

that works to inform policymakers and the general public about civil liberties issues related to technology and to act as a defender of those liberties. In support of its mission, EFF uses the FOIA to obtain and disseminate information concerning the activities of federal agencies.

3. Defendant Department of Justice (DOJ) is a Department of the Executive Branch of the United States Government. DOJ is an “agency” within the meaning of 5 U.S.C. § 552(f). The Federal Bureau of Investigation (FBI), U.S. Marshals Service (USMS), and DOJ Criminal Division are components of Defendant DOJ.

JURISDICTION AND VENUE

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

5. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1391(e).

FACTUAL ALLEGATIONS

U.S. Marshals Have Operated Small Aircraft Equipped with Receivers to Gather Americans’ Cell Phone Data Since 2007

6. On November 13, 2014, the *Wall Street Journal* reported that the USMS has been using small, fixed-wing Cessna aircraft equipped with receivers that act like cellphone towers to gather data from cellphones being used on the ground.¹ According to the *Journal*, USMS has, since 2007, flown small “aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population.”²

7. The USMS program is aimed at finding criminal suspects, but the article also notes that the USMS deploys the technology on targets as requested by other parts of the

¹ Devlin Barrett, “Americans’ Cellphones Targeted in Secret U.S. Spy Program,” *Wall St. J.* (Nov. 13, 2014), <http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>.

² *Id.*

Justice Department.³

8. The devices mounted on the aircraft appear to be IMSI catchers, also called “stingrays,”⁴ in that they “emulate a cellular base station to attract cellphones for a registration process even when [the phones] are not in use.”⁵ According to the *Journal*, they are sometimes called “dirtboxes” for the acronym of the company that manufactures the device—DRT, for Digital Receiver Technology, Inc. DRT is now a subsidiary of Boeing. The devices are capable of collecting identification and location data from “tens of thousands of cellphones in a single flight.”⁶ According to an unnamed source quoted in the article, the device “determines which phones belong to suspects and ‘lets go’ of the non-suspect phones.” Some similar devices are able to “jam signals and retrieve data from a target phone such as texts or photos.”⁷

9. According to the *Journal*’s sources, some within the DOJ have questioned the legality of these operations as well as the program’s internal safeguards.⁸

10. Immediately after the *Journal* reported on the USMS program, many other national and international news organizations also reported on the story.⁹

³ *Id.*

⁴ See <https://en.wikipedia.org/wiki/IMSI-catcher>. IMSI stands for “International Mobile Subscriber Identity.” A well-known and commonly used IMSI catcher is called a “Stingray.” See ACLU, *Stingray Tracking Devices: Who’s Got Them?* <https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them>.

⁵ Barrett, “Americans’ Cellphones Targeted in Secret U.S. Spy Program.”

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ See, e.g., Megan Geuss, “Feds gather phone data from the sky with aircraft mimicking cell towers,” *ArsTechnica* (Nov. 13, 2014) <http://arstechnica.com/tech-policy/2014/11/feds-gather-phone-data-from-the-sky-with-aircraft-mimicking-cell-towers/>; Kim Zetter, “The Feds Are Now Using ‘Stingrays’ in Planes to Spy on Our Phone Calls,” *Wired* (Nov. 14, 2014), <http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/>; Gail Sullivan, “Report: Secret government program uses aircraft for mass cellphone surveillance,” *Washington Post* (Nov. 14, 2014), <http://www.washingtonpost.com/news/morning-mix/wp/2014/11/14/report-secret-government-program-uses-aircraft-for-mass-cellphone-surveillance/>; Trevor Timm, “First Snowden. Then tracking you on wheels. Now spies on a plane. Yes, surveillance is everywhere,” *The Guardian* (Nov. 15, 2014) <http://www.theguardian.com/commentisfree/2014/nov/15/spies-plane-surveillance-us-marshals>.

Secrecy and Controversy Over IMSI Catchers and Dirtboxes

11. In recent years, there has been increasing interest and press coverage in law enforcement use of IMSI catchers, but much secrecy still surrounds their use.¹⁰ In the last few years, the federal government—including the FBI, DOJ and USMS—has tried to hide the use of this technology from public view—whether through nondisclosure agreements with state and local law enforcement agencies,¹¹ by seizing records held by those agencies,¹² or by withholding key pieces of information about the technology from judges and criminal defendants.¹³

12. Because of the secrecy surrounding the technology and the questionable legality of its use, law enforcement use of IMSI catchers has become increasingly controversial.¹⁴ Instead of requiring law enforcement to ask a cell phone carrier for access to cell phone data—and present that carrier with a court-authorized warrant for that data—IMSI catchers allow law enforcement to obtain the same data in secret and with no judicial oversight. Already several courts and judges—once they were informed of the government’s use of an IMSI catcher in a

¹⁰ See, e.g., CJ Ciaramella, “How the Justice Department Keeps Its Cell Phone Snooping a Secret,” *Vice* (June 18, 2014) <https://news.vice.com/article/how-the-justice-department-keeps-its-cell-phone-snooping-a-secret>; John Kelly, “Cellphone data spying: It’s not just the NSA,” *USA Today* (June 13, 2014) <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/>.

