

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Stingray Briefing
To: Harp, Jennifer C. (OPCL)
Sent: January 2, 2015 9:10 PM (UTC-05:00)

Thanks Jenny!

From: Harp, Jennifer C. (OPCL)
Sent: Friday, January 02, 2015 5:31 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: FW: Stingray Briefing

Hey KLS,

Just FYI that I saw this article on Stingray in the IAPP daily roundup: [http://news.yahoo.com/senators-
seek-information-fbi-cell-tracking-201824506--politics.html](http://news.yahoo.com/senators-
seek-information-fbi-cell-tracking-201824506--politics.html). We may want to anticipate further involvement from Congress.

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, November 20, 2014 5:52 PM
To: (b)(6), (7)(C) per FBI (FBI)
Cc: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); (b)(6), (7)(C) per FBI (FBI); Harp, Jennifer C. (OPCL); Cardwell, Christine (ODAG)
Subject: Stingray Briefing

Hi (b)(6), (7)(C) per FBI

I'm following up on your discussion this week with Erika. She would like to schedule a briefing regarding FBI's use of stingray technology. I'll work with Erika's assistant, Christine Cardwell, on the scheduling. Please let me know if you have any questions.

Thanks!

Kristi Lane Scott
Deputy Director
Office of Privacy and Civil Liberties
U.S. Department of Justice
1331 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
202.307.0693 (fax)
(S) (b) (6)
(TS) (b) (6)

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

From: Lane Scott, Kristi Z (OPCL)
Subject: Re: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley
To: Harp, Jennifer C. (OPCL)
Cc: Chung, Joo (OPCL); Brown Lee, Erika (ODAG)
Sent: January 6, 2015 5:13 PM (UTC-05:00)

That's right Jenny. I'm sorry for the confusion. I'll ask FBI for a copy of their policy tomorrow.

Kristi Lane Scott
DOJ/OPCL

On Jan 6, 2015, at 4:35 PM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

In the last sentence of the letter, it looks like they want an in-person briefing by Feb. 6th, and written responses prior to that briefing.

From: Chung, Joo (OPCL)
Sent: Tuesday, January 06, 2015 4:29 PM
To: Lane Scott, Kristi Z (OPCL); Brown Lee, Erika (ODAG); Harp, Jennifer C. (OPCL)
Subject: RE: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

Kristi,

I may not be looking in the right place, but where is the 2/16 due date from? Also, can you get a copy of the new policy from FBI when you talk to them tomorrow?

Thanks for sending!

Joo

From: Lane Scott, Kristi Z (OPCL)
Sent: Tuesday, January 06, 2015 4:16 PM
To: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); Harp, Jennifer C. (OPCL)
Subject: Fwd: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

All,

Although we haven't received anything from OLA, we should expect to see QFR responses from FBI regarding Stingray. The responses are due to the Hill by 2/16. I'll talk to FBI tomorrow. The QFRs are below.

Kristi Lane Scott
DOJ/OPCL

Begin forwarded message:

From: Kristi Lane Scott <(b) (6)>
Date: January 6, 2015 at 4:12:27 PM EST
To: Kristi Z Lane Scott <(b) (6)>
Subject: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program Print Share

WASHINGTON – Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) and Ranking Member Chuck Grassley (R-Iowa) pressed top Obama administration officials on the use of cell-site simulators, which can unknowingly sweep up the cell phone signals of innocent Americans.

Recent news reports have chronicled the use of such simulators by law enforcement, explaining that the simulators have the potential to capture data about the location of thousands of cell phones in their vicinity. Leahy and Grassley previously pressed the FBI about the use of this technology. In a joint letter sent last week to Attorney General Eric Holder and Secretary of Homeland Security Jeh Johnson, the Senators raised questions about exceptions to a new FBI policy to obtain a search warrant before using a cell-site simulator. The Senators also asked about other agencies' use of the technology.

“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,” Leahy and Grassley wrote.

Outlining privacy concerns for innocent individuals, the letter continues: “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.”

A copy of the text of the December 23 letter to Attorney General Holder and Secretary Johnson can be found below.

December 23, 2014

The Honorable Eric H. Holder, Jr.
Johnson
Attorney General
Security

The Honorable Jeh
Secretary of Homeland

Department of Justice
Homeland Security
950 Pennsylvania Avenue, N.W.
20528
Washington, D.C. 20530

Department of
Washington, D.C.

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 14, 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 a 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.

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*

January 22, 2015

VIA ELECTRONIC TRANSMISSION

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

Dear Attorney General Holder:

According to a recent USA Today article, the Federal Bureau of Investigation, the U.S. Marshals Service, and dozens of other law enforcement agencies have access to radar technology that can precisely detect movement inside buildings.¹ We appreciate the potential law enforcement value of these devices. However, technology that can essentially look inside peoples' homes presents privacy concerns of the highest order. There has been little to no public discussion of this technology and it is unclear whether agencies are obtaining any legal process — let alone a warrant — prior to deploying it.

Privacy of the home is at the core of the Fourth Amendment. More than a decade ago, the U.S. Supreme Court decided that the use without a warrant of thermal imaging equipment that could detect activity inside a home violated the Fourth Amendment.² Similarly, in 2013, the Court found a Fourth Amendment violation when police brought a drug-sniffing dog onto an individual's front porch without a warrant.³ Unsurprisingly, the U.S. Court of Appeals for the Tenth Circuit recently noted the "obvious" and "grave" Fourth Amendment concerns associated with the use of the radar technology that is the subject of this letter.⁴

On December 23, 2014, we raised similar concerns in a letter to you about the use of cell-site simulators (sometimes referred to as "Stingrays" or "dirtboxes"), which can collect data from large numbers of cell phones in their vicinity — including phones in private homes. This pattern of revelations raises questions about whether the Justice Department is doing enough to ensure that — prior to these technologies' first use — law enforcement officials address their privacy implications, seek appropriate legal process, and fully inform the courts and Congress

¹ Brad Heath, "New police radars can 'see' inside homes," *USA Today*, January 20, 2015, <http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/>.

² *Kyllo v. United States*, 533 U.S. 27 (2001).

³ *Florida v. Jardines*, 133 S.Ct. 1409 (2013).

⁴ *United States v. Denson*, 2014 WL 7380656 (10th Cir. 2014).

about how they work. There is also a question as to how many other new technologies are being used by law enforcement agencies that raise similar privacy concerns.

Accordingly, please arrange for knowledgeable officials to provide a briefing to Judiciary Committee staff no later than February 13, 2015. Should you have any questions, please contact Jay Lim at (b) (6) or Lara Flint at (b) (6). Thank you.

Sincerely,


Charles E. Grassley
Chairman


Patrick Leahy
Ranking Member

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.

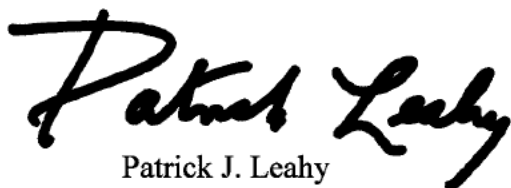
Accordingly, please provide written responses to these questions by January 30, 2015:

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

From: Chung, Joo (OPCL)
Subject: RE: USMS cell site / radar pre-brief
To: Brown Lee, Erika (ODAG)
Sent: February 10, 2015 12:09 PM (UTC-05:00)

At this point, I think we are all too pressed so sadly can't join.

From: Brown Lee, Erika (ODAG)
Sent: Tuesday, February 10, 2015 12:00 PM
To: Chung, Joo (OPCL)
Subject: USMS cell site / radar pre-brief
Importance: High

Just received this invite. Not sure if anyone can OPCL can attend. I plan to stop by.

-----Original Appointment-----

From: Wade Tyson, Jill C (OLA)
Sent: Tuesday, February 10, 2015 11:31 AM
To: Wade Tyson, Jill C (OLA); OBrien, Paul; Bonilla, Armando (ODAG); Tyrangiel, Elana (OLP); Brown Lee, Erika (ODAG); Wainscott, Kip (OLP); Driscoll, Derrick (USMS); (b)(6), (7)(C), (7)(F) per USMS (USMS); Rodenbush, Patrick (OPA); Lynch, Michael K. (JMD)
Subject: USMS cell site / radar pre-brief
When: Tuesday, February 10, 2015 1:00 PM-2:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: OLA Small Conference Room (1605, next to AAG Ofc)

I hear there was a calendar glitch so I am re-sending this invite. Sorry for any confusion.

Briefing will be for Grassley and Leahy National Security and Oversight Counsels to discuss USMS air and other technologies. We will do a "soft moot" during the prep session in OLA . Thank you.

<<2014-12-23 PJI and CEG to DOJ and DHS (cell-site simulators).pdf>> <<2015-01-22 CEG and PJI to DOJ (Radar Technology).pdf>>
<< File: 2014-12-23 PJI and CEG to DOJ and DHS (cell-site simulators).pdf >> << File: 2015-01-22 CEG and PJI to DOJ (Radar Technology).pdf >>

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: Brown Lee, Erika (ODAG)
Subject: RE: lawsuit on USMS use of cell site simulators
To: Bonilla, Armando (ODAG)
Sent: February 10, 2015 5:33 PM (UTC-05:00)

Many thanks, Armando. And thanks again for looping me in to the briefings.

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: Bonilla, Armando (ODAG)
Sent: Tuesday, February 10, 2015 5:16 PM
To: Brown Lee, Erika (ODAG)
Subject: Fwd: lawsuit on USMS use of cell site simulators

FYSA.

Begin forwarded message:

From: "Wade Tyson, Jill C (OLA)" <(b) (6)>
Date: February 10, 2015 at 5:14:18 PM EST
To: "Rodenbush, Patrick (OPA)" <(b) (6)>, "Bonilla, Armando (ODAG)" <(b) (6)>, "Gaston, Molly (OAG)" <(b) (6)>, "Tyrangiel, Elana (OLP)" <(b) (6)>, "Wainscott, Kip (OLP)" <(b) (6)>, "OBrien, Paul" <(b) (6)>
Subject: Re: lawsuit on USMS use of cell site simulators

Didn't see that one coming on the eve of our SJC briefing tomorrow. Adding OLP and Paul O'Brien.

Agree no comment.

-JCT

From: Rodenbush, Patrick (OPA)
Sent: Tuesday, February 10, 2015 05:12 PM Eastern Standard Time
To: Wade Tyson, Jill C (OLA); Bonilla, Armando (ODAG); Gaston, Molly (OAG)
Subject: lawsuit on USMS use of cell site simulators

The Electronic Frontier Foundation sued DOJ today over the alleged use of cell site simulators on airplanes. I'm assuming we won't comment on this, but also want to make you all aware that we are getting questions.

<https://www.eff.org/cases/us-marshals-airborne-imsi-catchers>

EFF Files FOIA Suit Over U.S. Marshals'™ Spy Planes

Justice Department Must Provide Records of Aircraft-mounted Cell Tower Simulators

San Francisco - The Electronic Frontier Foundation (EFF) today filed a Freedom of Information Act (FOIA) lawsuit to shine light on the U.S. Marshals Service's (USMS) use of small aircraft mounted with controversial cell-phone tracking systems.

The Wall Street Journal revealed last year that the Marshals have been flying small, fixed-wing Cessna planes mounted with IMSI catchers--devices that emulate cell phone towers and are able to capture the locational data of tens of thousands of cell phones during a single flight. The planes--in the air since 2007--reportedly were based out of five metropolitan airports and shared by multiple agencies within the U.S. Department of Justice, even as sources within the agency questioned the legality of the program.

In the press, IMSI catchers are also known as "stingrays," a name taken from the "Stingray II" device manufactured by Harris Corporation, or "dirtboxes," a nickname for Boeing subsidiary Digital Receiver Technology's "DRT" devices. Across the country, the Justice Department has intervened in local public records battles to prevent the release of information about these technologies, employing tactics such as signing nondisclosure agreements with state and local law enforcement agencies, seizing records held by those agencies, and withholding key pieces of information about the technology from judges and criminal defendants.

A week after the Wall Street Journal story kicked off a media firestorm, EFF filed a comprehensive FOIA request with Justice Department and FBI over the USMS program, seeking a wide variety of records, including policies, procedures, training materials, communications about the legality of the program, and documentation of each use of the spy planes. As of this filing, the Justice Department has produced no records in response to the request or offered a timeline for release of the documents.

"These devices pose obvious privacy concerns, but the government has been opaque about its use of stingrays," EFF Legal Fellow Andrew Crocker said. "It's time to do away with the secrecy."

For more information and documents related to the suit, visit:
<https://www.eff.org/cases/us-marshals-airborne-imsi-catchers>

For this release:
<https://www.eff.org/press/releases/eff-files-foia-suit-over-us-marshals-spy-planes>

About EFF

The Electronic Frontier Foundation is the leading organization protecting civil liberties in the digital

world. Founded in 1990, we defend free speech online, fight illegal surveillance, promote the rights of digital innovators, and work to ensure that the rights and freedoms we enjoy are enhanced, rather than eroded, as our use of technology grows. EFF is a member-supported organization. Find out more at <https://www.eff.org>.

-end-

From: Harp, Jennifer C. (OPCL)
Subject: USMS Dirtbox Technology
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Sent: March 10, 2015 6:29 PM (UTC-04:00)
Attached: Dirtbox Program Information.docx

Hi Erika,

In preparation for tomorrow's USMS briefing on its Dirtbox technology, I wanted to flag for you the following articles:

- Americans' Cellphones Targeted in Secret U.S. Spy Program (WSJ, 11/13/14):
<http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>
- U.S. Defends Marshals in Wake of Secret Cellphone Spying Report (WSJ, 11/14/14):
<http://www.wsj.com/articles/justice-dept-defends-u-s-marshals-in-wake-of-secret-cellphone-spy-report-1415980141>
- Senators Raise Concerns About Justice Department Scanning Cellphones (WSJ, 12/31/14):
<http://www.wsj.com/articles/senators-raise-concerns-about-justice-department-scanning-cellphones-1420048912>
- CIA Gave Justice Department Secret Phone Scanning Technology (WSJ, 3/10/15):
<http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924>

(b) (6), one of our interns, also compiled the attached document with additional media coverage and analysis of the program.

