Technology

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

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

Attachment

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

---

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

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

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

### ***BACKGROUND***

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

#### ***Basic Uses***

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

---

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



### *How They Function*

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

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

### *What They Do and Do Not Obtain*

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

## **MANAGEMENT CONTROLS AND ACCOUNTABILITY<sup>2</sup>**

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

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

---

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

2. Within 30 days, agencies shall designate an executive-level point of contact at each division or district office responsible for the implementation of this policy, and for promoting compliance with its provisions, within his or her jurisdiction.
3. Prior to deployment of the technology, use of a cell-site simulator by the agency must be approved by an appropriate individual who has attained the grade of a first-level supervisor. Any emergency use of a cell-site simulator must be approved by an appropriate second-level supervisor. Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction, as described in paragraph 2 of this section, or by a branch or unit chief at the agency's headquarters.

Each agency shall identify training protocols. These protocols must include training on privacy and civil liberties developed in consultation with the Department's Chief Privacy and Civil Liberties Officer.

### ***LEGAL PROCESS AND COURT ORDERS***

The use of cell-site simulators is permitted only as authorized by law and policy. While the Department has, in the past, appropriately obtained authorization to use a cell-site simulator by seeking an order pursuant to the Pen Register Statute, as a matter of policy, law enforcement agencies must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure (or the applicable state equivalent), except as provided below.

As a practical matter, because prosecutors will need to seek authority pursuant to Rule 41 and the Pen Register Statute, prosecutors should, depending on the rules in their jurisdiction, either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. § 3123 (or the state equivalent), or (2) seek a warrant and a pen register order concurrently. The search warrant affidavit also must reflect the information noted in the immediately following section of this policy ("Applications for Use of Cell-Site Simulators").

There are two circumstances in which this policy does not require a warrant prior to the use of a cell-site simulator.

#### ***1. Exigent Circumstances under the Fourth Amendment***

Exigent circumstances can vitiate a Fourth Amendment warrant requirement, but cell-site simulators still require court approval in order to be lawfully deployed. An exigency that excuses the need to obtain a warrant may arise when the needs of law enforcement are so compelling that they render a warrantless search objectively reasonable. When an officer has the requisite probable cause, a variety of types of exigent circumstances may justify dispensing with a warrant. These include the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice.



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

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

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

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

---

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

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

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

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

### ***APPLICATIONS FOR USE OF CELL-SITE SIMULATORS***

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

1. Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. If investigators will use the equipment to determine unique identifiers at multiple locations and/or multiple times at the same location, the application should indicate this also.
2. An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.
3. An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative investigative use of any non-target data absent further order of the court, except to identify and distinguish the target device from other devices.

---

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

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



## ***DATA COLLECTION AND DISPOSAL***

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

1. When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.
2. When the equipment is used to identify an unknown cellular device, all data must be deleted as soon as the target cellular device is identified, and in any event no less than once every 30 days.
3. Prior to deploying equipment for another mission, the operator must verify that the equipment has been cleared of any previous operational data.

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

## ***STATE AND LOCAL PARTNERS***

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

## ***TRAINING AND COORDINATION, AND ONGOING MANAGEMENT***

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

---

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

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



responsibility of each agency with respect to the way the equipment is being used (*e.g.*, significant advances in technological capabilities, the kind of data collected, or the manner in which it is collected). We expect that agents will familiarize themselves with this policy and comply with all agency orders concerning the use of this technology.

Each division or district office shall report to its agency headquarters annual records reflecting the total number of times a cell-site simulator is deployed in the jurisdiction; the number of deployments at the request of other agencies, including State or Local law enforcement; and the number of times the technology is deployed in emergency circumstances.

Similarly, it is vital that all appropriate Department attorneys familiarize themselves with the contents of this policy, so that their court filings and disclosures are appropriate and consistent. Model materials will be provided to all United States Attorneys' Offices and litigating components, each of which shall conduct training for their attorneys.

\* \* \*

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. As with other capabilities, the Department must always use the technology in a manner that is consistent with the Constitution and all other legal authorities. This policy provides additional common principles designed to ensure that the Department continues to deploy cell-site simulators in an effective, appropriate, and consistent way.

**From:** (b)(6) per NSD (NSD)  
**Subject:** Fwd: [Chip] New department policy on Cell Site Simulators  
**To:** Brown Lee, Erika (ODAG); Harp, Jennifer C. (OPCL); Lane Scott, Kristi Z (OPCL)  
**Sent:** September 3, 2015 6:19 PM (UTC-04:00)  
**Attached:** ATT00001.htm, ATT00002.htm, DOJ Cell-Site Simulator Policy 9-3-15.pdf, ATT00003.htm

Begin forwarded message:

**From:** "Downing, Richard" <(b) (6)>  
**To:** "(b)(6) per CRM" <(b)(6) per CRM usdoj.gov>  
**Subject:** [Chip] New department policy on Cell Site Simulators

Dear CHIPs:

I wanted to let you know about a new policy released today that governs our use of Cell Site Simulators (a.k.a. "stingrays" or "triggerfish"). The policy was developed by a working group that included various components and investigative agencies.

The core of the new policy is to require search warrants for use of the devices, except in rare circumstances such as a threat to life and limb. It also requires transparency with the courts in the way that we apply for legal process, and it dictates what should be done with information about cell phones that are not related to an investigation.

Below is the press release, and the full policy is attached. Go-bys for legal process will be available on [CCIPS Online](#) shortly, and of course we're available to consult about application of the new policy.

Thanks,  
Richard.

---

RICHARD W. DOWNING  
Principal Deputy Chief  
Computer Crime and Intellectual Property Section  
United States Department of Justice  
(b) (6)

---

FOR IMMEDIATE RELEASE

DAG

THURSDAY, SEPTEMBER 3, 2015

(202) 514-2007

[WWW.JUSTICE.GOV](http://WWW.JUSTICE.GOV)

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 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.

-

# # #

**From:** Alexander W Joel  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven (b)(6) per DHS; frank.baitman@hhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrila, Jim (b)(6) per WHCO; Groman, Marc (b)(6) per WHCO  
**Cc:** Zarek, Corinna  
**Sent:** September 8, 2015 9:47 AM (UTC-04:00)

Hi Beverly –

Thanks for sharing the new DOJ policy, which in my view is excellent and which responds to the underlying concerns of civil society regarding such technology. I of course defer to DOJ and FBI on your question below. Just for ease of reference, I've pasted below what I think is the relevant "ask" from civil society's Model Action Plan:

(b)(5) per ODNI

(b)(5) per ODNI

---

**From:** Lumpkin, Beverley (OPA) [mailto:(b)(6)]  
**Sent:** Monday, September 07, 2015 3:54 PM  
**To:** Alexander W Joel (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C), (7)(E) per FBI; Erika Brown-Lee (b)(6); (b)(6) per NSD (NSD); (b)(6); Harp, Jennifer C. (OPCL) (b)(6); (b)(6), (7)(C), (7)(E) per FBI; Proia, Andrew (OPCL) (b)(6); Jonathan Cantor (b)(6) per DHS; Richards, Steven (b)(6) per DHS; frank.baitman@hhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrila, Jim (b)(6) per WHCO; Groman, Marc (b)(6) per WHCO  
**Cc:** Zarek, Corinna (b)(6) per WHCO  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Thanks, Alex. I will send back our proposed NAP-ready language for these submissions asap for your review.

In the meantime, I wanted to ask about DOJ's newly-announced policy for the use of cell-site simulators. It seems to me that this new policy addresses some of the issues raised by our friends in civil society. I know this issue falls on the cusp between privacy and surveillance, but I would love to have your team's response to whether we can (b)(5)



(b) (5)

Thanks much,  
Beverley

---

**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Sunday, September 06, 2015 3:10 PM  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven (b)(6) per DHS; frank.bairman@hhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrila, Jim (b)(6) per WHCO  
**Cc:** Zarek, Corinna  
**Subject:** ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

My apologies for submitting this very late. Please find attached submissions from ODNI for the NAP 3.0. They are as follows:

(b)(5) per ODNI

---

**From:** Lumpkin, Beverley (OPA) [mailto:(b) (6)]  
**Sent:** Monday, July 06, 2015 11:55 AM  
**To:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI) <(b)(6), (7)(C), (7)(E) per FBI>; Erika

Brown-Lee <(b) (6)>; (b)(6) per NSD (NSD) <(b) (6)>; Harp, Jennifer C. (OPCL)  
<(b) (6)>; (b)(6), (7)(C), (7)(E) per FBI; Proia, Andrew (OPCL) <(b) (6)>;  
Jonathan Cantor <(b)(6) per DHS>; Richards, Steven ((b)(6) per DHS )  
<(b)(6) per DHS>; [frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); Alexander W Joel (b)(3), (b)(6) per ODNI  
(b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO;  
Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel  
(b)(6) per WHCO; Martz, Stephanie  
(b)(6) per WHCO; Fonzone, Christopher  
(b)(6) per WHCO; Petrila, Jim  
(b)(6) per WHCO  
Cc: Zarek, Corinna <(b)(6) per WHCO>  
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5542

**From:** (b)(6) per NSD (NSD)  
**Subject:** FW: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap  
**To:** Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL); Brown Lee, Erika (ODAG)  
**Sent:** September 8, 2015 9:52 AM (UTC-04:00)

Hi – I was pinged by Beverley yesterday about this – are you interested in including something in the NAP? I think you were looped into the group who wrote the policy. I think it might be a good idea to include at this point, if possible. Happy to help.