¹¹ Shawn Musgrave, “Before they could track cell phone data, police had to sign a NDA with the FBI,” *MuckRock* (Sept. 22, 2014) <https://www.muckrock.com/news/archives/2014/sep/22/they-could-track-cell-phone-data-police-had-sign-n/>

¹² Kim Zetter, “U.S. Marshals Seize Cops’ Spying Records to Keep Them From the ACLU,” *Wired* (June 3, 2014) <http://www.wired.com/2014/06/feds-seize-stingray-documents/>.

¹³ See <https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-isnt-warrant> (discussing documents received through FOIA); Cyrus Farivar, “Judges impose rare, stricter requirement for “stingray” use by police,” *ArsTechnica* (Nov. 17, 2014) <http://arstechnica.com/tech-policy/2014/11/judges-impose-rare-stricter-requirement-for-stingray-use-by-police/>.

¹⁴ See, e.g., John Kelly, “Cellphone data spying: It’s not just the NSA,” *USA Today* (June 13, 2014), <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/>; Nathan Wessler, “Police Hide Use of Cell Phone Tracker From Courts Because Manufacturer Asked,” *ACLU* (March 3, 2014) <https://www.aclu.org/blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because>; Shawn Musgrave, “Before they could track cell phone data, police had to sign a NDA with the FBI,” *MuckRock* (Sept. 22, 2014) <https://www.muckrock.com/news/archives/2014/sep/22/they-could-track-cell-phone-data-police-had-sign-n/>.

case—have demanded greater transparency and accountability for that device’s use.¹⁵

13. Meanwhile, the *Wall Street Journal* article from November 2014 was the first ever to report on USMS and DOJ’s use of this technology in conjunction with aircraft. The article notes the broad sweep of DOJ’s use of this technology—specifically that USMS’s Cessnas have a “flying range covering most of the U.S. population,” and despite the fact that nearly all Americans may be affected by DOJ’s use of this technology, there is little to no other information available to the public on what data is collected and how it is used.

14. In response to the *Journal* article, members of Congress have called on DOJ to provide more information about its use of this technology and expressed significant concerns about the privacy interests of individuals whose cell phone data is collected.¹⁶

Plaintiff’s FOIA Requests and Requests for Expedited Processing

15. In a letter dated November 20, 2014 and sent by e-mail to the DOJ, FBI and DOJ Criminal Division, and a letter also dated November 20, 2014 and sent by e-mail to USMS, Plaintiff requested under the FOIA all records, including but not limited to electronic records, generated between January 1, 2007 and the present concerning “dirtboxes” or other IMSI catcher devices operated from planes including:

- a. the case name or docket numbers of all criminal cases, federal or state, open or closed, in which data collected from a device aided in arrest;
- b. Any and all records detailing [Defendant and its components’] use of these devices and data collected from these devices, including but not limited to:

¹⁵ See <https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-isnt-warrant> (discussing documents received through FOIA); Cyrus Farivar, “Judges impose rare, stricter requirement for “stingray” use by police,” *Ars Technica* (Nov. 17, 2014) <http://arstechnica.com/tech-policy/2014/11/judges-impose-rare-stricter-requirement-for-stingray-use-by-police/>.

¹⁶ Letter from Senators Charles Grassley and Patrick Leahy to Eric Holder and Jeh Johnson (Dec. 23, 2014), <http://www.grassley.senate.gov/sites/default/files/news/upload/2014-12-23%20PJL%20and%20CEG%20to%20DOJ%20and%20DHS%20%28cell-site%20simulators%29.pdf>; Letter from Senator Al Franken to Eric Holder (Nov. 18, 2014), <http://www.franken.senate.gov/files/letter/141118%20DOJ%20Cellphone%20Dat.pdf>; Letter from Senator Edward Markey to Eric Holder (Nov. 14, 2014) http://www.markey.senate.gov/imo/media/doc/2014-11-14_DOJ_Surveillance.pdf.