See you tomorrow!

Best,
Jenny

Americans' Cellphones Targeted in Secret U.S. Spy Program

<http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>

- Justice Department is scooping up data from thousands of mobile phones through devices deployed on airplanes that mimic cellphone towers, a high-tech hunt for criminal suspects that is snagging a large number of innocent Americans,
- U.S. Marshals Service program operates Cessna aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population
- Planes are equipped with devices—some known as “dirtboxes” which mimic cell towers of large telecommunications firms and trick cellphones into reporting their unique registration information.
- The technology is aimed at locating cellphones linked to individuals under investigation by the government, including fugitives and drug dealers, but it collects information on cellphones belonging to people who aren't criminal suspects, these people said. They said the device determines which phones belong to suspects and “lets go” of the non-suspect phones.
- The device can briefly interrupt calls on certain phones. Authorities have tried to minimize the potential for harm, including modifying the software to ensure the fake tower doesn't interrupt anyone calling 911 for emergency help.
- The program cuts out phone companies as an intermediary in searching for suspects. Rather than asking a company for cell-tower information to help locate a suspect, which law enforcement has criticized as slow and inaccurate, the government can now get that information itself.
- People familiar with the program say they do get court orders to search for phones, but it isn't clear if those orders describe the methods used because the orders are sealed.
- The scanning is done by the Technical Operations Group of the U.S. Marshals Service, which tracks fugitives, among other things. Sometimes it deploys the technology on targets requested by other parts of the Justice Department
- A Verizon spokesman denied company involvement with the program

The Feds Are Now Using ‘Stingrays’ in Planes to Spy on Our Phone Calls

<http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/>

- The range of the equipment is currently unknown, but it means that data on potentially tens of thousands of phones could be collected during a single flight.
- The airplane-based system is a 2-foot-square box called the Dirtbox and appears to be the same or similar to so-called IMSI catchers or stingrays that law enforcement, the military, and intelligence agencies have been using for more than a decade.
- One of the main problems with this surveillance method, however, is that the devices force every cell phone in a region to connect to them
- The signal strength of the Dirtbox is probably greater than the ground-based stingrays—which likely means they pick up connections from many more phones unrelated to an investigation.
- The U.S. Marshals Service is known to loan out its stingray equipment to local police departments. So it very likely lends its Dirtbox service to multiple agencies around the

country as well—possibly even to the U.S. Customs Border Control to detect and track smugglers and illegal border crossings.

- There have been cases in which law enforcement agencies either bypassed the courts and used stingrays without obtaining an order as well as cases in which they lied to or withheld crucial information from judges about their use of the technology in order to get a court order without a lot of questions being asked.

U.S. Marshals Service Uses Airborne “Dirtboxes” to Collect Cell Phone Data

<http://jolt.law.harvard.edu/digest/privacy/u-s-marshals-service-uses-airborne-dirtboxes-to-collect-cell-phone-data>

- In a follow-up article in the Wall Street Journal, the Federal Communications Commission (“FCC”), which is responsible for licensing and regulating cell phone services, said, “We were not aware of this activity.” Frederick Joyce, a communications law attorney, questioned whether the program constituted “harmful interference” with licensed cell phone transmissions.
- “There are some serious and troubling legal questions about this program,” Hanni Fakhoury, a Staff Attorney for the Electronic Frontier Foundation, told Gizmodo. “It’s important to note this is very different from the government getting this information from a phone company. In the last few months, many state courts and legislatures have required law enforcement get a probable cause search warrant to use these devices. The US Marshals should explain how this program works and what kind of court authorization, if any, they’re obtaining to fly planes with ‘dirtboxes.’”
- Brian Owsley, a law professor at Indiana Tech and a former U.S. magistrate judge, told Ars Technica, “Regarding using planes as cell towers, that is problematic in my opinion. It strikes me as analogous to the use of Stingrays. Therefore, I think the government would need to obtain a search warrant based on probable cause consistent with the Fourth Amendment.”
- Senator Edward Markey of Massachusetts told the [Wall Street Journal](#), “The collection of American’s personal information raises significant legal and privacy concerns, particularly for innocent consumers.” Senator Al Franken of Minnesota, chairman of the Privacy, Technology, and the Law subcommittee, said, “While law-enforcement agents need to be able to track down and catch dangerous suspects, that should not come at the expense of innocent Americans’ privacy.”

The ‘dirtboxes’ of the US Marshals Service

<http://thehill.com/blogs/congress-blog/judicial/226823-the-dirtboxes-of-the-us-marshals-service>

- The fundamental issue involved in cell tower dumps and the collection of the same information from planes is whether accessing cell site location information by the government in order to track a person using his cell phone is a Fourth Amendment search for which a warrant based on probable cause is required, or whether it is covered by the Stored Communications Act (SCA). The answer to this question is critical because if obtaining such information is not a Fourth Amendment search, the government is not required to establish probable cause under the SCA, nor does the SCA, in most instances, require particularity or minimization of records.
- Courts are split on how to treat cell-site data. Most recently, the Florida Supreme Court in *Tracey v. State* __ So.3d __, 2014 WL 5285929 (2014) held that the defendant had a

subjective expectation of privacy in real time cell site location information (CSLI) regarding location of defendant's cellular telephone, as would support finding that police officers' use of CSLI to track defendant was a search falling under purview of Fourth Amendment. The court also concluded that simply knowing that a cell phone emitted locating signals to the service provider did not mean that defendant consented to use of that location information by third parties for unrelated purposes.

- In reaching this conclusion, the Court relied heavily upon Justice Sotomayor's concurrence in *United States v. Jones*, which held that the warrantless placement of a GPS tracking device on the defendant's vehicle and use of it to monitor the vehicle's movement on public streets constituted a search under the Fourth Amendment. Justice Sotomayor found that even short-term monitoring is problematic in that it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about" a person's private life and can be stored and mined for information for years. She also raised concerns that such monitoring may "alter the relationship between citizen and government in a way that is inimical to democratic processes" and that "[a]wareness that the Government may be watching chills associational and expressive freedoms."

ACLU Seeks Information About Airborne Cell Phone Snooping

<https://www.aclu.org/blog/national-security-technology-and-liberty/aclu-seeks-information-about-airborne-cell-phone-snoop>

- The ACLU is filing a Freedom of Information Act (FOIA) request today (11/19/14) for information about a newly revealed Marshals Service program that uses aircraft to suck up location data from tens of thousands of people's cell phones at a time.
- This is unacceptable — law enforcement must not purchase and deploy such powerful new technologies without the public's knowledge and input. Americans can only debate the merits and legality of new surveillance programs if we know they exist. Resistance against the government's secret, overzealous use of cell site simulators is spreading, and will surely grow as we learn more about these programs

From: Harp, Jennifer C. (OPCL)
Subject: RE: USMS Dirtbox Technology
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Sent: March 11, 2015 9:38 AM (UTC-04:00)

Hi Erika,

I just confirmed with Ed Bordley that we're all set for today's meeting at 1pm in Arlington. I'll meet you at your office around 12:20 so we can go down to the car together. Please let me know if you need anything else!

Best,
Jenny

From: Harp, Jennifer C. (OPCL)
Sent: Tuesday, March 10, 2015 6:29 PM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Subject: USMS Dirtbox Technology

Duplicative Information - See Document ID 0.7.12327.5060

From: Harp, Jennifer C. (OPCL)
Subject: RE: USMS Dirtbox Technology
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Sent: March 11, 2015 11:07 AM (UTC-04:00)
Attached: americans-cellphones-targeted-.pdf, justice-dept-defends-u-s-marshals-i.pdf, senators-raise-concerns-about-justi.pdf, cia-gave-justice-department-secret-.pdf

Yep, here you go.

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, March 11, 2015 10:23 AM
To: Harp, Jennifer C. (OPCL)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Subject: RE: USMS Dirtbox Technology

Jenny – thanks for the links. Can you scan the articles? I can't access the full version of the articles.

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: Tuesday, March 10, 2015 6:29 PM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Subject: USMS Dirtbox Technology

Duplicative Information - See Document ID 0.7.12327.5060



THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>

POLITICS AND POLICY

Americans' Cellphones Targeted in Secret U.S. Spy Program

Devices on Planes that Mimic Cellphone Towers Used to Target Criminals, but Also Sift Through Thousands of Other Phones

By DEVLIN BARRETT

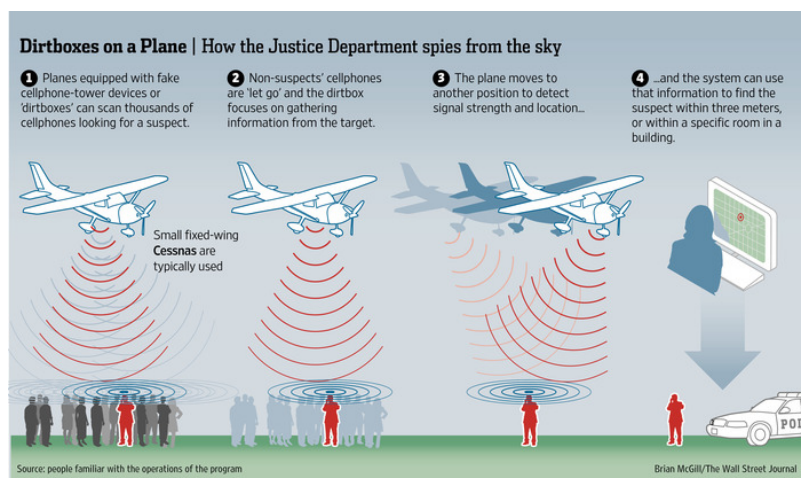
Updated Nov. 13, 2014 8:22 p.m. ET

WASHINGTON—The Justice Department is scooping up data from thousands of mobile phones through devices deployed on airplanes that mimic cellphone towers, a high-tech hunt for criminal suspects that is snagging a large number of innocent Americans, according to people familiar with the operations.

The U.S. Marshals Service program, which became fully functional around 2007, operates Cessna aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population, according to people familiar with the program.

Planes are equipped with devices—some known as “dirtboxes” to law-enforcement officials because of the initials of the Boeing Co. unit that produces them—which mimic cell towers of large telecommunications firms and trick cellphones into reporting their unique registration information.

The technology in the two-foot-square device enables investigators to scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location, these people said.



TK

People with knowledge of the program wouldn't discuss the frequency or duration of such flights, but said they take place on a regular basis.

A Justice Department official would neither confirm nor deny the existence of such a program. The official

said discussion of such matters would allow criminal suspects or foreign powers to determine U.S. surveillance capabilities. Justice Department agencies comply with federal law, including by seeking court approval, the official said.

MORE

- Justice Dept. Defends U.S. Marshals in Wake of Report (http://online.wsj.com/articles/justice-dept-defends-u-s-marshals-in-wake-of-secret-cellphone-spy-report-1415980141?mod=WSJ_hp_LEFTTopStories)
- Q&A: Explaining the Secret U.S. Cellphone Program (<http://blogs.wsj.com/briefly/2014/11/13/secret-u-s-cellphone-program-the-short-answer/>)

The program is the latest example of the extent to which the U.S. is training its surveillance lens inside the U.S. It is similar in approach to the National Security Agency's program to collect millions of Americans phone records, in that it scoops up large volumes of data in order to find a single person or a handful of people. The U.S. government justified the phone-records collection by arguing it is a minimally invasive way of searching for terrorists.

Christopher Soghoian, chief technologist at the American Civil Liberties Union, called it "a dragnet surveillance program. It's inexcusable and it's likely—to the extent judges are authorizing it—[that] they have no idea of the scale of it."

Cellphones are programmed to connect automatically to the strongest cell tower signal. The device being used by the U.S. Marshals Service identifies itself as having the closest, strongest signal, even though it doesn't, and forces all the phones that can detect its signal to send in their unique registration information.

PAST COVERAGE

- 'Stingray' Phone Tracker Fuels Constitutional Clash
(<http://online.wsj.com/articles/SB10001424053111904194604576583112723197574>) (9/22/11)
- New Details Show Broader NSA Surveillance Reach
(<http://online.wsj.com/articles/SB10001424127887324108204579022874091732470>) (8/20/13)

Even having encryption on a phone, such as the kind included on Apple Inc. 's iPhone 6, doesn't prevent this process.

The technology is aimed at locating cellphones linked to individuals under investigation by the government, including fugitives and drug dealers, but it collects information on cellphones belonging to people who aren't criminal suspects, these people said. They said the device determines which phones belong to suspects and "lets go" of the non-suspect phones.

The device can briefly interrupt calls on certain phones. Authorities have tried to minimize the potential for harm, including modifying the software to ensure the fake tower doesn't interrupt anyone calling 911 for emergency help, one person familiar with the matter said.

The program cuts out phone companies as an intermediary in searching for suspects. Rather than asking a company for cell-tower information to help locate a suspect, which law enforcement has criticized as slow and inaccurate, the government can now get that information itself. People familiar with the program say they do get court orders to search for phones, but it isn't clear if those orders describe the methods used because the orders are sealed.

Also unknown are the steps taken to ensure data collected on innocent people isn't kept for future examination by investigators. A federal appeals court ruled earlier this year that over-collection of data by investigators, and stockpiling of such data, was a violation of the Constitution.



The U.S. Justice Department's headquarters. *ASSOCIATED PRESS*

The program is more sophisticated than anything previously understood about government use of such technology. Until now, the hunting of digital trails created by cellphones had been thought limited to devices carried in cars that scan the immediate area for signals. Civil-liberties groups are suing for information about use of such lower-grade devices, some of them called Stingrays, by the Federal Bureau of Investigation.

By taking the program airborne, the government can sift through a greater volume of information and with greater precision, these people said. If a suspect's cellphone is identified, the technology can pinpoint its location within about 10 feet, down to a specific room in a building. Newer versions of the technology can be programmed to do more than suck in data: They can also jam signals and retrieve data from a target phone such as texts or photos. It isn't clear if this domestic program has ever used those features.