---

**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Tuesday, September 08, 2015 9:47 AM  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven (b)(6) per DHS; frank.baitman@dhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrila, Jim (b)(6) per WHCO; Groman, Marc (b)(6) per WHCO  
**Cc:** Zarek, Corinna  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5921

**From:** Lumpkin, Beverley (OPA)  
**Subject:** Re: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap  
**To:** Alexander W Joel  
**Cc:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSL (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven (b)(6) per DHS; frank.baitman@hhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrla, Jim (b)(6) per WHCO; Groman, Marc (b)(6) per WHCO; Zarek, Corinna  
**Sent:** September 8, 2015 10:36 AM (UTC-04:00)

Thanks, Alex. I think your suggested additional language is an excellent idea. FYI to all, (b)(6) per NSD is checking with the law enforcement side of the house about adding this.

Sent from my iPhone

On Sep 8, 2015, at 9:48 AM, Alexander W Joel <(b)(3) per ODNI> wrote:

Duplicative Information - See Document ID 0.7.12327.5921

**From:** Zarek, Corinna  
**Subject:** Re: OGP/NAP 3.0: DRAFT section on Surveillance Transparency  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODN; (b)(3) per NSA; (b)(6), (7)(C) per FBI; (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI; (OGC) (FBI); Proia, Andrew (OPCL); (b)(6) per DHS; frank.baitman@hhs.gov; (b)(3), (b)(6) per ODN; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher; Petrla, Jim; Groman, Marc  
**Sent:** September 8, 2015 1:27 PM (UTC-04:00)

Thanks, Beverley!

Let me echo thanks and say I hope we can find ways to share the details with stakeholders when the time is right -- even if NAPs are high-level docs, we all know the backwork is intensive!

Thanks for championing this work and giving us something to proudly include!

Cori

---

**From:** Lumpkin, Beverley (OPA) [mailto:(b)(6)]  
**Sent:** Tuesday, September 08, 2015 10:50 PM  
**To:** Alexander W Joel (b)(3) per ODN; (b)(3) per NSA; (b)(3) per NSA; (b)(6), (7)(C) per FBI; (OGC) (FBI); (b)(6), (7)(C), (7)(E) per FBI; Brown Lee, Erika (ODAG); (b)(6); (b)(6) per NSD (NSD); (b)(6); Harp, Jennifer C. (OPCL); (b)(6); (b)(6), (7)(C) per FBI; (OGC) (FBI); (b)(6), (7)(C), (7)(E) per FBI; Proia, Andrew (OPCL); (b)(6); Jonathan Cantor (b)(6) per DHS; Richards, Steven; (b)(6) per DHS; frank.baitman@hhs.gov <frank.baitman@hhs.gov>; (b)(3), (b)(6) per ODN; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher; Petrla, Jim; Groman, Marc  
**Cc:** Zarek, Corinna  
**Subject:** OGP/NAP 3.0: DRAFT section on Surveillance Transparency

Hi Alex and team,

Thank you so much for your efforts in shaping these submissions for the National Action Plan. As we hope you will understand, we have had to shrink your submission into a more high-level, "NAP-like" language and in doing so have had to lose some of the details over which I know you have labored long & hard. But please take a look at the below, and let me know no later than COB Thursday 9/10 if there are any errors we may have inadvertently introduced in the process of winnowing down.

Thanks in advance, and again, I appreciate your cooperation very much!

Best,  
Beverley  
(b)(6)

(b)(5)

(b)(5) per ODN



- (b)(5) per ODNI [REDACTED]
- (b)(5) per ODNI [REDACTED]
- (b)(5) per ODNI [REDACTED]

---

**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Sunday, September 06, 2015 3:10 PM  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven (b)(6) per DHS; frank.bairman@hhs.gov; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO; Heinzelman, Kate (b)(6) per WHCO; Prieto, Daniel (b)(6) per WHCO; Martz, Stephanie (b)(6) per WHCO; Fonzone, Christopher (b)(6) per WHCO; Petrila, Jim (b)(6) per WHCO  
**Cc:** Zarek, Corinna  
**Subject:** ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5921

[REDACTED]

**From:** (b)(6) per NSD (NSD)  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap  
**To:** Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)  
**Sent:** September 8, 2015 4:17 PM (UTC-04:00)

Yes – on a call – will be off in 5

---

**From:** Brown Lee, Erika (ODAG)  
**Sent:** Tuesday, September 08, 2015 4:17 PM  
**To:** (b)(6) per NSD (NSD); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

(b)(6) per NSD – can you give me a call when you get a chance?

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)

---

**From:** (b)(6) per NSD (NSD)  
**Sent:** Tuesday, September 08, 2015 9:52 AM  
**To:** Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL); Brown Lee, Erika (ODAG)  
**Subject:** FW: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5922

**From:** Harp, Jennifer C. (OPCL)  
**Subject:** Re: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society  
**To:** Brown Lee, Erika (ODAG)  
**Cc:** Lane Scott, Kristi Z (OPCL); Proia, Andrew (OPCL)  
**Sent:** September 9, 2015 8:21 PM (UTC-04:00)

Sounds good. I'll start working on something Monday, but am free to chat earlier if need-be.

On Sep 8, 2015, at 3:47 PM, Brown Lee, Erika (ODAG) <(b) (6)> wrote:

Jenny – many thanks for spearheading our response. Attached are my comments on the UAS portion. Given the timing, our response should include the cell-site simulator policy. I'll send along comments on the transparency of federal privacy work tomorrow. I'm also available to chat further when you're back in the office.

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:** Harp, Jennifer C. (OPCL)  
**Sent:** Thursday, September 03, 2015 6:43 PM  
**To:** Brown Lee, Erika (ODAG)  
**Cc:** Lane Scott, Kristi Z (OPCL); Proia, Andrew (OPCL)  
**Subject:** FW: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Hi Erika,

I wanted to touch base with you regarding the NAP 3.0. Given the flux of work surrounding the OMB memo, I think we'd all like to get the NAP 3.0 out of the way. I have attached draft templates for the two commitments we discussed- privacy and UAS. Much of the language in the privacy template was taken from the NAP 2.0 commitment, as the 3.0 is simply a continuation of the 2.0 one. The language in the UAS template is original. Kristi has already approved these, but we have one question for you in the UAS one.

As Alex Joel mentioned below, Version 1.1 of the civil society recommendations contained several national security commitments that directly implicated DOJ. We told Beverley Lumpkin, (b)(6) per NSD, and (b)(6), (7)(C) per F that OPCL would be deferring to FBI and NSD on those additional recommendations, as they are largely outside our jurisdiction. We indicated that OPCL would only be submitting two discrete privacy and UAS-related commitments. Since July, (b)(6) per NSD has requested that we wait to submit any DOJ commitments until she and (b)(6), (7)(C) per F have coordinated over whether they will submit any. I know Beverley and Cori are

anxious for submissions, and (b) (5). Thus, once you clear our submissions, I recommend that we (b) (5)(b)(6) per NSD(b) (5)(b)(6), (7)(C) per F (b) (5)

Regarding Alex's points below- I assume we will (b) (5) (b) (5)

Happy to chat once you get a chance to review.

Best,  
Jenny

---

**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Tuesday, September 01, 2015 6:11 PM  
**To:** (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven ((b)(6) per DHS); Lane Scott, Kristi Z (OPCL); (b)(3) per NSA; (b) (6); (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(3) per NSA  
**Cc:** Jennifer L Hudson; (b)(3), (b)(6) per ODNI; Nathan L Mitchell; Michael Thomas; (b)(3), (b)(6) per ODNI; Eva Kleederman  
**Subject:** FW: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Greetings:

I'm sending this to a subset of the addresses below (+ (b) (6) and (b) (6)).

