PATRICK J. LEAHY, VERMONT, CHAIRMAN

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

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

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

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

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?

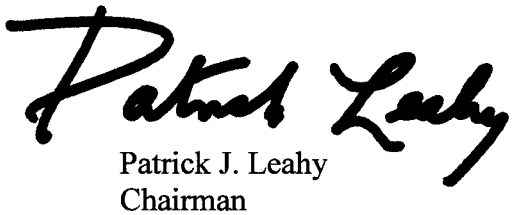
5. What is the policy of these agencies regarding the legal process needed for use of cell-site simulators?
    a. Are these agencies seeking search warrants specific to the use of cell-site simulators?
    b. If not, what legal authorities are they using?
    c. Do these agencies make use of public 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 (202) 224-7703, or Jay Lim at (202) 224-5225.

Sincerely,



Patrick J. Leahy
Chairman

Charles E. Grassley
Ranking Member