Similar devices are used by U.S. military and intelligence officials operating in other countries, including in war zones, where they are sometimes used to locate terrorist suspects, according to people familiar with the work. In the U.S., these people said, the technology has been effective in catching suspected drug dealers and killers. They wouldn't say which suspects were caught through this method.

The scanning is done by the Technical Operations Group of the U.S. Marshals Service, which tracks fugitives, among other things. Sometimes it deploys the technology on targets requested by other parts of the Justice Department.

Within the Marshals Service, some have questioned the legality of such operations and the internal safeguards, these people said. They say scooping up of large volumes of information, even for a short period, may not be properly understood by judges who approve requests for the government to locate a suspect's phone.

Some within the agency also question whether people scanning cellphone signals are doing enough to minimize intrusions into the phones of other citizens, and if there are effective procedures in place to safeguard the handling of that data.

It is unclear how closely the Justice Department oversees the program. "What is done on U.S. soil is completely legal," said one person familiar with the program. "Whether it should be done is a separate question."

Referring to the more limited range of Stingray devices, Mr. Soghoian of the ACLU said: "Maybe it's worth violating privacy of hundreds of people to catch a suspect, but is it worth thousands or tens of thousands or hundreds of thousands of peoples' privacy?"

The existence of the cellphone program could escalate tensions between Washington and technology companies, including the telecom firms whose devices are being redirected by the program.

If a suspect is believed to have a cellphone from Verizon Communications Inc., for example, the device would emit a signal fooling Verizon phones and those roaming on Verizon's network into thinking the plane is the nearest available Verizon cell tower. Phones that are turned on, even if not in use, would "ping" the flying device and send their registration information. In a densely populated area, the dirtbox could pick up data of tens of thousands of cellphones.

The approach is similar to what computer hackers refer to as a "man in the middle" attack, in which a person's electronic device is tricked into thinking it is relaying data to a legitimate or intended part of the communications system.

A Verizon spokesman said the company was unaware of the program. "The security of Verizon's network and our customers' privacy are top priorities," the spokesman said. "However, to be clear, the equipment referenced in the article is not Verizon's and is not part of our network."

An AT&T Inc. spokeswoman declined to comment, as did a spokeswoman for Sprint Corp.

For cost reasons, the flights usually target a number of suspects at a time, rather than just a single fugitive. But they can be used for a single suspect if the need is great enough to merit the resources, these people said.

The dirtbox and Stingray are both types of what tech experts call “IMSI catchers,” named for the identification system used by networks to identify individual cellphones.

The name “dirtbox” came from the acronym of the company making the device, DRT, for Digital Receiver Technology Inc., people said. DRT is now a subsidiary of Boeing. A Boeing spokeswoman declined to comment.

“DRT has developed a device that emulates a cellular base station to attract cellphones for a registration process even when they are not in use,” according to a 2010 regulatory filing Boeing made with the U.S. Commerce Department, which touted the device’s success in finding contraband cellphones smuggled in to prison inmates.

Corrections & Amplifications

An earlier version of this article incorrectly named Digital Receiver Technology Inc. as Digital Recovery Technology Inc. It also incorrectly listed what is known as IMSI catcher technology as ISMI catcher.

Write to Devlin Barrett at devlin.barrett@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

| | | | | | | | | |
|-------------------|-----------------------|-------------------------|------------------------------------|--|--|---|-----------------------------------|--------------------------------|
| FACTIVA | | | | | | FLIP THROUGH YOUR FACTIVA ALERTS | Now Available on Flipboard | » Learn more at factiva |
| RELIABLE ALERTING | 9 INTERFACE LANGUAGES | EASILY DISSEMINATE INFO | COVERAGE FROM NEARLY EVERY COUNTRY | | | | | |

THE WALL STREET JOURNAL.

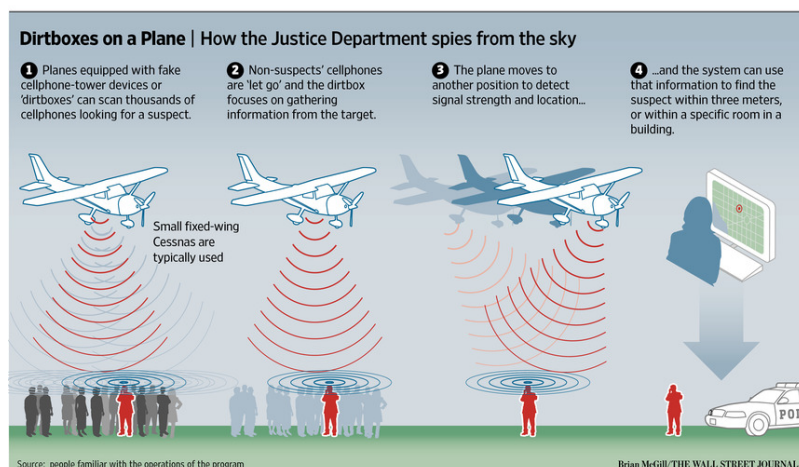
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924>

NATIONAL SECURITY

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



By DEVLIN BARRETT

Updated March 10, 2015 7:39 p.m. ET

WASHINGTON—The Central Intelligence Agency played a crucial role in helping the Justice Department develop technology that scans data from thousands of U.S. cellphones at a time, part of a secret high-tech alliance between the spy agency and domestic law enforcement, according to people familiar with the work.

The CIA and the U.S. Marshals Service, an agency of the Justice Department, developed technology to locate specific cellphones in the U.S. through an airborne device that mimics a cellphone tower, these people said.

Today, the Justice Department program, whose existence was reported by The Wall Street Journal last year, is used to hunt criminal suspects. The same technology is used to track terror suspects and intelligence targets overseas, the people said.

The program operates specially equipped planes that fly from five U.S. cities, with a flying range covering most of the U.S. population. Planes are equipped with devices—some past versions were dubbed “dirtboxes” by law-enforcement officials—that trick cellphones into reporting their unique registration information.

The surveillance system briefly identifies large numbers of cellphones belonging to citizens unrelated to the search. The practice can also briefly interfere with the ability to make calls, these people said.

Some law-enforcement officials are concerned the aerial surveillance of cellphone signals inappropriately mixes traditional police work with the tactics and technology of overseas spy work that is constrained by fewer rules. Civil-liberties groups say the technique amounts to a digital dragnet of innocent Americans’ phones.

READ MORE ON CAPITAL JOURNAL »

- Privacy Group Sues Over U.S. Cellphone Surveillance Program (<http://www.wsj.com/articles/privacy-group-sues-over-u-s-cellphone-surveillance-program-1423609467?mod=capitaljournalrelatedbox>) (Feb. 10)
- U.S. Spies on Millions of Drivers (<http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779?mod=capitaljournalrelatedbox>) (Jan. 26)
- Federal Agency Weighed Spying on Cars at Gun Shows (<http://www.wsj.com/articles/federal-agency-weighed-spying-on-cars-at-gun-shows-1422398739?mod=capitaljournalrelatedbox>) (Jan. 27)

The CIA has a long-standing prohibition that bars it from conducting most types of domestic operations, and officials at both the CIA and the Justice Department said they didn’t violate those rules.

The cooperation began a decade ago, when the CIA arranged for the Marshals Service to receive more than \$1 million in gear to conduct such surveillance, said people familiar with the program. More than \$100 million went into research and development of the devices.

For years, the U.S. Marshals' Technical Operations Group worked with the CIA's Office of Technical Collection to develop the technology. In the early days it was the CIA that provided the most resources, said the people familiar with the matter.

The CIA gave the Marshals Service the ability to conduct what officials called "silent stimulation" of cellphones. By using a device that mimics a cell tower, all phones in its range are compelled to send identifying information. When the device finds a target phone in that sea of information, the plane circles overhead until the device can locate it to within about 3 yards.

Some versions of the technology also can be used to intercept signals from phones, these people said. U.S. military and intelligence agencies have used the technology in Afghanistan, Iraq, and elsewhere to hunt terrorists, and map the use of cellphones in such places, according to people familiar with the work.

The cooperation between technical experts at the CIA and the Marshals Service, which law-enforcement officials have described as a "marriage," represents one way criminal investigators are increasingly relying on U.S. intelligence agencies for operational support and technical assistance in the wake of the Sept. 11, 2001, attacks. Many Justice Department officials view the joint effort with the CIA as having made valuable contributions to both domestic and overseas operations.

A CIA spokesman declined to comment on whether the CIA or any other agency uses the devices. Some technologies developed by the agency "have been lawfully and responsibly shared with other U.S. government agencies," the spokesman said. "How those agencies use that technology is determined by the legal authorities that govern the operations of those individual organizations—not CIA." He also said the relationship between the Marshals Service and CIA tech experts couldn't be characterized as a marriage.

The Justice Department, which oversees the Marshals Service, would neither confirm nor deny the existence of such technology, saying that doing so would tip off criminals.

A Justice Department spokesman said Marshals Service techniques are "carried out consistent with federal law, and are subject to court approval." The agency doesn't conduct "domestic surveillance, intelligence gathering, or any type of bulk data collection," the spokesman said, adding that it doesn't gather any intelligence on behalf of U.S. spy agencies.

To civil libertarians, the close involvement of America's premier international spy agency with a domestic law-enforcement arm shows how military and espionage techniques are now being used on U.S. citizens.

"There's a lot of privacy concerns in something this widespread, and those concerns only increase if we have an intelligence agency coordinating with them," said Andrew Crocker of the Electronic Frontier Foundation, which has filed a lawsuit seeking more details about the program and its origins.



The United States Department of Justice building PHOTO: EUROPEAN PRESSPHOTO AGENCY

The Marshals Service program is now the subject of congressional inquiries. The top Republican and Democrat on the Senate Judiciary Committee have raised concerns about possible invasion of privacy and legal oversight of the operations. Judiciary Committee Chairman Charles Grassley (R., Iowa) said the Justice Department must provide answers about its use of the technology, "including the legal authority agencies obtain prior to deploying these tools, the specific information they are giving to judges when requesting to use them, and what policies are in place to ensure the civil liberties of innocent Americans are protected."

Concerns about how the Marshals Service uses the equipment grew among some officials last year after an incident in the Sinaloa area of Mexico. In that operation, several U.S. Marshals personnel were dressed as Mexican marines and carrying Mexican weapons as a Marshals plane circled overhead, searching for a suspect's cellphone signal, according to people familiar with the operation.

As the men on the ground moved toward their target, they were fired on by drug-cartel suspects, and one of the Americans was badly wounded and airlifted to a hospital. The incident underscored for some law-enforcement officials the risks of such operations—that their personnel could be killed or possibly imprisoned while doing something that could be viewed as a crime in a foreign country. People familiar with the work say the agency conducts such operations roughly every few months, though each one is based on specific intelligence and needs.

The CIA and Marshals Service began field-testing one version of the device in 2004, said people familiar with the early years of the cooperation. That device worked on AT&T and T-Mobile phones, as well as most cellphones outside the U.S. As part of the joint work with the CIA, the Marshals Service received more than one of the devices at no cost. At the time, each unit had a price tag of more than \$300,000, these people said.

In 2005, the CIA gave the Marshals Service technology to conduct “silent stimulation” of those types of cellphones, both for identifying them and, with a court order, intercepting the communications, these people said. The following year, the CIA and Marshals Service began field testing a way of cracking a different cellphone system used widely in the U.S., giving them the ability to identify phones on the Verizon and Sprint/Nextel networks. A Sprint spokeswoman declined to comment while the other phone companies didn’t respond to requests for comment.

In 2008, the CIA arranged for the Marshals Service to receive without charge one of the new devices, which cost about \$500,000 each, these people said. That year, they began field testing a new version that would work against the next generation of cellphones, according to people familiar with the work.

Write to Devlin Barrett at devlin.barrett@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.



THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/justice-dept-defends-u-s-marshals-in-wake-of-secret-cellphone-spy-report-1415980141>

POLITICS AND POLICY

U.S. Defends Marshals in Wake of Secret Cellphone Spying Report

Devices on Planes Look for Criminals but Sift Through Other Phones;
Program Doesn't Track Public, Says Official

By DEVLIN BARRETT and GAUTHAM NAGESH

Updated Nov. 14, 2014 5:56 p.m. ET

WASHINGTON—A Justice Department official on Friday defended the legality of a program to scoop up data from thousands of mobile phones as the secret operation came under scrutiny from lawmakers and caught the federal agency that regulates the nation's airwaves by surprise.

RELATED

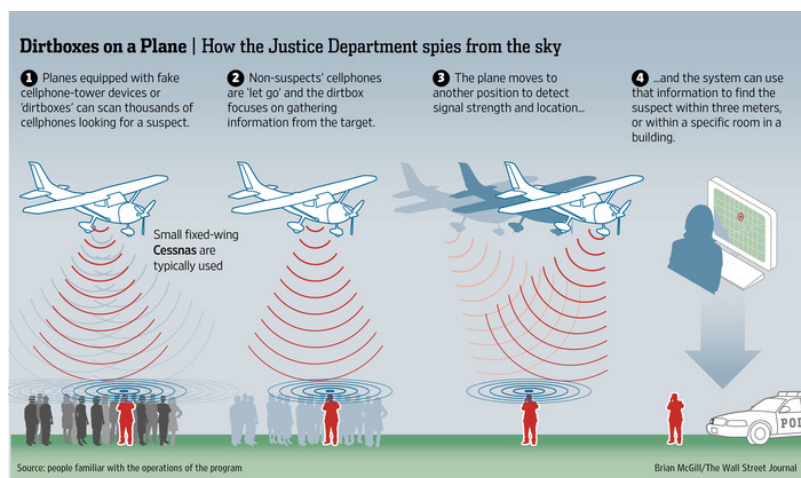
- Planes Secretly Track American Cellphones (http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533?mod=WSJ_hp_LEFTTopStories)
- Q&A: Explaining the Secret U.S. Cellphone Program (<http://blogs.wsj.com/briefly/2014/11/13/secret-u-s-cellphone-program-the-short-answer/>)

The Justice Department, without formally acknowledging the existence of the program, defended the legality of the operation by the U.S. Marshals Service, saying the agency doesn't maintain a database of everyday Americans' cellphones.

The Wall Street Journal on Thursday revealed the program, in which Cessna aircraft are outfitted with devices—some known as “dirtboxes” to law-enforcement officials—that mimic cell towers of large telecommunications companies and trick cellphones into reporting identifying information in a hunt for criminal suspects. The technology enables investigators to scoop data from tens of thousands of phones in a single flight, collecting the number and general location, according to people familiar with the program.

On Friday, the Federal Communications Commission, which regulates the nation’s airwaves, said it had no idea about the program.

“We were not aware of this activity,” said Kim Hart, a spokeswoman for the FCC, which licenses and regulates cell-service providers.



Democratic lawmakers also began looking for answers.

“Americans are rightfully disturbed by just how pervasive collection of mobile-phone information is, even of innocent individuals,” said Sen. Edward Markey (D., Mass.).

“While this data can be

an important tool for law enforcement to identify and capture criminals and terrorists, we must ensure the privacy rights of Americans are protected....The collection of American’s personal information raises significant legal and privacy concerns, particularly for innocent consumers.”

Sen. Al Franken (D., Minn.), said he was “concerned by recent reports about the Justice Department’s collection of cellphone data from aircraft, and we need to find out more details about this program.” Mr. Franken said “while law-enforcement agents need to be able to track down and catch dangerous suspects, that should not come at the expense of innocent Americans’ privacy.”

A Justice Department official on Friday refused to confirm or deny the existence of such a program, because doing so would allow criminals to better evade law enforcement. But the official said it would be “utterly false” to conflate the law-enforcement program with the collection of bulk telephone records by the National Security Agency, a controversial program already being challenged in the courts and by some members of Congress.

The official didn’t address the issue of how much data, if any, is held on the dirtboxes by law-enforcement officials but said the agency doesn’t maintain any databases of general public cellphone information and said any activity is legal and “subject to court approval.”

PAST COVERAGE

- ‘Stingray’ Phone Tracker Fuels Constitutional Clash
(<http://online.wsj.com/articles/SB10001424053111904194604576583112723197574>) (9/22/11)
- New Details Show Broader NSA Surveillance Reach
(<http://online.wsj.com/articles/SB10001424127887324108204579022874091732470>) (8/20/13)

The Marshals’ investigative techniques are deployed “only in furtherance of ordinary law-enforcement operations, such as the apprehension of wanted individuals, and not to conduct domestic surveillance or intelligence gathering,” the official said.

The program’s defenders say it has been an effective way of catching fugitives, including drug suspects and suspected killers, but they declined to provide specific examples in which it was used.

Frederick Joyce, an attorney specializing in communications law, said the program raises legal questions beyond just the privacy issues that concern civil libertarians.

“In my experience, the only folks authorized to transmit on those channels are licensed carriers, period,” said Mr. Joyce. The phone companies, he said, “are adamant about protecting their customers against any kind of harmful interference, and this to me is harmful interference.”

People familiar with the program say it is designed to be minimally disruptive to cellular networks.

The program operates from at least five metropolitan-area airports, with a flying range covering most of the U.S. population, according to people familiar with the program.



The U.S. Justice Department's headquarters. *ASSOCIATED PRESS*

The name dirtbox came from the acronym of the company making the device, DRT, for Digital Recovery Technology Inc., people familiar with the matter said. DRT is now a wholly owned subsidiary of Boeing Co. A Boeing spokeswoman declined to comment.

—Michael R. Crittenden contributed to this article.

Write to Devlin Barrett at devlin.barrett@wsj.com and Gautham Nagesh at gautham.nagesh@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

| | | | | | | | | |
|----------------------|-----------------------------|----------|-------------------------------|--|---|---|---|---|
| F | A | C | T | I | V | A | FLIP THROUGH YOUR FACTIVA ALERTS | Now Available on  Flipboard » Learn more at factiva |
| RELIABLE ALERTING | 9 INTERFACE LANGUAGES | | EASILY DISSEMINATE INFO | COVERAGE FROM NEARLY EVERY COUNTRY |  |  | | |

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/senators-raise-concerns-about-justice-department-scanning-cellphones-1420048912>

POLITICS AND POLICY

Senators Raise Concerns About Justice Department Scanning Cellphones

Letter From Top Democrat and Republican Cites Privacy Interests of Innocent Individuals



Attorney General Eric Holder, shown here in early December, was sent a letter by members of the Senate Judiciary Committee questioning agencies' use of secret devices to scan large numbers of cellphones. *GETTY IMAGES*

By DEVLIN BARRETT

Dec. 31, 2014 1:01 p.m. ET

The top Democrat and Republican on the Senate Judiciary Committee are seeking answers from the Justice Department about how often and under what circumstances it uses secret devices to scan large numbers of cellphones to hunt for criminal suspects, saying that one agency recently changed its internal rules on when and how to use the technology.

In a Dec. 23 letter to Attorney General Eric Holder and Homeland Security Secretary Jeh Johnson, Sens. Patrick Leahy (D., Vt.) and Charles Grassley (R., Iowa) said they have concerns about whether law-enforcement agencies “have adequately considered the privacy interests of other individuals who are not targets of the inception, but whose information is nevertheless being collected when these devices are used.”

The letter was written in response to a Wall Street Journal story in November describing how the U.S. Marshals Service uses devices that mimic cellphone towers to sift through large volumes of cellphone signals to try to find the phones of specific suspects.

The devices are put in planes, so they can fly over large areas and scan large quantities of phones—sometimes tens of thousands at a time in densely populated areas, according to people familiar with the technique. In the past, some of the devices have been called “dirtboxes” by law-enforcement personnel, a nickname derived from the company that manufactures them; but most of the devices currently in use aren’t dirtboxes, according to people familiar with the technique.

The technique of sifting through so many cellphones has raised the concerns of privacy advocates, who say it is a dragnet that gathers too much information about innocent people.

In their letter, the senators said they have been briefed that the Federal Bureau of Investigation recently changed its policies for the use of such technology, requiring investigators to get a search warrant before using such devices, including less powerful, handheld units used in police cars.

The lawmakers wrote they are concerned about the exceptions to the search-warrant policy, which include cases with an imminent danger to public safety, cases involving a fugitive and cases in which the technology is used in public places or where the FBI deems there is no reasonable expectation of privacy.

The lawmakers indicated they have had some knowledge in the past of the use of the technology, but wrote that the 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 [the government agencies] seek prior to using them.”

The Journal has also reported the same technology is used by American law enforcement operating in Mexico, where U.S. Marshals personnel have dressed as Mexican marines and carried weapons in raids seeking to capture drug-cartel suspects. One U.S. Marshals inspector was shot in one such raid in July.

The Justice Department has refused to confirm or deny the use of such technology, but said that what it does is legal and subject to court approval. Officials haven’t said whether judges approving such searches have been told the method by which the government will conduct the search. Government officials have said they don’t keep a database of innocent people’s phone information picked up by the devices.

A Justice Department spokeswoman said the agency is reviewing the letter.

Write to Devlin Barrett at devlin.barrett@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

From: O'Brien, Alicia C (OLA)
Subject: FW: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators)
To: Tyrangiel, Elana (OLP)
Sent: March 20, 2015 11:22 AM (UTC-04:00)
Attached: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators).pdf, 3202015_95910AM_12-23-14 PJJ and CEG to DOJ and DHS.pdf

I'll give you a ring, but let me know if there's a good time to speak briefly. Thanks much- Alicia

Alicia C. O'Brien
Office of Legislative Affairs

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

From: O'Brien, Alicia C (OLA)
Sent: Friday, March 20, 2015 10:01 AM
To: Kadzik, Peter J (OLA)
Subject: FW: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators)

Here's where we are now. Pinged Jill already to get a better understanding of where we are on this issue so we can respond to Jason; I'll call Elana too.

Alicia C. O'Brien
Office of Legislative Affairs

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

From: O'Brien, Alicia C (OLA)
Sent: Friday, March 20, 2015 9:49 AM
To: 'Foster, Jason (Judiciary-Rep)'; Wade Tyson, Jill C (OLA); Lim, Jay (Judiciary-Rep); Flint, Lara (Judiciary-Dem)
Subject: RE: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators)

Understood on our end too and we appreciate your efforts. I saw Jay's email as well. We would be happy to give you a call this afternoon. Will get back to you shortly with a time.

Alicia C. O'Brien
Office of Legislative Affairs

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

From: Foster, Jason (Judiciary-Rep) [[\(b\) \(6\)](mailto:(b) (6))]
Sent: Friday, March 20, 2015 9:27 AM
To: Wade Tyson, Jill C (OLA); Lim, Jay (Judiciary-Rep); Flint, Lara (Judiciary-Dem); O'Brien, Alicia C (OLA)
Subject: RE: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators)

Understood. We are attempting to consult with you and provide you the opportunity to articulate more specifically any legitimate concerns about the precise wording of our letter--rather than merely stating your general preference against discussing these technologies publicly.

From: Wade Tyson, Jill C (OLA) [[\(b\) \(6\)](mailto:(b) (6))]
Sent: Thursday, March 19, 2015 5:06 PM
To: Lim, Jay (Judiciary-Rep); Flint, Lara (Judiciary-Dem); O'Brien, Alicia C (OLA)
Cc: Foster, Jason (Judiciary-Rep)
Subject: Re: 2015-03-18 CEG and PJJ to DOJ (Cell-Site Simulators)

We appreciate your regard for the sensitivities surrounding technologies used by the Department's law enforcement components during investigations. As you know from the briefings we have provided, we continue to prefer to keep our specific technologies non-public. However, we leave to your discretion whether to make public your letter(s).

Thanks.

From: Lim, Jay (Judiciary-Rep) [mailto:(b) (6)]
Sent: Thursday, March 19, 2015 04:06 PM Eastern Standard Time
To: Flint, Lara (Judiciary-Dem) <(b) (6)>; O'Brien, Alicia C (OLA)
Cc: Foster, Jason (Judiciary-Rep) <(b) (6)>; Wade Tyson, Jill C (OLA)
Subject: RE: 2015-03-18 CEG and PJL to DOJ (Cell-Site Simulators)

Thanks Lara,

To be clear, if we do not hear either way from the Department by COB today (6pm EST), we will assume that the Department does not consider the letter LES.

Best,
Jay

From: Flint, Lara (Judiciary-Dem)
Sent: Thursday, March 19, 2015 4:04 PM
To: O'Brien, Alicia C (OLA); Lim, Jay (Judiciary-Rep)
Cc: Foster, Jason (Judiciary-Rep); Wade Tyson, Jill C (OLA)
Subject: RE: 2015-03-18 CEG and PJL to DOJ (Cell-Site Simulators)

Checking in on this. Thanks.

From: Flint, Lara (Judiciary-Dem)
Sent: Wednesday, March 18, 2015 4:31 PM
To: 'O'Brien, Alicia C (OLA)'; Lim, Jay (Judiciary-Rep)
Cc: Foster, Jason (Judiciary-Rep); Wade Tyson, Jill C (OLA)
Subject: RE: 2015-03-18 CEG and PJL to DOJ (Cell-Site Simulators)

I'm adding Jill, and would just add that we trust DOJ will check with relevant components. We have not separately sent it to FBI or others. Thanks all! Lara

From: O'Brien, Alicia C (OLA) [mailto:(b) (6)]
Sent: Wednesday, March 18, 2015 4:00 PM
To: Lim, Jay (Judiciary-Rep)
Cc: Foster, Jason (Judiciary-Rep); CEG (Judiciary-Rep); Flint, Lara (Judiciary-Dem)
Subject: RE: 2015-03-18 CEG and PJL to DOJ (Cell-Site Simulators)

Confirming receipt.

Alicia C. O'Brien
Office of Legislative Affairs
(b) (6)
(b) (6)

From: Lim, Jay (Judiciary-Rep) [[\(b\) \(6\)](mailto:(b) (6))]
Sent: Wednesday, March 18, 2015 3:58 PM
To: O'Brien, Alicia C (OLA)
Cc: Foster, Jason (Judiciary-Rep); CEG (Judiciary-Rep); Flint, Lara (Judiciary-Dem)
Subject: 2015-03-18 CEG and PJI to DOJ (Cell-Site Simulators)

Hey Alicia,

Attached is a letter from Chairman Grassley and Ranking Member Leahy. Please confirm receipt. Please send all formal correspondence electronically in PDF format to [\(b\)\(6\) Lara Flint](mailto:(b)(6) Lara Flint) me, [\(b\)\(6\) Jason Foster](mailto:(b)(6) Jason Foster), and CEG@judiciary-rep.senate.gov.

Additionally, please let us know by COB tomorrow (Thursday, March 19) whether the Department considers this letter Law Enforcement Sensitive. Department components asked us to consult with them prior to publicizing our letters, so this is an effort to address that concern.

Thank you,

Jay Lim
Investigative Counsel
Chairman Charles E. Grassley
U.S. Senate Committee on the Judiciary
[\(b\) \(6\)](mailto:(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 TILIS, 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

KYLAN L. DAVIS, Chief Counsel and Staff Director
KRISTINE J. LYONS, 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).
(b) (6) Thank you for your cooperation in 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

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

From: Brown Lee, Erika (ODAG)
Subject: FW: As promised
To: Lane Scott, Kristi Z (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Sent: May 7, 2015 10:27 AM (UTC-04:00)
Attached: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx

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

Best,
Erika

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

From: Tyrangiel, Elana (OLP)
Sent: Thursday, May 07, 2015 9:31 AM
To: Brown Lee, Erika (ODAG)
Subject: As promised

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

From: Brown Lee, Erika (ODAG)
Subject: RE: As promised
To: Tyrangiel, Elana (OLP)
Sent: May 8, 2015 11:44 AM (UTC-04:00)

Hi Elana – apologies that I will not be able to meet this afternoon. As I'm sure you can appreciate, there are several other urgent matters on my plate at present. It was very helpful to meet with you yesterday evening. I am working to expedite my review and will get additional comments back to you as soon as possible.

Best,
Erika

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

From: Tyrangiel, Elana (OLP)
Sent: Thursday, May 07, 2015 9:31 AM
To: Brown Lee, Erika (ODAG)
Subject: As promised

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

<< File: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx >>

From: Harp, Jennifer C. (OPCL)
Subject: RE: As promised
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: May 8, 2015 4:37 PM (UTC-04:00)
Attached: FBI Stingray Resources.docx

Hi Erika,

I've had a chance to review the Draft Policy for Cell-Site Simulator Technology. Although it may warrant more discussion, I think (b) (5)

. It appears as if during the FBI's congressional briefing this fall, FBI stated that "FBI's new policy requires FBI agents to obtain a search warrant whenever a cell-site simulator is used as part of a 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." The new draft policy (b)(5) per FBI

I've attached a small sampling of the media/congressional reactions to the program. I also inputted the text of the WSJ article since it is the most recent.

Happy to discuss on Monday or once you've digested the information and policy.

Best,
Jenny

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

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

Best,
Erika

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

From: Tyrangiel, Elana (OLP)
Sent: Thursday, May 07, 2015 9:31 AM
To: Brown Lee, Erika (ODAG)
Subject: As promised

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

<< File: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx >>

FBI's Stingray Program Resources

1. Leahy & Grassley Letter to Holder on the Stingray Program (Dec. 23, 2014): <http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program>
2. ARS Technica, FBI Says Search Warrants Not Needed to Use "Stingrays" in Public Places (Jan. 5, 2015): <http://arstechnica.com/tech-policy/2015/01/fbi-says-search-warrants-not-needed-to-use-stringrays-in-public-places/>
3. EPIC, EPIC Prevails in Stingray Case Against FBI (Feb. 20, 2015): <http://epic.org/foia/fbi/stingray/>
4. PC World, US Reviews Use of Cellphone Spying Technology (May 3, 2015): <http://www.pcworld.com/article/2918072/us-reviews-use-of-cellphone-spying-technology.html>
5. WSJ, U.S. Will Change Stance on Secret Phone Tracking (May 3, 2015): <http://www.wsj.com/articles/u-s-will-change-stance-on-secret-phone-tracking-1430696796?mod=mktw>

The Justice Department will start revealing more about the government's use of secret cellphone-tracking devices and has launched a wide-ranging review into how law-enforcement agencies deploy the technology, according to Justice officials.

In recent months, the Federal Bureau of Investigation has begun getting search warrants from judges to use the devices, which hunt criminal suspects by locating their cellphones, the officials said. For years, FBI agents didn't get warrants to use the tracking devices.

Senior officials have also decided they must be more forthcoming about how and why the devices are used — although there isn't yet agreement within the Justice Department about how much to reveal or how quickly.

The move comes amid growing controversy over the Justice Department's use of such devices, some versions of which, as The Wall Street Journal reported last year, are deployed in airplanes and scan data from thousands of phones used by Americans who aren't targets of investigations.

There are still many instances where law enforcement doesn't get warrants before using the devices, sometimes called "IMSI catchers" and known by various names like Stingray, Hailstorm, and "dirtbox," according to officials' public statements. The agencies that use the devices within the Justice Department — the FBI, the U.S. Marshals Service and the Drug Enforcement Administration — each have different rules and procedures for their use.

The Justice Department review will determine how they should be used, officials said.

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley
To: Moyer, Pam (OPCL)
Sent: May 13, 2015 11:35 AM (UTC-04:00)

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 13, 2015 10:49 AM
To: Wood, Alexander W (OPCL); Raut, Anant (ATR)
Subject: FW: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

FYI

From: Chung, Joo (OPCL)
Sent: Tuesday, January 06, 2015 5:00 PM
To: Harp, Jennifer C. (OPCL); Lane Scott, Kristi Z (OPCL); Brown Lee, Erika (ODAG)
Subject: RE: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

Yes, I saw that date, and the responses are due Jan. 30th. I just wanted to see if there was additional background that had a Feb. 16th date.

From: Harp, Jennifer C. (OPCL)
Sent: Tuesday, January 06, 2015 4:35 PM
To: Chung, Joo (OPCL); Lane Scott, Kristi Z (OPCL); Brown Lee, Erika (ODAG)
Subject: RE: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley

Duplicative Information - See Document ID 0.7.12327.5035



From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Draft Cell-Site Simulator Policy
To: Moye, Pam (OPCL)
Sent: May 13, 2015 11:35 AM (UTC-04:00)
Attached: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 13, 2015 10:54 AM
To: Wood, Alexander W (OPCL); Raut, Anant (ATR)
Subject: Draft Cell-Site Simulator Policy

A/A,

I've attached OLP's draft Cell-Site Simulator Policy. Please keep this policy close hold. Erika hasn't provided her official comments yet, but I think we are right to (b) (5). Once we hear from (b)(6), (7)(C), (7)(F) per DEA we can circle back to discuss.

Thanks,

Kristi Lane Scott
Acting Director
Office of Privacy and Civil Liberties
U.S. Department of Justice
1331 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
202.307.0693 (fax)
(S) (b) (6)
(TS) (b) (6)

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

From: Harp, Jennifer C. (OPCL)
Subject: Fwd: As promised
To: Wood, Alexander W (OPCL); Lane Scott, Kristi Z (OPCL)
Sent: May 13, 2015 5:15 PM (UTC-04:00)
Attached: FBI Stingray Resources.docx, ATT00001.htm

AWW,

Since you've got an OLA review on cell site simulators, I figured I'd forward you what I sent Erika on FBI's Stingray program. Not sure if it's at all helpful. Happy to help further once I get back!

-JH

Begin forwarded message:

From: "Harp, Jennifer C. (OPCL)" <(b) (6)>
Date: May 8, 2015 at 4:37:14 PM EDT
To: "Brown Lee, Erika (ODAG)" <(b) (6)>
Cc: "Lane Scott, Kristi Z (OPCL)" <(b) (6)>
Subject: RE: As promised

Duplicative Information - See Document ID 0.7.12327.5339

**Senator John Boozman
Questions for the Record
CJS Subcommittee Hearing
March 12, 2015**

Department of Justice Law Enforcement Agencies FY 2016 Budget Request

Not Responsive

Not Responsive

**Senator Patrick Leahy
Questions for the Record
CJS Subcommittee Hearing
March 12, 2015**

Department of Justice Law Enforcement Agencies FY 2016 Budget Request

Under the DEA's current policies relating to the use of cell-site simulators, how many times has the DEA employed such a device without prior court approval, and what were the reasons for doing so? What is the policy regarding retention of data?

(b) (5) [REDACTED]

(b) (5) [REDACTED]

Since 2001, how many cell-site simulators has the DEA purchased or obtained from another government agency? What has been the cost, per year, for the acquisition, maintenance and deployment of the DEA's cell-site simulators?

(b) (5) [REDACTED]

(b) (5) [REDACTED]

Not Responsive

Sen. Leahy

Recent media reports have raised questions about federal law enforcement's use of sophisticated surveillance technology, like cell-site simulators and license plate reading cameras, to track suspects historically and in real-time. Although I appreciate the

potential value of this technology to law enforcement, I am concerned about the potential impact on the privacy rights of innocent Americans.

Under the BATFE's current policies relating to the use of cell-site simulators, how many times has the BATFE employed such a device without prior court approval, and what were the reasons for doing so? What is the policy regarding retention of data?

(b) (5)

[Redacted]

(b) (5)

[Redacted]

(b) (5)

[Redacted]

(b) (5)

[Redacted]

(b) (5)

[Redacted]

| | |
|------------|------------|
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |
| [Redacted] | [Redacted] |

Not Responsive

From: Wood, Alexander W (OPCL)
Subject: RE: Cell Site Simulators
To: Krissoff, Sarah R. (ATF)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: May 15, 2015 4:02 PM (UTC-04:00)

Sarah,

Thanks for taking the time to talk with me today.

We'll assume the ATF legislative affairs team will (b) (5) [REDACTED].

Best regards,
Alex

From: Wood, Alexander W (OPCL)
Sent: Thursday, May 14, 2015 10:28 AM
To: Krissoff, Sarah R. (ATF)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: FW: Cell Site Simulators

Hi Sarah,

I am following up on Stephanie's email below.

The reason I reached out to Stephanie was because we received QFRs for ATF on a number of issues, including ATF programs/system, including the use of cell-site simulator technology. These are attached. (Comments are due by noon on Monday).

We particularly concerned about (b) (5) [REDACTED]

As you may or may not know DOJ OLP is drafting a policy on the use of cell-site simulator and we also want to be sure any QFRs are consistent with that policy.

Lastly, I was asked to set up a briefing for our Chief Privacy and Civil Liberties Officer (CPCLO) Erika Brown Lee on ATF's use of cell-site simulator technology. Would you or another ATF representative be willing to provide a short briefing next week?

Please feel free to call me to discuss this in more detail.

Best regards,
Alex

Alexander Wood
Senior Counsel
Office of Privacy and Civil Liberties (OPCL)
U.S. Department of Justice
1331 Pennsylvania Ave. NW Suite 1000
Washington, DC 20530

(b) (6) (e-mail)

(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: (b)(6) Stephanie Boucher [[\(b\)\(6\)](mailto:(b)(6))]

Sent: Wednesday, May 13, 2015 5:30 PM

To: Wood, Alexander W (OPCL)

Cc: Krissoff, Sarah R. (ATF)

Subject: Cell Site Simulators

Alex,

The point of contact for cell site simulators for ATF is Sarah Krissoff, Acting Deputy Chief Counsel. I have cc'd her on this email. If you need anything from me or Amanda on the other issues prior to Friday let me know. Thanks.

Stephanie

1. **From** 2. Tyrangiel, Elana (OLP)
:
3. **Subj** 4. auditing
ect:
5. **To:** 6. Brown Lee, Erika (ODAG)
7. **Sent:** 8. May 20, 2015 6:41 PM (UTC-04:00)

9. (b) (5) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

From: Brown Lee, Erika (ODAG)
Subject: RE: DRAFT 5-20 redlines - DOJ Cell-Site Simulator Policy
To: Tyrangiel, Elana (OLP); Fried, Hannah (OLP)
Cc: Jain, Samir (ODAG)
Sent: May 20, 2015 6:55 PM (UTC-04:00)

Elana – thanks for incorporating the edits. The proposed additions address my concerns.

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: Tyrangiel, Elana (OLP)
Sent: Wednesday, May 20, 2015 6:50 PM
To: Fried, Hannah (OLP); Brown Lee, Erika (ODAG)
Cc: Jain, Samir (ODAG)
Subject: DRAFT 5-20 redlines - DOJ Cell-Site Simulator Policy

Hi all –

Erika and I just spoke again, and I think we're in agreement that the redlines in this version on page 2 and 3 will resolve Erika's issues with the policy. Erika, if you could confirm, that would be great.

Assuming we're all good, we'll go back to the components with these and will let you know if there's any problem.

Thanks,
Elana

<< File: DRAFT 5-20 redlines - DOJ Cell-Site Simulator Policy.docx >>

From: Fried, Hannah (OLP)
Subject: stingray- latest
To: Tyrangiel, Elana (OLP)
Sent: May 21, 2015 6:55 PM (UTC-04:00)
Attached: DRAFT 5-21 redlines - DOJ Cell-Site Simulator Policy.docx

This draft incorporates (b) (5) . (It is otherwise also up-to-date, including Erika's (b) (5) edits; (b) (5) per Joe Mazel; and the (b) (5) edit from Joyce.)

From: Lane Scott, Kristi Z (OPCL)
Subject: Stingray
To: Moss, Robin (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Sent: June 11, 2015 2:19 PM (UTC-04:00)
Attached: Stingray Briefing.eml, FW_ Stingray Briefing.eml, RE_ Stingray Briefing.eml, FW_ Stingray Briefing (1).eml, RE_ Stingray Briefing (1).eml, RE_ Stingray Briefing (2).eml, Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley.eml, Fwd_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley.eml, RE_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley.eml, RE_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley (1).eml, RE_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley (2).eml, Re_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley (3).eml, FW_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley.eml, FW_ Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program _ Chuck Grassley (1).eml

Hi Robin,

Please let me know if you aren't able to open these. I've attached my documents for Stingray. I'll separately send Dirtbox emails. I'm still waiting on Erika to send me her materials. I know she's been attending to the breach incident.

Thanks,

Kristi

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Stingray Briefing
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI)
Cc: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); Harp, Jennifer C. (OPCL); Cardwell, Christine (ODAG)
Sent: January 5, 2015 9:24 AM (UTC-05:00)

This message has been archived.

Hi (b)(6), (7)(C) per FBI

I wanted to touch base with you regarding the Stingray briefing Erika requested. Given the Senate Judiciary Committee's inquiry last week, it's important for Erika to understand the FBI's use of this technology. I've attached an article below. Please let us know what dates are available.

http://www.law360.com/privacy/articles/607712?nl_pk=85c4ed9f-2337-4cae-accc-535a8e37689b&utm_source=newsletter&utm_medium=email&utm_campaign=privacy

Best,

Kristi Lane Scott
Deputy Director
Office of Privacy and Civil Liberties
U.S. Department of Justice
1331 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
202.307.0693 (fax)
(S) (b) (6)
(TS) (b) (6)

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

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, November 20, 2014 5:52 PM
To: (b)(6), (7)(C) per FBI (FBI)
Cc: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); (b)(6), (7)(C) per FBI (FBI); Harp, Jennifer C. (OPCL); Cardwell, Christine (ODAG)
Subject: Stingray Briefing

Hi (b)(6), (7)(C) per FBI

I'm following up on your discussion this week with Erika. She would like to schedule a briefing regarding FBI's use of stingray technology. I'll work with Erika's assistant, Christine Cardwell, on the scheduling. Please let me know if you have any questions.

Thanks!

Kristi Lane Scott
Deputy Director

Office of Privacy and Civil Liberties
U.S. Department of Justice
1331 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20530
(b) (6) (office)
(b) (6) (mobile)
202.307.0693 (fax)

(S) (b) (6)
(TS) (b) (6)

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

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Stingray Briefing
To: (b)(6), (7)(C) per FBI (OGC) (FBI); (b)(6), (7)(C) per FBI (OGC) (FBI)
Cc: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); Harp, Jennifer C. (OPCL); Cardwell, Christine (ODAG)
Sent: January 5, 2015 4:38 PM (UTC-05:00)

This message has been archived.

Thanks (b)(6), (7)(C) per FBI. Please keep us posted.

From: (b)(6), (7)(C) per FBI [mailto:(b)(6), (7)(C), (7)(E) per FBI]
Sent: Monday, January 05, 2015 4:25 PM
To: Lane Scott, Kristi Z (OPCL); (b)(6), (7)(C) per FBI (FBI)
Cc: Brown Lee, Erika (ODAG); Chung, Joo (OPCL); Harp, Jennifer C. (OPCL); Cardwell, Christine (ODAG)
Subject: RE: Stingray Briefing

Thanks, Kristi, we are still working on this and hope to get back to you in the near future. (b)(6), (7)(C) per FBI

(b)(6), (7)(C) per FBI

Deputy General Counsel

General Law Branch, Office of the General Counsel

Federal Bureau of Investigation

935 Pennsylvania Ave, NW

Washington, D.C. 20535

(b)(6), (7)(C), (7)(E) per FBI

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling (b)(6), (7)(C), (7)(E) per FBI.

From: Lane Scott, Kristi Z (OPCL) [mailto:(b) (6)]
Sent: Monday, January 05, 2015 9:24 AM
To: (b)(6), (7)(C) per FBI
Cc: Brown Lee, Erika (ODAG) (JMD); Chung, Joo (OPCL) (JMD); Harp, Jennifer C. (OPCL) (JMD); Cardwell, Christine (ODAG) (JMD)
Subject: FW: Stingray Briefing

Duplicative Information - See Document ID 0.7.12327.26619-000004

From: Wood, Alexander W (OPCL)
Subject: Re: As promised
To: Harp, Jennifer C. (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: May 13, 2015 5:21 PM (UTC-04:00)

Thanks. Seems to be the same thing. As Kristi and I discussed today there doesn't appear to be any consistent DOJ public relations message on the use of this technology.

Alexander Wood
Senior Counsel
U.S. Department of Justice
Office of Privacy and Civil Liberties

On May 13, 2015, at 5:15 PM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

Duplicative Information - See Document ID 0.7.12327.21672

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: More stingray emails
To: Moss, Robin (OPCL)
Sent: June 12, 2015 12:53 PM (UTC-04:00)

Thanks Robin. OPCL was trying to obtain this elusive policy from FBI. We found out about from a news article. I think the breach issues are dissipating. I'll send dirtbox now.

From: Moss, Robin (OPCL)
Sent: Friday, June 12, 2015 12:52 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: More stingray emails

Hi Kristi,

Thanks for the "Stingray" documents. I still need the "dirt box" group. Also, in reviewing the group of emails on "Stingray," there was an email from Jenny regarding reviewing draft policy on the Cell-Site technology. Where is that draft policy? I have yet to receive any documentation from Jenny (for the FBI or USMS). Will that briefing package Jenny had from USMS also be included as responsive documents? I know you stated that Erika is swamped with the "breach" matter. Just keep in mind, OIP is waiting for these documents and the 20-day response time has probably been exhausted by now. Thanks.

Robin

From: Lane Scott, Kristi Z (OPCL)
Sent: Thursday, June 11, 2015 2:20 PM
To: Moss, Robin (OPCL)
Subject: More stingray emails

<< Message: FW: Operationalizing the PIA >> << Message: FW: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley >> << Message: FW: Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program | Chuck Grassley >> << Message: Fwd: As promised >> << Message: Re: As promised >>

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: More stingray emails
To: Harp, Jennifer C. (OPCL)
Sent: June 12, 2015 12:54 PM (UTC-04:00)

Hi Jenny,

Can you send Robin any emails that you have regarding Dirtbox or Stingray?

Thanks,

Kristi

From: Moss, Robin (OPCL)
Sent: Friday, June 12, 2015 12:52 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: More stingray emails

Duplicative Information - See Document ID 0.7.12327.26916



From: Wood, Alexander W (OPCL)
Subject: RE: OIP FOIA Search W. Green (DAG/15-01898 (F))
To: Lane Scott, Kristi Z (OPCL); Moss, Robin (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Sent: May 20, 2015 4:00 PM (UTC-04:00)

After talking with Robin it looks the requester made the same exact request to FBI and USMS. The words "stingray" and dirtbox" are used in the request.

I guess we'll see how to proceed after talking with OIP. Thanks, Robin.

Cheers,
Alex

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 20, 2015 3:39 PM
To: Moss, Robin (OPCL)
Cc: Wood, Alexander W (OPCL); Harp, Jennifer C. (OPCL)
Subject: Re: OIP FOIA Search W. Green (DAG/15-01898 (F))

I'd still like to reach out to FBI. Erika has sent official correspondence to (b)(5); (b)(6), (7)(C) per FBI on this subject. Please set up a call for OPCL and OIP for next week. I would like to see the original request and have OIP all of their interpretation in their official memo to OPCL.

Kristi Lane Scott
DOJ/OPCL

On May 20, 2015, at 3:35 PM, Moss, Robin (OPCL) <(b) (6)> wrote:

Kristi,

I contacted OIP and OIP states that for searching, use the exact names for the devices provided by the requester. There was no need for me to reach out to the FBI. Thanks.

Robin

From: Lane Scott, Kristi Z (OPCL)
Sent: Wednesday, May 20, 2015 3:30 PM
To: Wood, Alexander W (OPCL); Moss, Robin (OPCL)
Cc: Harp, Jennifer C. (OPCL)
Subject: Re: OIP FOIA Search W. Green (DAG/15-01898 (F))

Alex,

The requester is referring to Cell Site Simulator technology, which we have asked the FBI to get briefings. Let's get the original request and then we'll set up a call with OIP to determine scope of request. Robin, can you let OIP know we will call them next week? We may need to coordinate with FBI to (b) (5)

Kristi Lane Scott
DOJ/OPCL

On May 20, 2015, at 2:52 PM, Podolskiy, Aleksandr V. (OIP) <(b) (6)> wrote:

Robin,

There is no need to reach out to the FBI for more information. Since the requester is seeking specific systems, the search should be limited to the terms the requester provided.

Thank you for such a quick reply,

Alex

From: Moss, Robin (OPCL)
Sent: Wednesday, May 20, 2015 2:43 PM
To: Podolskiy, Aleksandr V. (OIP)
Cc: Lane Scott, Kristi Z (OPCL)
Subject: RE: OIP FOIA Search W. Green (DAG/15-01898 (F))

Hi Aleksandr,

I've searched the OPCL spreadsheet for tracking incoming IPAs, PIAs, SORNs, etc. and I see nothing with the names of the systems the requester provided. Am I to reach out to the FBI to determine if these systems are under another name or just accept the systems named by the requester? Thanks.

Robin Moss
Privacy Analyst
DOJ/OPCL
NPB, Suite 1000
(b) (6)

From: Podolskiy, Aleksandr V. (OIP)
Sent: Wednesday, May 20, 2015 1:21 PM
To: Moss, Robin (OPCL)
Subject: OIP FOIA Search W. Green (DAG/15-01898 (F))

Dear Robin,

The Office of Information Policy received a Freedom of Information Act request seeking records pertaining to Privacy Impact Assessments submitted by the Federal Bureau of Investigation (FBI) regarding its use of devices known as International Mobile Subscriber Identity (IMSI) catchers. Please see the attached search memorandum and feel free to contact me if you have any questions.

Thank you,

Aleksandr V. Podolskiy
Attorney Advisor
Office of Information Policy

Department of Justice

Phone: (b) (6)

Fax: 202-514-1009

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: FBI NGI privacy documents
To: Brown Lee, Erika (ODAG)
Cc: Chung, Joo (OPCL); Harp, Jennifer C. (OPCL)
Sent: January 8, 2015 6:05 PM (UTC-05:00)

This message has been archived.

Thanks, Erika. Here is a status of the NGI project for your response to (b)(6), (7)(C). If you'd like, we can discuss over the phone tomorrow. It may be important to (b) (5) (b)(5), (b)(6), (7) (b) (5). Also, there are only a few meetings next week. I'll finish out everything on our end.

NGI Privacy Compliance Status

- Civil Retention: Final draft status. You submitted your final review. OPCL will (b) (5)
- Latent and Palm: Final draft status. (b) (5)
- Rap Back: Still under review. (b) (5)
- NGI SORN: (b) (5)
- NGI Facial Recognition PIA: (b) (5)

Thanks,

Kristi

From: Brown Lee, Erika (ODAG)
Sent: Thursday, January 08, 2015 2:58 PM
To: Lane Scott, Kristi Z (OPCL)
Cc: Chung, Joo (OPCL); Harp, Jennifer C. (OPCL)
Subject: RE: FBI NGI privacy documents

Thanks, Kristi. Of course I'm aware that OPCL has been working hard to move forward on all of the PIAs, and I appreciate the tremendous efforts.

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: Thursday, January 08, 2015 2:50 PM
To: Brown Lee, Erika (ODAG)
Cc: Chung, Joo (OPCL); Harp, Jennifer C. (OPCL)
Subject: FW: FBI NGI privacy documents

Erika,

I am working on a timeline of the NGI documents, but we have not been delinquent on NGI privacy PIAs. In fact, we're still waiting for FBI to draft the NGI Facial Recognition PIA, which is the basis of a GAO audit. I suspect my recent ping of (b)(6), (7)(C) per FBI regarding the Stingray briefing may have played a role in the timing of (b)(6), (7)(C) per FBI request. I'll send you the factual update shortly.

Thanks,

Kristi

From: (b)(6), (7)(C) per FBI [mailto:(b)(6), (7)(C), (7)(E) per FBI]
Sent: Thursday, January 08, 2015 1:29 PM
To: Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL)
Cc: (b)(6), (7)(C) per FBI (FBI); (b)(6), (7)(C) per FBI (FBI)
Subject: FBI NGI privacy documents

(b)(6), (7)(C) per FBI have been asked by management to report on the status of your review of these items and any other PIAs. I would appreciate an update. Thank you. (b)(6), (7)(C) per FBI

(b)(6), (7)(C) per FBI

Deputy General Counsel

General Law Branch, Office of the General Counsel

Federal Bureau of Investigation

935 Pennsylvania Ave, NW

Washington, D.C. 20535

(b)(6), (7)(C), (7)(E) per FBI

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling (b)(6), (7)(C), (7)(E) per FBI.

From: Harp, Jennifer C. (OPCL)
Subject: FW: List of pending issues for Erika
To: Lane Scott, Kristi Z (OPCL)
Sent: April 16, 2015 4:29 PM (UTC-04:00)

This message has been archived.

FYI

From: Harp, Jennifer C. (OPCL)
Sent: Wednesday, April 15, 2015 6:59 PM
To: Chung, Joo (OPCL)
Subject: RE: List of pending issues for Erika

Hi Joo,

Here are my updates that come to mind. Please let me know if you have any questions/comments.

Reporting requirements:

Not Responsive

- * USMS Dirtbox program potentially needs a CPCLO response
- * FBI Stingray program still needs to brief the CPCLO

Legislation

Not Responsive

From: Chung, Joo (OPCL)
Sent: Monday, April 13, 2015 10:39 AM
To: Wood, Alexander W (OPCL); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL); Moss, Robin (OPCL)
Subject: RE: List of pending issues for Erika

Also, please include your internal and external working group participation.

From: Chung, Joo (OPCL)

Sent: Monday, April 13, 2015 10:37 AM

To: Wood, Alexander W (OPCL); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL); Moss, Robin (OPCL)

Subject: List of pending issues for Erika

All,

Can you send me a high-level list of outstanding work so that I can prepare a list for Erika.

You should include any work on:

Overview

Reporting requirements

Personnel

Compliance

Training

Oversight

If you have any miscellaneous work, please include this. Please have this to me ASAP. If you are on leave, please have it to me when you get back.

Thanks,

Joo

From: Harp, Jennifer C. (OPCL)
Subject: RE: Dirtbox briefing
To: Lane Scott, Kristi Z (OPCL)
Sent: February 2, 2015 10:54 AM (UTC-05:00)

This message has been archived.

Yep, I've got it. Thanks!

From: Lane Scott, Kristi Z (OPCL)
Sent: Monday, February 02, 2015 10:53 AM
To: Harp, Jennifer C. (OPCL)
Subject: Dirtbox briefing

Hi Jenny,

I sent Christine an email about setting up a date for a Dirtbox briefing. I haven't heard back from her. Can you work with Christine and Ed on a date. We'll need to make arrangements to travel to USMS, where Ed is located.

Thanks,

Kristi

From: Bordley, Ed (USMS) [mailto:(b) (6)]
Sent: Thursday, January 29, 2015 5:10 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: Meeting

That would be great if Erika is willing to do so.

Thanks,

Ed

From: Lane Scott, Kristi Z (OPCL) [mailto:(b) (6)]
Sent: Thursday, January 29, 2015 5:02 PM
To: Bordley, Ed (USMS)
Cc: Cardwell, Christine (ODAG) (JMD)

Subject: FW: Meeting

Happy New Year Ed!

I've copied Erika's assistant, Christine, who can assist us with scheduling. Should we plan on making a trip to your office?

Thanks!

Kristi

From: Bordley, Ed (USMS) [mailto:(b) (6)]
Sent: Wednesday, January 28, 2015 12:36 PM
To: Lane Scott, Kristi Z (OPCL)
Subject: Meeting

Happy New Year Kristi,

I haven't forgotten your request on behalf of Erika for a meeting/briefing regarding USMS use of technology and privacy. Perhaps if you could provide a couple dates in the next two weeks, I could arrange something.

Thanks,

Ed Bordley

Associate General Counsel

U.S. Marshals Service

Washington, DC 20530-1000

(b) (6) (off)

(703) 603-7004 (fax)

From: Harp, Jennifer C. (OPCL)
Subject: RE: USMS Dirtbox Technology
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Sent: March 11, 2015 11:07 AM (UTC-04:00)

This message has been archived.

Yep, here you go.

From: Brown Lee, Erika (ODAG)
Sent: Wednesday, March 11, 2015 10:23 AM
To: Harp, Jennifer C. (OPCL)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Subject: RE: USMS Dirtbox Technology

Jenny – thanks for the links. Can you scan the articles? I can't access the full version of the articles.

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: Tuesday, March 10, 2015 6:29 PM
To: Brown Lee, Erika (ODAG)
Cc: Lane Scott, Kristi Z (OPCL); (b) (6) (OPCL)
Subject: USMS Dirtbox Technology

Duplicative Information - See Document ID 0.7.12327.5060

From: Harp, Jennifer C. (OPCL)
Subject: USMS email
To: Lane Scott, Kristi Z (OPCL)
Sent: November 19, 2014 5:33 PM (UTC-05:00)

This message has been archived.

Hey KLS,

Below is my draft email... it might be helpful if we want to add a suggested timeframe or any other info.

Thanks,
JH

Hi Ed,

Erika Brown Lee, the Chief Privacy and Civil Liberties Officer, is interested in receiving a briefing on the USMS Cessna aircraft "dirtbox" program. Given the recent media attention the program has received, Erika would like to be able to assess the program from a privacy perspective. In particular, she would like more information on the pre-deployment process, how the technology is actually used, what sort of retention policy is in use, and whether USMS believes any privacy documentation would be appropriate. If possible, Joo Chung, Jennifer Harp, and I would also like to attend the briefing.

Thank you so much and please let me know if you have any questions.

Best,

From: Harp, Jennifer C. (OPCL)
Subject: Re: Today
To: Lane Scott, Kristi Z (OPCL)
Sent: May 20, 2015 10:20 AM (UTC-04:00)
Sounds good!

> On May 20, 2015, at 10:10 AM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

>

> Thanks Jenny. I'm hoping they've answered most of the questions. Let me know what you think before sending to them to FBI. We may be at a point to send to Erika.

>

> Kristi Lane Scott

> DOJ/OPCL

>

>

>> On May 20, 2015, at 10:02 AM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

>>

>> Ok, that frees up some time, then. Erika sounded like she wanted the Stingray stuff ASAP (due to the attention the QFRs brought to it), but I'm almost done with a first round summary. If I don't need to update the training materials just yet, I should have 1/2 of Thursday to review FBI's comments on NGI IPS and hopefully send back to them. I'm out on Friday. Can review DM with you on Tuesday (holiday Monday).

>>

>>

>>

>>> On May 20, 2015, at 9:56 AM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

>>>

>>> Don't worry about the Overview or training materials for now. I'll explain to Alex that I want to wait to post until I come back. Andrew doesn't start until June 1 and the interns can read the Overview.

>>>

>>> NGI and DM are our top priorities for now. Did Erika mention when she wanted the FOIA materials? Thanks for everything!

>>>

>>> Kristi Lane Scott

>>> DOJ/OPCL

>>>

>>>

>>>> On May 20, 2015, at 9:51 AM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

>>>>

>>>> Yep, it's #3 on my list. Alex wanted the Overview up by tomorrow; tomorrow I've got to finish the stingray materials for Erika (she wanted me to go through FBI's 26,000 page FOIA response...) and update the training materials for Andrew and Danielle (they start on Tuesday, right?). Will be able to get to NGI IPS next week, but we should read the Data Mining Report as well.

>>>>

>>>> Hope (b) (6)!

>>>>

>>>>

>>>>

>>>>> On May 20, 2015, at 9:38 AM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

>>>>>

>>>>> No worries! These things can be tricky when sending to the group. We'll get you set up when we get back. You have to watch a video in LMS and sign an agreement. I'll also get you a laptop.

>>>>>

>>>>> If you get a chance this week, can you work on the NGI/IPS PIA? I hope everything is well. I'll talk

to you soon:)

>>>>>

>>>>> Thanks!

>>>>>

>>>>> Kristi Lane Scott

>>>>> DOJ/OPCL

>>>>>

>>>>>

>>>>>> On May 20, 2015, at 9:30 AM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

>>>>>>

>>>>>> Ahh ok, sorry. It was just a one-time thing since I'm hand-reading the document. Happy to head to the office now instead if it'd be better! Just let me know.

>>>>>>

>>>>>>

>>>>>>

>>>>>>> On May 20, 2015, at 9:23 AM, Lane Scott, Kristi Z (OPCL) <(b) (6)> wrote:

>>>>>>>

>>>>>>> Hi Jenny,

>>>>>>>

>>>>>>> When we get back, we have to do a telework agreement. We have to have that in place first. Next time, just send me an email before sending the group the telework email.

>>>>>>>

>>>>>>> Thanks!

>>>>>>>

>>>>>>> Kristi Lane Scott

>>>>>>> DOJ/OPCL

>>>>>>>

>>>>>>>

>>>>>>>> On May 20, 2015, at 8:31 AM, Harp, Jennifer C. (OPCL) <(b) (6)> wrote:

>>>>>>>>

>>>>>>>> Hi all,

>>>>>>>>

>>>>>>>> I'll be teleworking today to work on editing the Overview. Please call/email me if you need anything!

>>>>>>>>

>>>>>>>> -Jenny

From: Harp, Jennifer C. (OPCL)
Subject: FW: As promised
To: Moss, Robin (OPCL)
Cc: Lane Scott, Kristi Z (OPCL)
Sent: June 12, 2015 1:56 PM (UTC-04:00)
Attached: DRAFT - DOJ Cell-Site Simulator Policy -5-6-15 (2).docx

Hi Robin,

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

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

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

Best,
Erika

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

From: Tyrangiel, Elana (OLP)
Sent: Thursday, May 07, 2015 9:31 AM
To: Brown Lee, Erika (ODAG)
Subject: As promised

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

From: Lane Scott, Kristi Z (OPCL)
Subject: FW: Green FOIA Requests (Stingray and Dirtbox)
To: Brown Lee, Erika (ODAG)
Cc: Moss, Robin (OPCL); Harp, Jennifer C. (OPCL)
Sent: June 12, 2015 6:23 PM (UTC-04:00)
Hi Erika,

Since the FOIA clock is running, can you run a search on your email for the following search terms:

- Cell site
- Stingray
- Dirtbox

We can answer any questions you may have regarding this search.

Thanks,

Kristi

From: Moss, Robin (OPCL)
Sent: Thursday, June 04, 2015 2:58 PM
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Subject: FW: Green FOIA Requests

Hi Ladies,

I know you have been swamped with other matters, but I need any documents you have subject to this FOIA Request. Kristi, I also need any documents Erika may have. Thanks.

Robin

From: Moss, Robin (OPCL)
Sent: Tuesday, May 26, 2015 4:03 PM
To: Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Subject: Green FOIA Requests

Hi Kristi/Jenny,

I have established a folder on the G:drive under FOIA Request for Mr. Green's requests. Any documents you may have concerning his requests can be copied to this folder. I will then copy the documents for each FOIA Request. Kristi, if you have not yet done so, as per the conference call, you should contact Erika and have her download her information to the folder as well. However, if she feels copying them and forwarding to OPCL via mail is what she would like to do, that is fine too. Thanks.

Robin

From: Brown Lee, Erika (ODAG)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)
To: Lane Scott, Kristi Z (OPCL)
Cc: Moss, Robin (OPCL); Harp, Jennifer C. (OPCL)
Sent: June 12, 2015 6:28 PM (UTC-04:00)

Thanks for the reminder, Kristi. Will do.

Have a great weekend, all!

Erika Brown Lee

***Chief Privacy and Civil Liberties Officer and
Associate Deputy Attorney General***

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: Friday, June 12, 2015 6:23 PM
To: Brown Lee, Erika (ODAG)
Cc: Moss, Robin (OPCL); Harp, Jennifer C. (OPCL)
Subject: FW: Green FOIA Requests (Stingray and Dirtbox)

Duplicative Information - See Document ID 0.7.12327.5473

From: Brown Lee, Erika (ODAG)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)
To: Lane Scott, Kristi Z (OPCL)
Sent: June 15, 2015 9:45 AM (UTC-04:00)

Hi Kristi – I have a few questions. Can you give me a call when you a chance?

Thanks,
Erika

Erika Brown Lee
Chief Privacy and Civil Liberties Officer and
Associate Deputy Attorney General

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: Friday, June 12, 2015 6:23 PM
To: Brown Lee, Erika (ODAG)
Cc: Moss, Robin (OPCL); Harp, Jennifer C. (OPCL)
Subject: FW: Green FOIA Requests (Stingray and Dirtbox)

Duplicative Information - See Document ID 0.7.12327.5473

From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)
To: Brown Lee, Erika (ODAG)
Sent: June 15, 2015 9:54 AM (UTC-04:00)

Of course. I'll call you in 10 minutes.

From: Brown Lee, Erika (ODAG)
Sent: Monday, June 15, 2015 9:45 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)

Duplicative Information - See Document ID 0.7.12327.5477



From: Lane Scott, Kristi Z (OPCL)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)
To: Brown Lee, Erika (ODAG)
Sent: June 15, 2015 10:13 AM (UTC-04:00)
Erika,

Robin is out today. Robin works closely with OIP on these matters. It may be helpful to have her participate in our discussion. I'll send out a meeting invitation for tomorrow.

Thanks,

Kristi

From: Brown Lee, Erika (ODAG)
Sent: Monday, June 15, 2015 9:45 AM
To: Lane Scott, Kristi Z (OPCL)
Subject: RE: Green FOIA Requests (Stingray and Dirtbox)

Duplicative Information - See Document ID 0.7.12327.5477



From: Fried, Hannah (OLP)
Subject: Re: Stingray question
To: Brown Lee, Erika (ODAG)
Sent: June 17, 2015 3:22 PM (UTC-04:00)

Sounds good - thank you.

On Jun 17, 2015, at 3:16 PM, Brown Lee, Erika (ODAG) <(b) (6)> wrote:

Hi Hannah - I'm in meetings here and out of the bldg through 6, but will try to give you a call in-between or afterwards.

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)

On Jun 17, 2015, at 2:21 PM, Fried, Hannah (OLP) <(b) (6)> wrote:

Hey Erika,

Just tried to catch you at your desk – would you give me a buzz when you have a second?
This is re Stingray. I'm going to be away from my desk for some portion of the afternoon,
but my cell is (b) (6) .

Thanks,
Hannah

From: Brown Lee, Erika (ODAG)
Subject: RE: Stingray memo
To: Fried, Hannah (OLP)
Sent: June 18, 2015 2:25 PM (UTC-04:00)

Thanks, Hannah. I don't have any issues with the added text below.

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: Fried, Hannah (OLP)
Sent: Thursday, June 18, 2015 11:57 AM
To: Brown Lee, Erika (ODAG)
Subject: RE: Stingray memo

Hey again, Erika,

To follow up on this – we decided to make one small tweak to this section. I don't think that's going to change your analysis, but here it is, for completeness (change in red font):

IMPROPER USE OF CELL-SITE SIMULATORS

(b) (5)

Any questions, concerns -- let me know.

Thanks

From: Fried, Hannah (OLP)
Sent: Wednesday, June 17, 2015 9:35 PM
To: Brown Lee, Erika (ODAG)
Subject: Stingray memo

Hey Erika,

Thanks for checking in earlier. The section we were discussing is (b) (5)
Let me know if you have any concerns or questions about it.

Thanks,
Hannah

From: Fried, Hannah (OLP)
Subject: FW: Stingray memo
To: Tyrangiel, Elana (OLP)
Sent: June 18, 2015 2:26 PM (UTC-04:00)

FYI – Erika is all good on the (b) (5) section of the draft policy

From: Brown Lee, Erika (ODAG)
Sent: Thursday, June 18, 2015 2:25 PM
To: Fried, Hannah (OLP)
Subject: RE: Stingray memo

Duplicative Information - See Document ID 0.7.12327.5508



From: Fried, Hannah (OLP)
Subject: RE: Stingray memo
To: Brown Lee, Erika (ODAG)
Sent: June 18, 2015 3:48 PM (UTC-04:00)

Thanks, appreciate it.

From: Brown Lee, Erika (ODAG)
Sent: Thursday, June 18, 2015 2:25 PM
To: Fried, Hannah (OLP)
Subject: RE: Stingray memo

Duplicative Information - See Document ID 0.7.12327.5508

From: Harp, Jennifer C. (OPCL)
Subject: FW: cell site simulator
To: Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL)
Sent: June 18, 2015 5:17 PM (UTC-04:00)
Attached: PAG -- Cell Site Simulators (4-29-2015).docx

FYI; not sure if either of you have seen this...

From: Lumpkin, Beverley (OPA)
Sent: Thursday, June 18, 2015 5:16 PM
To: Harp, Jennifer C. (OPCL)
Subject: FW: cell site simulator

Fyi, this is something the FBI uses internally to brief on the subject. Although the info may be provided to reporters orally, the actual paper is not passed on. This is what the Bureau calls "guidance" as opposed to a "release"! I did promise the OPA that we would not use it externally, but thought you'd like to see.

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.¹

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").² 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:

¹ 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.

² 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

From: Grooms, Daniel (ODAG)
Subject: FW: Stingray Policy
To: Gauhar, Tashina (ODAG)
Sent: June 25, 2015 5:34 PM (UTC-04:00)
Attached: Memo for the DAG - DOJ Stingray policy 6 23 2015.docx, DRAFT 6-23 redlines
- DOJ Cell-Site Simulator Policy.docx

Forwarding to you for awareness on the (b) (5) .

From: Jain, Samir (ODAG)
Sent: Thursday, June 25, 2015 5:33 PM
To: Brown Lee, Erika (ODAG); Bonilla, Armando (ODAG); Lan, Iris (ODAG); Grooms, Daniel (ODAG); Goldsmith, Andrew (ODAG); Ferber, Scott (ODAG); Hulsey, G. Scott (ODAG)
Subject: FW: Stingray Policy

All,

Attached is the current draft of the policy, as well as a draft cover memo from OLP. This will be going to the DAG probably early next week (with a couple of issues left for her to resolve as described in the cover memo). Let me know if you have any concerns/issues other than those that will already be teed up. Thanks!

From: Gauhar, Tashina (ODAG)
Subject: FW: Stingray Policy
To: Evans, Stuart (NSD)
Sent: June 25, 2015 9:32 PM (UTC-04:00)
Attached: Memo for the DAG - DOJ Stingray policy 6 23 2015.docx, DRAFT 6-23 redlines
- DOJ Cell-Site Simulator Policy.docx

Wanted to make sure you had visibility on this. The memos are attached below, but the important part is the scope which is described in the cover memo (found on the last page) and copied below. Let me know if you have any concerns. Thanks.

(b)(5) per FBI

(b)(5) per FBI

(b)(5) per FBI

(b)(5) per FBI

From: Grooms, Daniel (ODAG)
Sent: Thursday, June 25, 2015 5:34 PM
To: Gauhar, Tashina (ODAG)
Subject: FW: Stingray Policy

Duplicative Information - See Document ID 0.7.12327.15276

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*

June 3, 2015

The Honorable Loretta E. Lynch
Attorney General
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Attorney General Lynch and Director Comey:

In light of recent reports of the Federal Bureau of Investigation conducting aerial surveillance above American cities, I write to you to request additional information about these programs. Many Americans have been troubled by these reports, and as ranking member of the Senate Judiciary Subcommittee on Privacy, Technology and the Law, I believe it is important to ensure that these programs adequately protect Americans' privacy while furthering public safety and national security.

Yesterday, a report by the Associated Press ("FBI behind mysterious surveillance aircraft over US cities") revealed that the FBI is flying aircraft equipped with surveillance or monitoring equipment over the United States. The AP described the Bureau's practice of using low-flying planes carrying video and cell phone surveillance technology to assist in ongoing investigations. According to the report, over a 30-day period, the FBI deployed aircraft above more than 30 cities in 11 states. This revelation follows reports of small, fixed-wing aircraft circling highly populated areas of the Twin Cities in my state of Minnesota, including downtown Minneapolis, the Mall of America, and Southdale Center.

I wrote to former Attorney General Holder in November 2014 to express concern about the Department of Justice's collection of Americans' cell phone data from aircraft. Other senators wrote similar letters requesting additional information. At the time, reports described the Department's use of wireless surveillance systems, known as International Mobile Subscriber Identity Catcher devices (IMSI-catchers), "DRTBoxes," "dirtboxes," or "Stingrays," which have the ability to impersonate cellular phone towers and compel affected mobile phones to reveal their location and users' registration information. I cautioned that the need for law enforcement to monitor and apprehend criminal suspects should not come at the expense of innocent Americans' privacy.

Since my initial letter requesting additional information on the topic, the FBI has provided lawmakers with some clarity regarding the legal process the Bureau requires before deploying wireless surveillance, and explained that Bureau policy requires that the FBI obtain a warrant prior to using technology capable of impersonating a cell phone tower. However, the extent to which those same processes extend to aerial surveillance more broadly remains unclear.

In light of the Bureau's apparent increase in its use of aerial surveillance, I request that you provide greater detail about the FBI's policies regarding its use. I also request that you provide detailed written answers to the following questions:

1. What technologies are used by the FBI during the course of aerial surveillance? To what extent does the FBI use IMSI-catchers, "DRTBoxes," "dirtboxes," or "Stingrays"? To what extent does the FBI use infrared cameras? To what extent does the FBI use video cameras?
2. How frequently does the FBI engage in aerial surveillance that utilizes IMSI-catchers, infrared cameras, or video technology? In what types of operations does the FBI deploy aerial surveillance utilizing these technologies? More generally, under what circumstances is aerial surveillance using these technologies deployed?
3. Under what legal authority is the FBI acting when conducting aerial surveillance, including aerial surveillance that utilizes IMSI-catchers, infrared cameras, or video technology? To the extent that the Department of Justice is seeking court approval before deploying any of these technologies during aerial surveillance, is this done on a case-by-case basis or does the Department seek broader authorization? What are judges told about how the technologies deployed work, and the potential impact on innocent Americans? Please provide a representative sample of the applications for these court orders.
4. To the extent that the Department of Justice has developed policies governing the use of IMSI-catchers, infrared cameras, or video technology during aerial surveillance, please identify the policies and legal processes used. Are different technologies subject to different policies or forms of legal process? If so, please describe the application of these policies.
5. Has the Department of Justice developed policies on the retention of data collected in the course of aerial surveillance that utilizes IMSI-catchers, infrared cameras, or video technology? Has the Department developed policies on the destruction of that data? If so, please describe these policies.
6. How many individuals can be detected, tracked, and/or monitored during each surveillance flight? If IMSI-catchers are being used, how many phones can be detected, tracked, and/or monitored during each flight?
7. Reports indicate that some of 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 the FBI's aerial surveillance?
8. To the extent that aerial surveillance has been deployed above large public gatherings, what steps is the government taking to ensure that such surveillance does not chill constitutionally protected conduct, such as political and religious activity?

9. Has the Department of Justice's Office of Privacy and Civil Liberties conducted a privacy impact assessment or otherwise reviewed the use of technologies utilized during aerial surveillance? Has a review or privacy impact assessment been conducted on the FBI's use of aerial surveillance more broadly? If so, please provide copies of such assessments or reviews.
10. What safeguards are in place to ensure that innocent American's privacy is protected during aerial surveillance utilizing technology that collects data and personal information?

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

Sincerely,



Senator Al Franken
Ranking Member, Subcommittee on
Privacy, Technology and the Law

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINOSEY O. CHAMBERS, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA
DAVID VITTER, LOUISIANA
DAVID A. PERDUE, GEORGIA
THOM TILLES, 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. LUNDGREN, Democratic Chief Counsel and Staff Director

June 1, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Comey:

According to *The Washington Post*, two airplanes were spotted flying in circles over parts of West Baltimore for several days last month, following the riots concerning the death of Freddie Gray.¹ The Federal Bureau of Investigation (FBI) reportedly confirmed that it made planes available to the Baltimore Police Department for the purpose of "providing aerial imagery of possible criminal activity," but that the FBI did not use cell-site simulators in any operation pertaining to the riots in Baltimore.²

Other reports have alleged that similar flights have been spotted in Chicago, Boston, California, and the Twin Cities.³ Please have knowledgeable FBI staff provide a briefing to Committee staff on this matter no later than June 12, 2015. Specifically, I would like to know (1) the scope, nature, and purpose of these operations; (2) what types of surveillance equipment were used in the operations, if not cell-site simulators; and (3) what legal authorities, if any, are being relied upon in carrying out these operations.

Should you have any questions, please contact Jay Lim of my Committee staff at (b) (6).
(b) (6) Thank you for your cooperation in this important matter.

Sincerely,



Charles E. Grassley
Chairman

¹ Craig Timberg, "Surveillance planes spotted in the sky for days after West Baltimore rioting," *The Washington Post*, May 5, 2015.

² *Id.*

³ Matt McKinney and John Rienan, "Mysterious low-flying plane over Twin Cities raises questions of surveillance. Small aircraft circled downtown Minneapolis, 2 malls for hours," *StarTribune*, May 29, 2015; Kit O'Connell, "Department of Justice Flying Secret Airplane Fleet Over American Cities," *Mint Press News*, May 27, 2015.

From: Lumpkin, Beverley (OPA)
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap
To: (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; Richards, Steven ((b)(6) per DHS); frank.baitman@hhs.gov; Alexander W Joel (b)(3), (b)(6) per ODN; Schwartz, Ari ((b)(6)); Heinzelman, Kate ((b)(6)); Prieto, Daniel ((b)(6)); Martz, Stephanie ((b)(6)); Fonzone, Christopher ((b)(6)); Petrila, Jim ((b)(6))
Cc: Zarek, Corinna
Sent: July 6, 2015 11:55 AM (UTC-04:00)
Attached: NAP Submissions Template.docx

Thank you so much for participating in our call Thursday afternoon. I know you all have a lot on your plate and I particularly appreciate your taking the time right before the holiday weekend. FYI, I am copying those on our Privacy group, since these topics are so often intertwined.

Again, our goal is to develop ambitious, relevant, specific and measurable goals for whistleblower policy to be included in our third National Action Plan. Attached is the submissions template which we would appreciate your using when submitting your ideas.

We will hold a meeting with civil society representatives on **Monday July 20th, from 1pm to 2pm**, in the Adams Room on the 2nd floor of the National Archives building, which you should enter at the Special Events Entrance at 7th & Constitution Ave., N.W.

During our call last Thursday, several of you noted that the civil society Model Action Plan, (b)(5), (7)(E) per DHS

(b)(6) per NSD (b)(5)
(b)(5), (7)(E) per DHS (b)(5) per NSD; (b)(5), (7)(E) per DHS
(b)(5) per NSD; (b)(5), (7)(E) per DHS (b)(5), (7)(E) per DHS

FBI and DOJ criminal policy people (CRM and OLP) need to be brought onboard, as well as DHS. There was concern that so many different equities are involved that it would be difficult to come up with something by 8/1.

Alex Joel of ODN said that an interagency group has been working on a high-level plan on Principles of Intelligence Transparency that will be presented to Director Clapper on 8/1. (b)(5) per DHS

(b)(5) per NSD; (b)(5), (7)(E) per DHS
(b)(5), (7)(E) per DHS

I pushed for (b) (5) [REDACTED]
[REDACTED]. Jenny of DOJ/OPCL said perhaps we can have explain why we do certain things and why it is important.

Jenny noted that there are a lot of policy issues involved in publishing PIAs, and there would be a need to coordinate with the FBI, but she thought there could be “some form of transparency” in posting PIAs online.

Another idea floated was (b) (5) [REDACTED]
[REDACTED]
[REDACTED].

Jenny pointed out that there is a PIA in the works on the use of UAVs and she will reach out to CRM and OLP.

(b)(6) per NSD added later that she and Jenny would set up a meeting with DEA, FBI, Marshals, ATF and other relevant law enforcement parties to discuss possibilities.

I am hopeful that some of these admittedly vague ideas can be firmed up into positive commitments by August 1st. Again, thank you for participating, and please feel free to contact me with any comments or concerns, especially if you feel I have left anything out or misconstrued anything.

Beverley

Beverley Lumpkin
Public Affairs
Open Government Working Group
US Department of Justice

(b) (6) [REDACTED]

From: Harp, Jennifer C. (OPCL)
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap
To: Lane Scott, Kristi Z (OPCL)
Sent: July 6, 2015 5:31 PM (UTC-04:00)

From: Harp, Jennifer C. (OPCL)
Sent: Monday, July 06, 2015 4:21 PM
To: Lumpkin, Beverley (OPA)
Subject: RE: NAP 3.0 // Surveillance Conference Call Recap

Hi Beverley,

I spoke with Erika today about the NAP 3.0 call. She apologized for not being able to be on it- she was at a meeting at the White House. She has some questions/concerns and was wondering if you and I could have a call with her this week to discuss. Are you available any time Thursday morning? She is also interested in speaking to Cori from the White House later this week.

Thanks,
Jenny

From: Lumpkin, Beverley (OPA)
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); 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; Richards, Steven ((b)(6) per DHS); frank.baitman@hhs.gov; Alexander W Joel ((b)(3), (b)(6) per ODNI); (b)(3), (b)(6) per ODNI; Schwartz, Ari ((b)(6)); Heinzelman, Kate ((b)(6)); Prieto, Daniel ((b)(6)); Martz, Stephanie ((b)(6)); Fonzone, Christopher ((b)(6)); Pettila, Jim ((b)(6))
Cc: Zarek, Corinna
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap

<< File: NAP Submissions Template.docx >>

Duplicative Information - See Document ID 0.7.12327.5542



Hi (b)(6) per NSD,

From: "Lumpkin, Beverley (OPA)" <(b) (6)>
Date: July 6, 2015 at 11:55:08 AM EDT
To: (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 NSA (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)>,
(b)(6) per DHS, "Richards, Steven
(b)(6) per DHS, "frank.baitman@hhs.gov"
<frank.baitman@hhs.gov>, "Alexander W Joel (b)(3), (b)(6) per ODN
(b)(3), (b)(6) per ODN, "Schwartz, Ari
(b) (6), "Heinzelman, Kate
(b) (6), "Prieto, Daniel
(b) (6), "Martz, Stephanie
(b) (6), "Fonzone, Christopher
(b) (6), "Petrila, Jim
(b) (6)
Cc: "Zarek, Corinna" <(b) (6)>
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5542

From: Harp, Jennifer C. (OPCL)
Subject: RE: NAP 3.0 // Surveillance Conference Call Recap
To: (b)(6) per NSD (NSD); Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL)
Sent: July 9, 2015 11:39 AM (UTC-04:00)

Thanks, (b)(6) per NSD. We did speak with Beverley and the White House and got some good clarification on expectations. No decisions were made, but we will keep you updated.

From: (b)(6) per NSD (NSD)
Sent: Thursday, July 09, 2015 10:42 AM
To: Brown Lee, Erika (ODAG); Lane Scott, Kristi Z (OPCL); Harp, Jennifer C. (OPCL)
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap

Hi – just checking in to see if you were able to discuss with Beverley and the White House. I am available to participate in an internal DOJ meeting to discuss options either this week or next. Please advise regarding next steps.

Many thanks,

(b)(6) per NSD

From: Lumpkin, Beverley (OPA)
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); 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; Richards, Steven (b)(6) per DHS; frank.baitman@hhs.gov; Alexander W Joel (b)(3), (b)(6) per ODNI; (b)(3), (b)(6) per ODNI; Schwartz, Ari (b)(6); Heinzelman, Kate (b)(6); Prieto, Daniel (b)(6); Martz, Stephanie (b)(6); Fonzone, Christopher (b)(6); Petrila, Jim (b)(6)
Cc: Zarek, Corinna
Subject: FW: NAP 3.0 // Surveillance Conference Call Recap

Duplicative Information - See Document ID 0.7.12327.5542