As a reminder, the WH has been running a process for the past few years called the Open Government Partnership. As part of that, the WH generates "national action plans for open government" and has published two so far – referred to as NAP 1.0 and 2.0 (NAP 2.0 is attached for reference). They are now working on NAP 3.0. They are looking for ambitious/achievable open government commitments. This process includes engagement with open government advocates, who submit their "wish list" of items (see attached "Model Action Plan"). Folks will recall that several of us met with the open government advocates, (b)(5) per ODNI

(b)(5) per ODNI

(b)(5) per ODNI

(b)(5) per ODNI

(b)(5) per ODNI

I will be submitting these to the WH later this week but wanted to first share this with you. Let me know if you'd like to discuss any of this. Thanks.

Regards,  
Alex

Alexander W. Joel  
ODNI Civil Liberties Protection Officer  
Civil Liberties and Privacy Office  
Office of the Director of National Intelligence  
(b)(3) per ODNI (main); (b)(3) per ODNI (second office)  
[www.dni.gov/clpo](http://www.dni.gov/clpo)

---

**From:** Lumpkin, Beverley (OPA) [[mailto:\(b\) \(6\)](#)]  
**Sent:** Monday, July 20, 2015 4:34 PM  
**To:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI)  
<(b)(6), (7)(C), (7)(E) per FBI>; Erika Brown-Lee <(b) (6)>; (b)(6) per NSD (NSD)  
<(b) (6)>; Harp, Jennifer C. (OPCL) <(b) (6)>; (b)(6), (7)(C) per FBI  
<(b)(6), (7)(C), (7)(E) per FBI>; Proia, Andrew (OPCL) <(b) (6)>; Jonathan Cantor  
<(b)(6) per DHS>; Richards, Steven <(b)(6) per DHS>  
<(b)(6) per DHS>; [frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); Alexander W Joel (b)(3), (b)(6) per ODNI  
(b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6) per WHCO  
; Heinzelman, Kate (b)(6) per WHCO  
; Prieto, Daniel (b)(6) per WHCO  
; Martz, Stephanie (b)(6) per WHCO  
; Fonzzone, Christopher (b)(6) per WHCO  
; Petrila, Jim (b)(6) per WHCO  
<(b)(6), (7)(C) per FBI (OGC) (FBI) <(b)(6), (7)(C), (7)(E) per FBI>  
**Cc:** Zarek, Corinna <(b)(6) per WHCO>  
**Subject:** RE: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Hi again,  
Thanks very much both to those who attended and those who wanted to attend our meeting today!  
Attached are the Model Action Plan version 1.1 from civil society, as well as the template on which we would like you to submit your upcoming fabulous ideas for the NAP 3.0, ideally by August 1<sup>st</sup>.

A number of you wanted to set up another meeting to discuss further various privacy issues. Please let me know who wants to be in such a meeting, and whether/when you may have upcoming NON-availability. Do we prefer an in-person meeting, or would a conference call suffice?

Thanks much,  
Beverley



---

**From:** Lumpkin, Beverley (OPA)

**Sent:** Thursday, July 16, 2015 11:09 AM

**To:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSL (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); (b)(6) per DHS; Richards, Steven ((b)(6) per DHS); [frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); Alexander W Joel (b)(3), (b)(6) per ODNI; Schwartz, Ari ((b)(6) per WHCO); Heinzelman, Kate ((b)(6) per WHCO); Prieto, Daniel ((b)(6) per WHCO); Martz, Stephanie ((b)(6) per WHCO); Fonzone, Christopher ((b)(6) per WHCO); Petrila, Jim ((b)(6) per WHCO); (b)(6), (7)(C) per FBI (OGC) (FBI)

**Cc:** Zarek, Corinna

**Subject:** RE: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Hi again,

Thanks so much to those who have gotten back to me about attending Monday's meeting. I am grateful for those who are able to attend, as I realize you all have busy schedules. I look forward to rsvp's from the rest of you by tomorrow!

Just to be sure you all have had the opportunity to thumb through the civil society wish-list, I am re-sending their "Model Action Plan." FYI the following representatives have said they will attend:

Liza Goitein, Brennan Center  
Jeramie Scott, EPIC  
Scott Roehm, Constitution Project  
Katherine Hawkins, OpenTheGovernment  
Rachel Levinson-Waldman, Brennan Center  
Rita Siemon, Constitution Project, if a conference line is available

<< File: Model Action Plan NAP Final June 9 2015.pdf >>

Thanks again for your continuing cooperation,  
Beverley

---

**From:** Lumpkin, Beverley (OPA)

**Sent:** Tuesday, July 14, 2015 2:57 PM

**To:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSL (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); (b)(6) per DHS; Richards, Steven ((b)(6) per DHS); [frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); Alexander W Joel (b)(3), (b)(6) per ODNI; Schwartz, Ari ((b)(6) per WHCO); Heinzelman, Kate ((b)(6) per WHCO); Prieto, Daniel ((b)(6) per WHCO); Martz, Stephanie ((b)(6) per WHCO); Fonzone, Christopher ((b)(6) per WHCO); 'Petrila, Jim ((b)(6) per WHCO); 'Gary, Arthur (JMD)'

**Cc:** Zarek, Corinna

**Subject:** OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Hello Privacy and Surveillance Experts!

As part of the preparation for the third Open Government National Action Plan, the Administration is

holding targeted consultations with civil society organizations on a variety of topics. We have scheduled a meeting to discuss privacy and surveillance issues on **Monday, July 20<sup>th</sup>, from 1pm-2pm**, at the National Archives building. The meeting will take place in the Adams Room on the 2<sup>nd</sup> floor of the National Archives Building located at 700 Pennsylvania Avenue, N.W., although you should use the Special Events entrance at the corner of 7<sup>th</sup> and Constitution Avenue. We hope you will plan to attend.

This meeting will follow the format of our regular consultations with civil society: The Open Gov team will open the meeting with some background and context of the Open Government Partnership and National Action Plan work, then we will ask the USG colleagues to start with updates on the work that you are doing. We will invite civil society to offer feedback and suggest priorities for future efforts and engage in a discussion around that.

As always, we will use Chatham House rules for these meetings (i.e., the fact of the meeting is not secret, but nothing said is to be attributed to any participants). You should feel free to engage in the discussion to the extent most appropriate for you – if you would prefer to treat this as more of a listening session, that is fine; if you wish to share your thoughts or seek feedback on possible new efforts, that is fine, too. You may also wish to flag for your leadership or communications teams that this meeting is taking place.

Please confirm that you will be able to join this meeting at your earliest opportunity. We will circulate a list of civil society attendees in advance of the meeting.

Thank you again for your continued work to advance these important open government priorities.

As always, please feel free to reach out to me with any questions or concerns. I look forward to seeing you in person next week!

Best,  
Beverley

Beverley Lumpkin  
Public Affairs  
Open Government Working Group  
US Department of Justice  
(b) (6)

<NAP 3 0 Submissions Template (UAS)(kls edits) (EBL Edits).docx>

**From:** (b)(6) per NSD (NSD)  
**Subject:** RE: OGP/NAP 3.0 -- Privacy & Surveillance Sections  
**To:** Harp, Jennifer C. (OPCL); Lumpkin, Beverley (OPA)  
**Cc:** Alexander W Joel (b)(3) per ODNI; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Lane Scott, Kristi Z (OPCL)  
**Sent:** September 10, 2015 7:11 PM (UTC-04:00)

+Kristi

---

**From:** Harp, Jennifer C. (OPCL)  
**Sent:** Thursday, September 10, 2015 6:58 PM  
**To:** Lumpkin, Beverley (OPA)  
**Cc:** Alexander W Joel (b)(3) per ODNI; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL)  
**Subject:** Re: OGP/NAP 3.0 -- Privacy & Surveillance Sections

Hi Beverley,

We have two submissions ready to go- one related to privacy transparency, one to UAS. I will start working on a cell site simulator one on Monday. Please feel free to touch base with me then.

Best,  
Jenny

On Sep 10, 2015, at 8:55 AM, Lumpkin, Beverley (OPA) <(b) (6)> wrote:

Hi,  
I wanted to check back in with DOJ/law enforcement POCs to see if anyone can suggest any way to take credit for the new policy on cell site stimulators in the NAP.  
Thanks for your thoughts!  
Best,  
Beverley  
(b) (6)

---

**From:** Lumpkin, Beverley (OPA)  
**Sent:** Tuesday, September 08, 2015 10:36 AM  
**To:** Alexander W Joel  
**Cc:** (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; Richards, Steven ((b)(6) per DHS); [frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); (b)(3), (b)(6) per ODNI; Schwartz, Ari ((b)(6) per WHCO); Heinzelman, Kate ((b)(6) per WHCO); Prieto, Daniel ((b)(6) per WHCO); Martz, Stephanie ((b)(6) per WHCO); Fonzone, Christopher ((b)(6) per WHCO); Petrla, Jim ((b)(6) per WHCO); Groman, Marc ((b)(6) per WHCO); Zarek, Corinna  
**Subject:** Re: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5929

**From:** Harp, Jennifer C. (OPCL)  
**Subject:** RE: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society  
**To:** Lane Scott, Kristi Z (OPCL)  
**Sent:** September 14, 2015 3:06 PM (UTC-04:00)

I'm free to chat whenever, so just call my cell when it's good for you.

---

**From:** Harp, Jennifer C. (OPCL)  
**Sent:** Monday, September 14, 2015 2:33 PM  
**To:** Lane Scott, Kristi Z (OPCL)  
**Subject:** Re: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Does 2:45 work for you?

On Sep 14, 2015, at 12:46 PM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

Hi Jenny,

Give me a call before sending a version to Erika. There have been a ton of conversations about this. I just want to fill you in. Let me know what time works for you. I hope you had a good time at (b) (6).

Thanks,

Kristi

---

**From:** Harp, Jennifer C. (OPCL)  
**Sent:** Monday, September 14, 2015 12:11 PM  
**To:** Brown Lee, Erika (ODAG)  
**Cc:** Lane Scott, Kristi Z (OPCL); Proia, Andrew (OPCL)  
**Subject:** RE: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Thanks, Erika. I'm working on incorporating cell site simulators into the UAS one. Will get you and Kristi something today. I've updated Beverley.

---

**From:** Brown Lee, Erika (ODAG)  
**Sent:** Monday, September 14, 2015 11:16 AM  
**To:** Harp, Jennifer C. (OPCL)  
**Cc:** Lane Scott, Kristi Z (OPCL); Proia, Andrew (OPCL)  
**Subject:** RE: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Hi Jenny – attached are my minor edits to the federal privacy submission.

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:** Harp, Jennifer C. (OPCL)

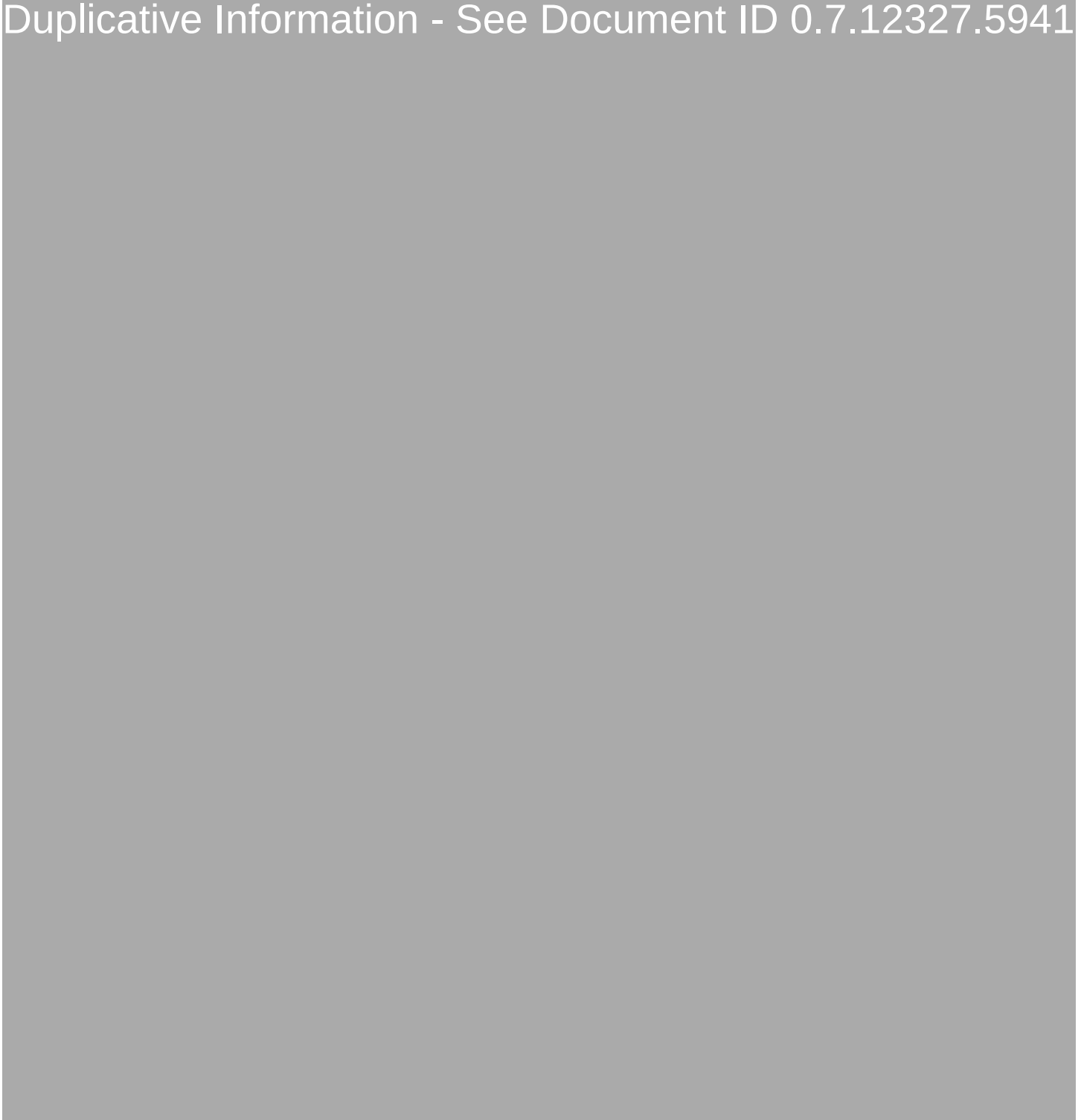
**Sent:** Thursday, September 03, 2015 6:43 PM

**To:** Brown Lee, Erika (ODAG)

**Cc:** Lane Scott, Kristi Z (OPCL); Proia, Andrew (OPCL)

**Subject:** FW: OGP // NAP 3.0 // Privacy and Surveillance Issues -- Meeting between Federal Experts and Civil Society

Duplicative Information - See Document ID 0.7.12327.5941





**From:** Alexander W Joel  
**Subject:** RE: OGP/NAP 3.0: DRAFT section on Surveillance Transparency  
**To:** Lumpkin, Beverley (OPA); Zarek, Corinna; (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSL (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; (b)(6) per DHS; 'frank.baitman@hhs.gov'; (b)(3), (b)(6) per ODNI; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher; Petrila, Jim; Groman, Marc  
**Sent:** September 17, 2015 6:48 PM (UTC-04:00)

Thanks for doing this and apologies for not replying sooner. Lots going on....

I think I would slightly edit as follows:

(b)(5) per ODNI

Regards,  
Alex



Alexander W. Joel  
ODNI Civil Liberties Protection Officer  
Civil Liberties and Privacy Office  
Office of the Director of National Intelligence  
(b)(3) per ODNI (main); (b)(3) per ODNI (second office)  
[www.dni.gov/clpo](http://www.dni.gov/clpo)

---

**From:** Lumpkin, Beverley (OPA) [mailto:(b)(6)]  
**Sent:** Monday, September 14, 2015 11:02 AM  
**To:** Zarek, Corinna <(b)(6) per OSTP>; Alexander W Joel <(b)(3) per ODNI>;  
(b)(3) per ODNI <(b)(3) per NSA>; (b)(6), (7)(C) per FBI (OGC) (FBI) <(b)(6), (7)(C), (7)(E) per FBI>; Erika  
Brown-Lee <(b)(6)>; (b)(6) per NSD (NSD) <(b)(6)>; Harp, Jennifer C. (OPCL)  
<(b)(6)>; (b)(6), (7)(C), (7)(E) per FBI; Proia, Andrew (OPCL) <(b)(6)>;  
Jonathan Cantor <(b)(6) per DHS>; (b)(6) per DHS  
'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; (b)(3), (b)(6) per ODNI  
<(b)(6) per WHCO>; Heinzelman, Kate <(b)(6) per WHCO>; Prieto, Daniel  
<(b)(6) per WHCO>; Martz, Stephanie <(b)(6) per WHCO>; Fonzone, Christopher  
<(b)(6) per WHCO>; Petrila, Jim <(b)(6) per WHCO>; Groman, Marc  
<(b)(6) per WHCO>  
**Subject:** RE: OGP/NAP 3.0: DRAFT section on Surveillance Transparency

Hi again team,

Please let me know if you have any issues with the below draft; otherwise, we will assume that all is well!

Thanks very much,  
Beverley

---

**From:** Zarek, Corinna [mailto:(b)(6) per OSTP]  
**Sent:** Tuesday, September 08, 2015 1:27 PM  
**To:** Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC)  
(FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); Proia,  
Andrew (OPCL); (b)(6) per DHS; (b)(6) per DHS; 'frank.baitman@hhs.gov';  
(b)(3), (b)(6) per ODNI; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher;  
Petrila, Jim; Groman, Marc  
**Subject:** Re: OGP/NAP 3.0: DRAFT section on Surveillance Transparency

Duplicative Information - See Document ID 0.7.12327.5932

**From:** Alexander W Joel  
**Subject:** FW: OGP/NAP 3.0: DRAFT section on Surveillance Transparency  
**To:** Rebecca J Richards (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); Erica R Bomsey; (b)(3), (b)(6) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Erica R Bomsey; Brown Lee, Erika (ODAG); (b)(6); (b)(3) per NSA; (b)(3), (b)(6) per ODNI; Jennifer L Hudson; (b)(3), (b)(6) per ODNI  
**Cc:**  
**Sent:** September 17, 2015 6:53 PM (UTC-04:00)

Again- sending the below to a subset (+(b) (6))....

Regards,  
Alex



Alexander W. Joel  
ODNI Civil Liberties Protection Officer  
Civil Liberties and Privacy Office  
Office of the Director of National Intelligence  
(b)(3) per ODNI (main); (b)(3) per ODNI (second office)  
[www.dni.gov/clpo](http://www.dni.gov/clpo)

---

**From:** Alexander W Joel  
**Sent:** Thursday, September 17, 2015 6:48 PM  
**To:** 'Lumpkin, Beverley (OPA)' <(b) (6)>; Zarek, Corinna <(b)(6) per OSTP>; (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI) <(b)(6), (7)(C), (7)(E) per FBI>; Erika Brown-Lee <(b) (6)>; (b)(6) per NSD (NSD) <(b) (6)>; Harp, Jennifer C. (OPCL) <(b) (6)>; (b)(6), (7)(C), (7)(E) per FBI; Proia, Andrew (OPCL) <(b) (6)>; Jonathan Cantor <(b)(6) per DHS>; (b)(6) per DHS; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; (b)(3), (b)(6) per ODNI; Schwartz, Ari <(b)(6) per WHCO>; Heinzelman, Kate <(b)(6) per WHCO>; Prieto, Daniel <(b)(6) per WHCO>; Martz, Stephanie <(b)(6) per WHCO>; Fonzone, Christopher <(b)(6) per WHCO>; Petrila, Jim <(b)(6) per WHCO>; Groman, Marc <(b)(6) per WHCO>  
**Subject:** RE: OGP/NAP 3.0: DRAFT section on Surveillance Transparency

Duplicative Information - See Document ID 0.7.12327.5953

**From:** Zarek, Corinna  
**Subject:** RE: OGP/NAP 3.0: DRAFT section on Surveillance Transparency  
**To:** Alexander W Joel; Lumpkin, Beverley (OPA); (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI; (OGC) (FBI); Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI; (OGC) (FBI); Proia, Andrew (OPCL); Jonathan Cantor; (b)(6) per DHS; 'frank.baitman@hhs.gov'; (b)(3), (b)(6) per ODNI; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher; Petrila, Jim; Groman, Marc  
**Sent:** September 18, 2015 11:13 AM (UTC-04:00)

Many thanks, Alex. Will take these edits into account. We plan to circulate a full draft NAP for informal comments first thing next week and will ask you all to take a close look at the full doc then.

Thanks!  
Cori

---

**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Thursday, September 17, 2015 6:48 PM  
**To:** 'Lumpkin, Beverley (OPA)'; Zarek, Corinna; (b)(3) per ODNI; (b)(3) per NSA; (b)(6), (7)(C) per FBI (OGC) (FBI); Erika Brown-Lee; (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI; Proia, Andrew (OPCL); Jonathan Cantor; (b)(6) per DHS; 'frank.baitman@hhs.gov'; (b)(3), (b)(6) per ODNI; Schwartz, Ari; Heinzelman, Kate; Prieto, Daniel; Martz, Stephanie; Fonzone, Christopher; Petrila, Jim; Groman, Marc  
**Subject:** RE: OGP/NAP 3.0: DRAFT section on Surveillance Transparency

Duplicative Information - See Document ID 0.7.12327.5953

**From:** Brown Lee, Erika (ODAG)  
**Subject:** RE: NAP 3.0 submissions  
**To:** Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)  
**Sent:** September 23, 2015 3:02 PM (UTC-04:00)

Hi Kristi – I think your response is on target; I would only add that going beyond your statement below and (b) (5) may raise privacy, legal, and investigative issues.

As Beverly is facilitating the process, she may be in a better position to advise on the persons with whom the submission has been shared.

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:** Wednesday, September 23, 2015 2:52 PM  
**To:** Brown Lee, Erika (ODAG); Harp, Jennifer C. (OPCL)  
**Subject:** FW: NAP 3.0 submissions

E/J,

Following a meeting with OLP to discuss (b) (5), we discussed (b) (5). Perhaps we can respond that (b) (5). This brings up a point that Jenny raised, which is: (b) (5)

With respect to Mark's involvement, I defer to Erika. I'm happy to discuss today. Maybe we can set up an internal DOJ call for tomorrow, before others begin responding to Cori. I'll standby for your responses.

Kristi

---

**From:** Zarek, Corinna [[mailto:\(b\)\(6\) per OSTP](#)]  
**Sent:** Wednesday, September 23, 2015 2:32 PM  
**To:** Lumpkin, Beverley (OPA); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL)  
**Cc:** Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Wood, Alexander W (OPCL); Proia, Andrew (OPCL); (b)(6), (b)(7)(C) (OGC) (FBI)  
**Subject:** RE: NAP 3.0 submissions

Hi everyone,

Thanks so much for this. Has this been shared with Marc Groman at OMB yet?



And one quick Q about the text:

(b) (5)

I know it may be too soon to know, but are we contemplating any sort of (b) (5) of the highlighted section?

Thanks!  
Cori

---

**From:** Lumpkin, Beverley (OPA) [mailto:(b) (6)]  
**Sent:** Monday, September 21, 2015 6:12 PM  
**To:** (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL)  
**Cc:** Zarek, Corinna; Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Wood, Alexander W (OPCL); Proia, Andrew (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI)  
**Subject:** RE: NAP 3.0 submissions

Thanks for the clarification, (b)(6) per NSD.

---

**From:** (b)(6) per NSD (NSD)  
**Sent:** Monday, September 21, 2015 6:01 PM  
**To:** Harp, Jennifer C. (OPCL)  
**Cc:** Zarek, Corinna; Lumpkin, Beverley (OPA); Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Wood, Alexander W (OPCL); Proia, Andrew (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI)  
**Subject:** Re: NAP 3.0 submissions

Thanks, Jennifer. NSD will not have something separate for this submission. To the extent that the intelligence community's proposal touches upon surveillance, we will provide assistance to them.

Regards, (b)(6) per NSD

On Sep 21, 2015, at 5:18 PM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

Cori and Beverley,

On behalf of Erika Brown Lee, I have attached DOJ OPCL's two submissions for the NAP 3.0 commitments. One is (b) (5), and one is (b) (5). As we have mentioned, FBI and NSD may or may not have their own submissions. It's our understanding, however, that they do not plan on submitting anything independently at this time.

Please let us know if you have any questions.

Best,

Jenny Harp  
Attorney Advisor

U.S. Department of Justice  
Office of Privacy and Civil Liberties  
National Place Building, Suite 1000  
1331 Pennsylvania Avenue NW  
Washington, DC 20530

(b) (6) (ph)  
(b) (6) (mobile)  
(202) 307-0693 (fax)

(b) (6)  
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.

<NAP 3 0 (Privacy).pdf>

<NAP 3 0 (Investigative Technologies).pdf>



# Department of Justice

---

**STATEMENT OF  
ELANA TYRANGIEL  
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL**

**BEFORE THE COMMITTEE ON THE JUDICIARY  
UNITED STATES SENATE**

**AT A HEARING ENTITLED  
“REFORMING THE ELECTRONIC  
COMMUNICATIONS PRIVACY ACT”**

**PRESENTED  
SEPTEMBER 16, 2015**

**Statement of  
Elana Tyrangiel  
Principal Deputy Assistant Attorney General**

**Before the  
Committee on the Judiciary  
United States Senate**

**At a Hearing Entitled  
“Reforming the Electronic Communications Privacy Act”**

**September 16, 2015**

Chairman Grassley, Ranking Member Leahy, and Members of the Committee, thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). This topic is particularly important to the Department because of the wide-ranging impact the statute has on public safety and both criminal and civil law enforcement operations. We are pleased to engage with the Committee in discussions about how ECPA is used and how it might be updated and improved.

ECPA includes the Pen Register Statute and the Stored Communications Act (SCA), as well as amendments to the Wiretap Act. These statutes are part of a set of laws that control the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. Although originally enacted in 1986, ECPA has been updated several times since, with significant revisions occurring in both 1994 and 2001.

I intend to focus the majority of my testimony on the SCA, which contains three primary components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications: anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates the government’s ability to compel disclosure of both stored content and non-content information from a service provider; it creates a set of rules that governmental entities generally must follow in order to compel disclosure of stored communications and other records.

Since its inception, the SCA has served multiple purposes. It provides rules governing how providers of communications services disclose stored information—including contents of communications, such as the body of an email, and non-content information—to a wide variety of government entities. In doing so, it imposes requirements on the government and providers to ensure that the privacy of individuals is protected. The statute thus seeks to ensure public safety

and other law enforcement imperatives, while at the same time ensuring individual privacy. It is important that efforts to amend the SCA remain focused on maintaining both of these goals.

## **I. The Stored Communications Act Plays an Important Role in Government Investigations**

Any consideration of the SCA must begin with an understanding of the statute's extremely broad scope. The paradigm that generally comes to mind in discussions of the SCA is a law enforcement agency conducting a criminal investigation and seeking a target's email from a service provider that makes its services available to the public. And, indeed, the SCA is critical to all sorts of criminal investigations into murder, kidnapping, organized crime, sexual abuse or exploitation of children, financial fraud, and more. As technology has advanced, electronic communications and electronic data storage have augmented traditional means of communicating and storing information. Appropriate governmental access to electronic communications and stored data, including both content and non-content information, has thus become even more important to upholding our law enforcement and national security responsibilities.

Even within these criminal investigations, it is important to understand the kind of information that the government obtains under the SCA as well as how that information is used. Under the SCA, the government may use legal process to compel service providers to produce both content and non-content information related to electronic communications. It is clear that the contents of a communication—for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography—can be important evidence in a criminal case. But non-content information can also be essential to building a case.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Non-content information about a communication may include, for example, information about the identity of the parties to the communication, and the time and duration of the communication. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without a mechanism to obtain non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant.

For example, the SCA has been critical to tracking down violent criminals. In one case, law enforcement obtained graphic photographs of a man sexually abusing his prepubescent son. Because of the offender's careful protection of his true identity, including the use of an anonymous online network, investigators needed to engage in a number of steps to ascertain the offender's location. Using information obtained from undercover chat sessions, officers identified a "proxy computer" – an intermediate computer used to obscure the offender's communication. Law



enforcement obtained computer routing information from the proxy computer, and from that routing information, identified an IP address from which the offender's internet traffic appeared to originate. After taking additional steps to confirm that the IP address was associated with the unlawful conduct, pursuant to ECPA agents served a subpoena on the offender's Internet service provider to obtain his physical address, leading to the eventual arrest of three individuals involved in the offense and the rescue of a minor victim from extreme, ongoing abuse.

Similarly, agents used evidence gathered using a process under ECPA in the investigation of the Boston Marathon bombing. Subpoenas to phone companies provided subscriber information and call detail records, which were critical during the investigation to help identify the bombers and their associates, and some of which were used at trial to show the communications between the bombers at critical times.

The SCA has broad effect in other ways as well. The statute applies not only to public and widely accessible service providers but also to non-public providers, such as companies or governments that provide email to their employees. Moreover, federal criminal investigations are only a subset of the circumstances in which the SCA applies. The statute applies to the federal government in civil contexts as well as to state and local governments when they seek to obtain content or non-content information from a service provider. This means that the statute also applies when the government is acting as a civil regulator—or even as an ordinary civil litigant. For instance, the SCA applies in all of the following circumstances that could arise, just within the Department of Justice:

- Civil Rights Enforcement: DOJ's Civil Rights Division brings a civil suit against a landlord who is sending racially harassing text messages to tenants. The target of the messages deletes them, and the landlord denies ownership of the account from which they were sent. The SCA governs the Division's ability to obtain those messages from the provider during civil discovery.
- False Claims Act: The DOJ Civil Division investigates a business for submitting false claims to the Federal government. The Division has reason to believe that the defendant's employees used email messages sent via the business's customer service email accounts to orchestrate the fraud. However, the defendant claims that it did not use email for business purposes. The SCA governs the ability of the Division to compel the internet service provider that hosted the company's website to disclose the contents of the business's email account.
- Environmental Litigation: The Department's Environment and Natural Resources Division brings a civil enforcement suit under the Superfund statute, a company relevant to the litigation has gone bankrupt, and the company's cloud provider has the only copies of that company's relevant corporate email. The SCA governs the Division's ability to obtain that email during civil discovery.

- Antitrust Investigations: The Department’s Antitrust Division is conducting a civil investigation of several companies for engaging in an unlawful agreement to restrain trade. During the course of the investigation, DOJ attorneys discover that executives of those companies are using their personal email accounts to continue communications about the agreement. The SCA governs the Division’s ability to obtain that email from the service provider.
- Tax Enforcement: The DOJ Tax Division investigates a tax preparation service that advertises via social networking sites. The company fraudulently inflates the amount of refunds due to the taxpayer and profits from taking a significant share of the fraudulent refund. Based on complaints about the preparer, the social networking site closes the company’s account. The SCA governs the Tax Division’s ability to obtain the posts advertising the company’s tax preparation services.

During any discussions of possible changes to the SCA and ECPA more broadly, it is important to keep in mind its wide-ranging application and scope.

## **II. Modernizing the Rules for Compelled Disclosure of Email and Other Similar Stored Content Information**

As I mentioned, ECPA was originally enacted in 1986—a time when the internet was still a nascent technology and landline telephones predominated. Although ECPA has been updated several times since its enactment, the statute—and specifically the portion of the SCA addressing law enforcement’s ability to use legal process to compel disclosure of the stored contents of communications from a service provider—has been criticized for making outdated distinctions and failing to keep up with changes in technology and the way people use it today.

Many have noted—and we agree—that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications. We agree, for example, that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old. Similarly, it makes sense that the statute not accord lesser protection to opened emails than it gives to emails that are unopened.

Acknowledging that the so-called “180-day rule” and other distinctions in the SCA no longer make sense is an important first step. The harder question is how to update those outdated rules and the statute in light of new and changing technologies while maintaining protections for privacy and adequately providing for public safety and other law enforcement imperatives.

Personal privacy is critically important to all Americans—including those of us who serve in the government. It is also of increasing importance to individuals around the world, many of whom use communications services provided by U.S. companies. All of us use email and other

technologies to share personal and private information, and we want it to be protected appropriately. We also know that companies in the United States and elsewhere depend on privacy as a driver of innovation and competitiveness. Some have suggested that the best way to enhance privacy under the SCA would be to require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider. We appreciate the appeal of this approach and believe that it has considerable merit, provided that Congress consider contingencies for certain, limited functions for which this may pose a problem.

In the past several years, we have worked to help facilitate a better understanding of how the warrant requirement affects the Department of Justice's ability to enforce the law. And the Department appreciates, for example, that most recent proposals (*i.e.*, the "ECPA Amendments Act" (S. 356)), would not impose a warrant requirement in investigations involving corporate email. This type of provision would help preserve the manner in which corporate investigations have historically been conducted. Corporations often act as "electronic communications service providers" under the SCA when they provide email and internet service to their employees. It would be anomalous, however, for the SCA to afford greater protection to electronic corporate records than to the identical records in hard copy, and such a rule could be abused by organizations and individuals seeking to avoid accountability for violating the law. Retaining the current use of subpoenas in that context therefore makes sense.

The Department remains concerned, however, about the effect a blanket warrant requirement would have on its civil operations. Civil regulators and litigators do extremely important work. But they typically are investigating conduct that, while unlawful, is not a crime. Criminal search warrants are only available if an investigator can show probable cause that a crime has occurred. Lacking warrant authority, civil investigators enforcing civil rights, environmental, antitrust, and a host of other laws would be left unable to obtain stored communications content from providers. As information is increasingly stored electronically, and as wrongdoers take new steps to shield that information from civil investigators, the amount of critical information off-limits to government regulators and litigators will only increase. It is also not the case that these civil regulators and litigators can ask criminal law enforcement officers to obtain a warrant on their behalf, because such warrants can only be obtained in furtherance of a criminal investigation—a step that would be impermissible unless the underlying conduct appeared to be criminal in nature.

Nor could civil litigators and regulators reliably obtain email and other content information solely by serving a subpoena directly on a subscriber (rather than a provider). As several of the examples described above demonstrate, serving a subpoena on a provider may be the only way for civil law enforcement to obtain certain stored communications. For example, where the subscriber no longer exists—as in the case of a bankrupt corporation or a deceased individual—or a purported subscriber denies ownership of the communications and therefore refuses to comply with a subpoena, civil litigators and investigators without the ability to obtain

relevant evidence from a provider would be unable to obtain that evidence. Moreover, many individuals who violate the law may be tempted to destroy their communications rather than turn them over. Having the ability to seek records only from the individual, rather than the provider, could serve to encourage such illegal obstruction of justice. Thus, it is important that any proposed changes to ECPA take into account the ability of civil regulators and litigators to ask a court to compel disclosure of information from providers.

The Department also has several more technical, yet important, concerns that we believe merit consideration, including ensuring that the definition of “remote computing service” is appropriately scoped.

Finally, given the increasing prevalence of electronic communications, critical investigations involving widespread or complex crimes – such as those involving terrorism, transnational crime, financial fraud, or child exploitation – can last years and involve hundreds of search warrants, court orders, and subpoenas issued pursuant to ECPA to a variety of providers. ECPA reform proposals should account for investigations of this type and avoid enacting new obstacles to investigations that are already among the most challenging and important ones that law enforcement undertakes.

Efforts to update ECPA can reflect these considerations and, at the same time, incorporate strong mechanisms that protect individual privacy and ensure appropriate judicial oversight of government access to individual’s communications.

### **III. The Need for Additional Updates to the SCA and ECPA**

Although discussions about updating ECPA have often focused on the standard for governmental access to stored content information, we also believe there are a number of other parts of the statute that merit further examination during any process of updating and clarifying the statute.

#### *(A) Clarifying Exceptions to the Pen Register Statute*

First, Congress could consider clarifying the exceptions to the Pen Register statute. The Pen Register statute governs the real-time collection of non-content “dialing, routing, addressing, or signaling information” associated with wire or electronic communications. This information includes phone numbers dialed as well as the “to” and “from” fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are actually less extensive than the exceptions to the Wiretap Act. This makes little sense—if the government is authorized to intercept communications in real-time, it is reasonable that the government should also be permitted to acquire the accompanying non-content information. Congress could harmonize the exceptions in these two sections of the statute by amending the Pen Register Act to bring it into line with the Wiretap Act. Moreover, the Pen Register Act’s consent provision may be read so that a user can only consent to the use of a pen/trap device by

the provider as opposed to by the government or the user herself. The Pen Register Act's consent provision could be clarified to allow the user to provide direct consent for implementation of a pen/trap device by the government.

*(B) Clarifying the Standard for Issuing 2703(d) Orders*

Second, Congress could consider clarifying the standard for the issuance of a court order under § 2703(d) of the SCA, which can be used by criminal law enforcement authorities to compel disclosure of various types of stored records. According to that provision of the statute, “[a] court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the [records] sought are relevant and material to an ongoing criminal investigation.”

The Fifth Circuit has interpreted this provision to require a court to issue a 2703(d) order when the government makes the “specific and articulable facts” showing specified by § 2703(d). *See In re Application of the United States*, 724 F.3d 600 (5th Cir. 2013). However, the Third Circuit has held that because the statute says that a § 2703(d) order “may” be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not.

*(C) Making the Standard for Non-content Records Technology-Neutral*

Third, Congress could consider modernizing the SCA so that the government can use the same legal process to compel disclosure of addressing information associated with modern communications, such as email addresses, as the government already uses to compel disclosure of telephone addressing information. Historically, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA endorsed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Therefore, while law enforcement can obtain records of calls made to and from a particular phone using a subpoena, the same officer can only obtain “to” and “from” addressing information associated with email using a court order or a warrant, both of which are only available in criminal investigations. This results in a different level of protection for the same kind of information (e.g., addressing information) depending on the particular technology (e.g., telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal and national security investigations. Congress could consider updating the SCA to set the same



standard for addressing information related to newer technologies as that which applies in traditional telephony.

*(D) Clarifying that Subscribers May Consent to Law Enforcement Access to Communications Content*

Fourth, Congress could consider clarifying the consent provision of the SCA. Under section 2702, a provider *may* disclose the contents of communications with the consent of a user or customer, but the provider is not required to do so. This has the impact of allowing the provider to overrule its customer's direction to disclose content associated with the customer's account. Thus when the victim of a crime seeks to share his or her own emails or other messages that may provide evidence, providers can refuse to disclose that information to law enforcement, even when provided with a written release from the account owner or subscriber.

*(E) Appellate Jurisdiction for Ex Parte Orders in Criminal Investigations*

Fifth, Congress could consider clarifying that higher courts have appellate jurisdiction over denials of warrants or other ex parte court orders in criminal investigations. Under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact. Congress may wish to consider clarifying that these denials are appealable so that the disagreements among courts are resolved and the law becomes standardized.

#### **IV. Obtaining Stored Information Abroad**

Some discussion concerning ECPA has focused on changing the standards and protocols for law enforcement access to content that a provider has chosen for its own business reasons to store outside the United States. The Administration is studying these legislative proposals, but the Department has significant concerns about aspects of these proposals.

\* \* \*

In conclusion, I would like to reemphasize that in discussing any efforts to modernize ECPA, it is important to take into account the statute's broad application. As technology continues to advance, ECPA's importance to both criminal and civil law enforcement will only increase.

The Department of Justice stands ready to work with the Committee as it considers potential changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.



**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

September 22, 2015

The Honorable Al Franken  
United States Senate  
Washington, D.C. 20510

Dear Senator Franken:

This responds to your letter to former Attorney General Eric H. Holder, Jr., dated November 18, 2014, concerning the use of cell-site simulator technologies. We apologize for our delay in responding.

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

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

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for

warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may be of additional assistance

Sincerely,

A handwritten signature in blue ink, appearing to read "P. J. Kadzik", is positioned above the printed name.

Peter J. Kadzik  
Assistant Attorney General

Enclosure





**U.S. Department of Justice**

Office of Legislative Affairs

---

Office of the Assistant Attorney General

*Washington, D.C. 20530*

September 22, 2015

The Honorable Edward J. Markey  
United States Senate  
Washington, D.C. 20510

Dear Senator Markey:

This responds to your letter to former Attorney General Eric H. Holder, Jr., dated November 14, 2014, concerning the use of cell-site simulator technologies. We apologize for our delay in responding.

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

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

While the Department has, in the past, obtained appropriate legal authorizations to use cell-site simulators, law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator. There are limited exceptions in the policy for exigent circumstances or exceptional circumstances where the law does not require a search

warrant and circumstances make obtaining a search warrant impracticable. Department divisions or district offices will be subject to a number of tracking requirements. To ensure that the use of the technology is well managed and consistent across the Department, the policy also requires appropriate supervision and approval.

To enhance privacy protections, the new policy establishes a set of required practices with respect to the treatment of information collected through the use of cell-site simulators. This includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily. Additionally, the policy makes clear that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations. This means data contained on the phone itself, such as emails, texts, contact lists and images, may not be collected using this technology.

We hope this information is helpful. Please do not hesitate to contact this office if we may be of additional assistance

Sincerely,



Peter J. Kadzik  
Assistant Attorney General

Enclosure



CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA  
DAVID VITTER, LOUISIANA  
DAVID A. PERDUE, GEORGIA  
THOM TILLIS, NORTH CAROLINA

PATRICK J. LEAHY, VERMONT  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KOLAN L. DAVIS, *Chief Counsel and Staff Director*  
KRISTINE J. LUCIUS, *Democratic Chief Counsel and Staff Director*

September 29, 2015

### VIA ELECTRONIC TRANSMISSION

The Honorable Jeh Johnson  
Secretary of the Department of Homeland Security  
U.S. Department of Homeland Security  
Washington, D.C. 20528

Dear Secretary Johnson:

Thank you for the responses you have previously provided to questions we have raised regarding the use of cell-site simulators (sometimes referred to as “IMSI Catchers” or “Stingrays”) by components of the Department of Homeland Security (DHS). These devices mimic cell towers, forcing cell phones in the area to convey their approximate location and registration information. While these devices can be useful tools for identifying the location of a suspect’s cell phone or identifying an unknown cell phone, they also present significant privacy concerns because they gather information about the cell phones of many people who are not investigative targets but happen to be in the vicinity.

We have previously expressed concerns about the privacy implications of these devices, as well as the inconsistent practices and policies across federal, state and local agencies that employ them. Earlier this month, the Department of Justice (DOJ) publicly issued new policy guidance governing the use of cell-site simulators by DOJ components. We are pleased that DOJ made this new guidance public; established uniform rules across its components; instituted a default warrant requirement for the use of these devices; required disclosure to reviewing courts about the way the technology works and its effect on non-target phones; and mandated deletion periods for data about non-target phones. While we remain concerned about some of the details, and in particular the potential scope of the largely undefined “exceptional circumstances” exception to the warrant requirement, we believe the DOJ guidance is a step in the right direction.

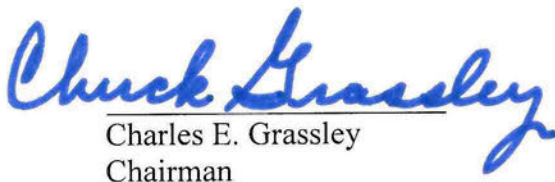
In light of reports that DHS also is working on a Department-wide policy to govern the use of cell-site simulators, we urge you to adopt a default warrant requirement, as DOJ did, but to avoid any ill-defined and potentially overbroad exceptions to that warrant requirement. We also remain concerned about the use of cell-site simulators by state and local agencies, which previously have been required to sign non-disclosure agreements when purchasing this equipment.

Accordingly, please provide responses to the following questions by no later than October 9, 2015:

1. What is the status of the DHS policy guidance review?
2. Will the Department-wide policy be public? If not, please explain why not.
3. Will the Department-wide policy establish uniform rules across its components? If not, please explain why not.
4. Will the Department-wide policy impose a default warrant requirement for the use of these devices and avoid any ill-defined and potentially overbroad exceptions? If not, please explain why not.
5. Will the Department-wide policy require the disclosure to reviewing courts about the way the technology works and its effect on non-target phones? If not, please explain why not.
6. Will the Department-wide policy mandate deletion periods for data about non-target phones? If not, please explain why not.
7. Does DHS loan cell-site simulators to state and local agencies, or provide federal grants that are used by state and local agencies to obtain cell-site simulators? If so, does DHS place any conditions on the use of those devices when purchased with federal money? If not, are there alternative methods by which DHS can incentivize state and local agencies to adopt the above-mentioned safeguards?

Also by October 9, 2015, please arrange for knowledgeable DHS officials to provide a briefing to Judiciary Committee staff that is responsive to these questions. We appreciate your assistance on this important matter.

Sincerely,

  
Charles E. Grassley  
Chairman

  
Patrick Leahy  
Ranking Member

cc: The Honorable Loretta Lynch  
Attorney General  
U.S. Department of Justice

**From:** Zarek, Corinna  
**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap  
**To:** Alexander W Joel  
**Cc:** (b)(3) per NSA; Rebecca J Richards (b)(3) per NSA; (b)(3), (b)(6) per ODNI; Brown Lee, Erika (ODAG); (b)(6) per NSD (NSD); Harp, Jennifer C. (OPCL); (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI)  
**Sent:** September 30, 2015 3:20 PM (UTC-04:00)

Thanks, Alex. I will let them know. This sounds like a good approach.

---

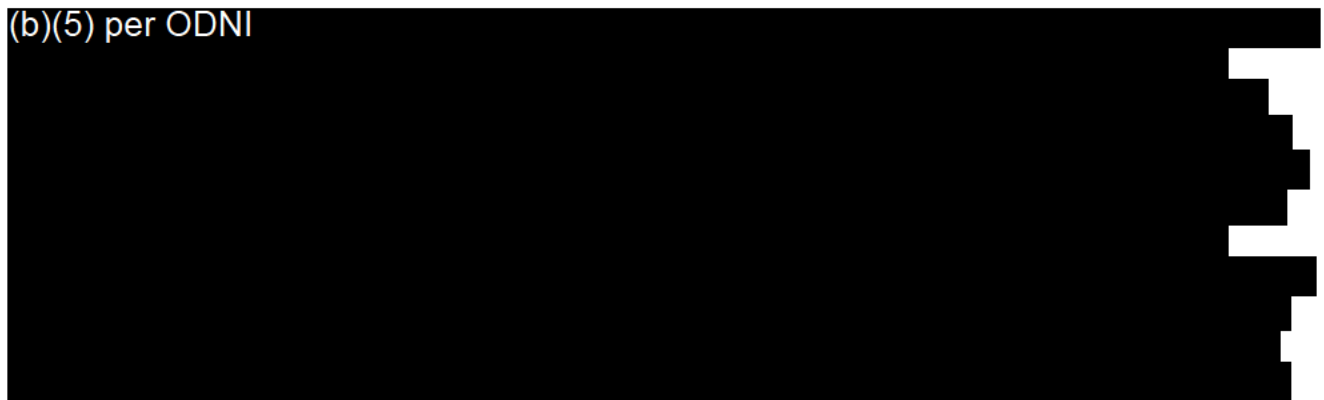
**From:** Alexander W Joel (b)(3) per ODNI  
**Sent:** Monday, September 28, 2015 2:56 PM  
**To:** Zarek, Corinna  
**Cc:** (b)(3) per NSA; Rebecca J Richards (b)(3) per NSA; (b)(3), (b)(6) per ODNI; Erika Brown-Lee; (b)(6) per NSD (b)(6); Harp, Jennifer C. (OPCL); (b)(6), (7)(C), (7)(E) per FBI  
**Subject:** FW: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Hi Cori

As I mentioned to you in a separate email, I'm resending this to you regarding your question about meeting again with civil society to talk about their surveillance requests in their Model Action Plan.

I addressed the Model Action Plan requests in my September 6<sup>th</sup> email below. I've pasted the relevant paragraph for ease of reference:

(b)(5) per ODNI



So, we'd like to address these issues in meetings, so we're all agreed on that part. However, given where we are in NAP 3.0 development, we don't think it's feasible to have the meetings and THEN, based on those meetings, to come up with a "commitment" that would go into NAP 3.0. Rather, we'd like to use the structured engagements outlined in the draft NAP to clarify their questions and then to see if we can provide answers. Here's what the time now says:

(b)(5) per ODNI



Regards,  
Alex



Alexander W. Joel  
ODNI Civil Liberties Protection Officer  
Civil Liberties and Privacy Office  
Office of the Director of National Intelligence  
(b)(3) per ODNI (main); (b)(3) per ODNI (second office)  
[www.dni.gov/clpo](http://www.dni.gov/clpo)

**From:** Alexander W Joel

**Sent:** Tuesday, September 08, 2015 9:47 AM

**To:** 'Lumpkin, Beverley (OPA)' <(b) (6)>; (b)(3) per ODNI ; (b)(3) per NSA, (b)(6), (7)(C) per FBI  
(OGC) (FBI) <(b)(6), (7)(C), (7)(E) per FBI>; Erika Brown-Lee <(b) (6)>; (b)(6) per NSD  
(NSD) <(b) (6)>; Harp, Jennifer C. (OPCL) <(b) (6)>; (b)(6), (7)(C), (7)(E) per  
>; Proia, Andrew (OPCL) <(b) (6)>; Jonathan Cantor  
<(b)(6) per DHS>; Richards, Steven (b)(6) per DHS ;  
[frank.baitman@hhs.gov](mailto:frank.baitman@hhs.gov); (b)(3), (b)(6) per ODNI ; Schwartz, Ari  
(b)(6) per WHCO ; Heinzelman, Kate  
(b)(6) per WHCO ; Prieto, Daniel  
(b)(6) per WHCO ; Martz, Stephanie  
(b)(6) per WHCO ; Fonzone, Christopher  
(b)(6) per WHCO ; Petrila, Jim  
(b)(6) per WHCO ; Groman, Marc (b)(6) per WHCO  
(b)(6) per WHCO

**Cc:** Zarek, Corinna <(b)(6) per WHCO>

**Subject:** RE: ODNI submissions --> RE: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5921