- i. logs of who, when and why the devices were used;
 - ii. any and all communications between [Defendant and its components] and other federal and/or state agencies concerning the devices, including requests from [the Defendant and its components] or other federal and/or state agencies for USMS to use the devices to collect data on their behalf;
 - iii. records discussing legal protocols or standards for using the devices;
 - iv. model or sample requests for subpoenas, court orders or warrants to use the devices and/or model or sample affidavits in support of legal requests to use the devices;
 - v. policies and procedures for using the devices—including agency protocol or standards for approving use of the devices—and for storing, accessing and sharing data collected by the devices;
 - vi. policies and procedures for deleting data collected using the devices;
 - vii. geographic locations and/or metropolitan areas where the devices have been deployed;
- c. records discussing how many phones a device may collect data from during a given flight, including how many phones are specifically targeted during a flight, how many phones are not specifically targeted but still have data collected from them; and how many “non-suspect phones” are “let go” by the device;
 - d. training and promotional records and materials, including presentations, memoranda, policies and guidelines concerning use of the devices, whether produced or created by a federal agency, or produced, created or received from some other third party, including the device manufacturer;
 - e. records describing the types of data collected by the devices and whether the devices are used to jam signals and/or retrieve data from a target phone such as texts or photos;

- f. contracts, service agreements or memoranda of understanding concerning the devices between [the Defendant and its components] and the device manufacturer or between [Defendant and its components] and any other federal or state agency;
- g. all Privacy Impact Assessments, System of Records Notices or other similar documents concerning the collection and use of data using the devices;
- h. procedures or protocol concerning data collected using the devices from cell phones or cell phone users that are not the target of an investigation;
- i. communications discussing the legality of operations using the devices as well as internal safeguards; and
- j. communications with Congress concerning the devices.

16. In its November 20 letters, Plaintiff also formally requested that the processing of these requests be expedited because they pertain to information about which there is “[a]n urgency to inform the public about an actual or alleged federal government activity,” and were “made by a person primarily engaged in disseminating information.” 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(d)(1)(ii).

17. The DOJ acknowledged Plaintiff’s request via a letter dated November 21, 2014. The DOJ assigned Plaintiff’s request tracking number EMRUFOIA112014-8. The DOJ advised Plaintiff it had referred Plaintiff’s request to the USMS.

18. The USMS acknowledged Plaintiff’s request via a letter dated November 24, 2014 and stated it had begun a search for responsive records. The USMS assigned Plaintiff’s request tracking number 2015USMS27189.

19. The FBI acknowledged Plaintiff’s request via an e-mail dated November 24, 2014.

20. To date, Defendant and its components have not produced any documents in response to Plaintiff’s request described in paragraph 15 nor informed Plaintiff of an anticipated date for the completion of the processing of the requests.

21. Not only have Defendant and its components failed to expedite the processing of Plaintiff's requests, but it has also exceeded the generally applicable twenty-day deadline for the processing of *any* FOIA request.

22. Plaintiff has exhausted the applicable administrative remedies with respect to all of its FOIA requests referenced herein.

23. Defendant has wrongfully withheld the requested records from Plaintiff.

CAUSES OF ACTION

Violation of the Freedom of Information Act for Failure to Expedite Processing

24. Plaintiff repeats and realleges paragraphs 1-23.

25. Defendant has violated the FOIA by failing to expedite the processing of Plaintiff's FOIA requests.

26. Plaintiff has exhausted the applicable administrative remedies with respect to Defendant's failure to expedite the processing of Plaintiff's requests.

27. Plaintiff is entitled to injunctive relief with respect to the expedited processing of the requested agency records.

Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records

28. Plaintiff repeats and realleges paragraphs 1-23.

29. Defendant has wrongfully withheld agency records requested by Plaintiff by failing to comply with the statutory time limit for the processing of FOIA requests.

30. Plaintiff has exhausted the applicable administrative remedies with respect to Defendant's wrongful withholding of the requested records.

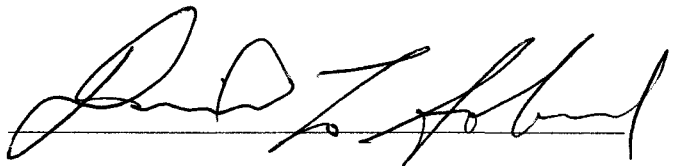
31. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested documents.

REQUESTED RELIEF

WHEREFORE, Plaintiff prays that this Court:

1. order Defendant and its components to process immediately the requested records in their entirety;
2. order Defendant and its components, upon completion of such expedited processing, to disclose the requested records in their entirety and make copies available to Plaintiff;
3. provide for expeditious proceedings in this action;
4. award Plaintiff its costs and reasonable attorneys fees incurred in this action; and
5. grant such other relief as the Court may deem just and proper.

DATED: February 10, 2015

By: 

DAVID L. SOBEL
D.C. Bar. No. 360418
Electronic Frontier Foundation
5335 Wisconsin Avenue, N.W.
Suite 640
Washington, D.C. 20015
(202) 246-6180

JENNIFER LYNCH
(admitted in California)
ANDREW CROCKER
(admitted in California)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION