IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF JUSTICE,
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

Defendant.

Civ. Action No. 18-1814

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, to compel disclosure of records requested by Plaintiff Electronic Privacy Information Center ("EPIC") from the Executive Office for United States Attorneys ("EOUSA"), a subcomponent of the Defendant U.S. Department of Justice ("DOJ").

2. EPIC seeks the release of records related to the DOJ's collection of cell site location information ("CSLI") in 2016 and 2017. EPIC submitted two separate FOIA requests to the DOJ ("EPIC's 2016 CSLI FOIA Request" and "EPIC's 2017 CSLI FOIA Request"). In this Complaint, EPIC challenges (1) the DOJ's failure to make a timely decision about EPIC's FOIA requests; and (2) the DOJ's failure to release records responsive to EPIC's FOIA requests. EPIC seeks injunctive and other appropriate relief.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331, 5 U.S.C. §§ 552(a)(6)(E)(iii), (a)(4)(B). This Court has personal jurisdiction over Defendant DOJ.

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

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is education, oversight, and analysis of government activities that impact individual privacy, free expression, and democratic values in the information age.[1] EPIC's Advisory Board includes distinguished experts in law, technology, and public policy.

6. EPIC maintains one of the most popular privacy websites in the world, https://epic.org, which provides EPIC's members and the public with access to information about emerging privacy and civil liberties issues. EPIC has a robust FOIA practice and routinely disseminates information obtained under the FOIA to the public through the EPIC website, the biweekly *EPIC Alert* newsletter, and various news organizations. EPIC is a representative of the news media. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

7. Defendant Department of Justice is a federal agency within the meaning of the FOIA, 5 U.S.C. § 552(f)(1). The DOJ is headquartered in Washington, D.C.

Facts

8. The Department of Justice has never released to the public any comprehensive reports concerning the collection and use of cell site location information. Unlike the use of Wiretap Act

[1] *See* EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

authorities, which is subject to detailed reporting requirements under 18 U.S.C. § 2519, law enforcement use of cell site data is not subject to any comparable public accounting.

9. Through EPIC's 2016 CSLI FOIA Request and EPIC's 2017 CSLI FOIA Request, EPIC seeks to determine the use, effectiveness, cost, and necessity in the collection and use of cell site location information so that the public, lawmakers, and the courts may have a better understanding of the use of this investigative technique.

10. Today, cell phones are as necessary as they are ubiquitous for Americans. Spanning a wide range of demographic groups, about 95% of Americans own a cell phone.[2] But cell phones also generate precise location records that can track an individual's movements over time. Telecommunication companies routinely collect and store this data, and law enforcement has sought access to this data.

11. Surveys show that Americans are acutely concerned about the privacy of their personal data, skeptical about companies' data collection practices, and a desire limits on location data tracking. A 2016 Pew Research survey found that "65% of Americans say there are not adequate limits on 'what telephone and internet data the government can collect.'"[3] Americans "express a consistent lack of confidence" that "records maintained [by companies] will remain private and secure," and 56% are either not too confident or not at all confident that cell phone companies adequately protect their records.[4] Cell phone users do not consent to location tracking; only 52%

[2] *Mobile Fact Shee*t, Pew Research Center (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.
[3] Lee Rainie, *The State of Privacy in Post-Snowden America*, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
[4] *Id.*

of those surveyed understood "that turning off the GPS function of a smartphone *does not* prevent all tracking of that device."[5]

12. But as the Supreme Court recently explained in *Carpenter v. United States*, modern cell phones "tap into the wireless network several times a minute whenever their signal is on" and these connections generate "a time-stamped record known as cell-site location information (CSLI)." 138 S. Ct. 2206, 2211 (2018). This location information can be very precise, depending "on the size of the geographic area covered by the cell site," and is especially precise in cities where there is a greater "concentration of cell sites." *Id.* The Supreme Court held in *Carpenter* that these location records are protected under the Fourth Amendment.

§ 2703(d) Orders Under the Stored Communications Act

13. Prior to the Supreme Court's decision in *Carpenter*, law enforcement officials routinely collected location information, without a warrant, pursuant to orders issued under the Stored Communications Act, 18 U.S.C. § 2703(d) ("§ 2703(d) Orders").

14. Enacted in 1986, the Electronic Communications Privacy Act ("ECPA") protects a wide range of electronic communications in transit and at rest.[6] ECPA expanded and revised federal wiretapping and electronic eavesdropping provisions, including the Wiretap Act, and created the Stored Communications Act ("SCA"). *See* 18 U.S.C. §§ 2701–2712. The SCA makes it unlawful to intentionally access a facility in which electronic communication services are provided and obtain, alter, or prevent unauthorized access to a wire or electronic communication while it is in

[5] Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, Pew Research Center (Mar. 22, 2017), http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.
[6] EPIC, *The Privacy Law Sourcebook 2016: United States Law, International Law, and Recent Developments* 258 (Marc Rotenberg ed., 2016).

electronically stored in such system. The SCA also requires law enforcement to obtain a court order or subpoena to access certain subscriber records.

15. As part of the Stored Communications Act, 18 U.S.C. § 2703(d) authorizes the government to compel a provider of electronic communication services to disclose certain subscriber records through a court order. *See* 18 U.S.C. § 2703(c)(1)(B). Section 2703(d) Orders can be granted based on a showing of "reasonable grounds to believe" that the records sought are "relevant and material" to an ongoing criminal investigation. This standard is lower than the "probable cause" standard of a warrant, which is required under the Fourth Amendment.

Law Enforcement's Use of § 2703(d) Orders to Obtain CSLI

16. Cell phones use radio waves to send and receive voice calls and data whenever it is within range of an antenna or cellular tower.[7] Cell phones connect to a service provider's network through "cell sites," each of which contains a transceiver and controller used to relay signals between mobile devices and the network to enable calls and other communications.[8] Cell phones communicate with nearby cell sites during a process called "registration," which occurs automatically when a device is idle.[9] During the registration process, cell phones ping nearby cell sites to identify the strongest signal.[10] A similar process occurs when a cell phone user moves from one cell site to another while making a call. Once registration occurs, the information is stored temporarily in service provider databases in order to route calls.[11] When a cell phone communicates with a tower, information is collected that can be used to determine the location of

[7] CTIA: The Wireless Association, Wireless in America: How Wireless Works, http://files.ctia.org/pdf/Brochure_HowWirelessWorks.pdf.
[8] Axel Küpper, *Location-Based Services: Fundamentals and Operation* 91–97 (2006).
[9] *A Guide to the Wireless Engineering Body of Knowledge* 77 (Andrzej Jajszcyk ed., 2d ed. 2011)
[10] Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* 104 (2010).
[11] Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013), http://www.mattblaze.org/blog/celltapping.

the device, and consequently, the location of the person using the phone. Called CSLI, this data can be combined from multiple cell towers to triangulate a phones location "with a high degree of accuracy (typically under fifty meters)."[12]

17. Law enforcement typically uses CSLI records in an investigation to pinpoint the location of individuals and create a map their movements over time. For example, in *United States v. Graham*, the government compiled as much as 221 days' worth of CSLI, around 29,000 location data points generated per defendant, without a warrant. 824 F.3d 421, 446–47 (4th Cir. 2016) (en banc) (Wynn, J., dissenting). In *Carpenter*, the government obtained over five months of CSLI and used this data to create maps showing that the plaintiff's cell phone had been near four of the charged robberies. 138 S. Ct. 2206, 2212–13 (2018).

18. Several major telecommunications companies have released reports that include aggregate statistics about government requests for customers data. But these reports are neither comprehensive nor detailed enough to evaluate the full scope of law enforcement access to location data. For example, AT&T's report stated that in 2017 the company received 16,385 demands for historic CSLI.[13] Sprint Corporation's report stated that in 2017, the company received 29,595 court ordered requests for customer information but did not distinguish which orders were § 2703(d) orders.[14] T-Mobile's reports reveal that in 2014, the company received 34,913 court orders for CSLI while in 2015 it received 47,998—a 37% increase.[15] These reports

[12] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. 117, 128 (2012).
[13] AT&T, Transparency Report (2018), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2018-Transparency-Report.pdf.
[14] Sprint, Sprint Corporation Transparency Report 2 (2018), http://goodworks.sprint.com/content/1022/files/Transparency%20Report%20January%202018.pdf.
[15] T-Mobile, Transparency Report for 2013 and 2014 (2015), https://www.t-mobile.com/content/dam/t-mobile/corporate/media-library/public/documents/NewTransparencyReport.pdf; T-Mobile, Transparency

are limited in other significant ways—they provide no geographic breakdown of where these § 2703(d) orders are being executed, how many days' worth of CLSI are sought, and are inconsistent in how to convey the types of CSLI court orders.[16] And the overall number of § 2703(d) orders cannot be assessed solely from these transparency reports because smaller telecommunications carriers do not publish transparency reporting.

Location Data and the Fourth Amendment After *Carpenter*

19. The Supreme Court in *Carpenter* considered the constitutionality of the Government's use of § 2703(d) Orders to obtain CSLI. The Court ultimately held that cell phone location records are protected by the Fourth Amendment, declining "to grant the state unrestricted access to a wireless carrier's database of physical location information." *Carpenter*, 138 S. Ct. at 2223. The Court found that "police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation," but left open the question of what legal process is required in emergencies or other unique situations. *Id.*

20. The legal regime for law enforcement access to CSLI implicates privacy interests of nearly all U.S. persons. As the Court stated in *Carpenter*, "cell phone location information is detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216. CSLI can reveal the most intimate details of everyday life: a trip to a place of worship, attendance at a political protest, or a visit to a medical specialist. Cell site location records obtained by the government are even more

Report for 2015 (2016), https://www.t-mobile.com/content/dam/t-mobile/corporate/media-library/public/documents/2015TransparencyReport.pdf.

[16] *See* Verizon, United States Report, http://www.verizon.com/about/portal/transparency-report/us-report/ (aggregating law enforcement demands for customer data under the table heading "General Orders"); *cf.* AT&T, Transparency Report 3 (2018), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2018-Transparency-Report.pdf. (dividing law enforcement demands by "General" court orders and "Search Warrants/Probable Cause" court orders as well as sub-dividing each category into historic and real-time CSLI).

comprehensive than GPS records and this precision only increases with advancements in technology.

EPIC's FOIA Requests

A. EPIC's 2017 CSLI FOIA Request

21. On June 14, 2017, EPIC submitted a FOIA request ("EPIC's 2017 CSLI FOIA Request") to the DOJ's Executive Office for United States Attorneys via e-mail.

22. EPIC's FOIA Request sought records related to the federal use of 18 U.S.C. § 2703(d) orders to obtain cell site location information. Specifically, EPIC sought:

1) The first page of all 2703(d) orders for production of cell site location information during January 1, 2017 through March 31, 2017.

23. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii)(II) and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

24. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

25. EPIC received no acknowledgement letter from the DOJ.

26. On December 6, 2017, EPIC contacted the DOJ FOIA office to inquire about a status update. The FOIA office stated there was no record of the original request in the system. On the same day, EPIC re-submitted its original FOIA request.

27. On July 25, 2018, EPIC called the DOJ FOIA office to confirm that the office received the re-submitted FOIA request on December 6, 2017. EPIC's 2017 CSLI FOIA Request was given reference number EOUSA-2018-001445 and assigned to Mr. John Kornmeier for processing.

28. EPIC attempted to contact Mr. Kornmeier on July 12, 2018, July 16, 2018, and July 18, 2018 to ask for a status update. EPIC left voicemail messages, but they were never returned.

B. EPIC's 2016 CSLI FOIA Request

29. On June 21, 2017, EPIC submitted a FOIA request ("EPIC's 2016 CSLI FOIA Request") to the DOJ's Executive Office for United States Attorneys via e-mail.

30. EPIC's FOIA Request sought records related to the federal use of 18 U.S.C. § 2703(d) orders to obtain cell site location information. Specifically, EPIC sought:

> 2) The first page of all 2703(d) orders for production of cell site location information during 2016.

31. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii)(II) and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

32. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

33. EPIC received no acknowledgement letter from the DOJ.

34. On December 6, 2017, EPIC called the DOJ FOIA office for a status update and the officer informed EPIC that the request was assigned reference number EOUSA-2017-002018. The FOIA officer stated that the request was assigned to Mr. John Kornmeier and the office was still processing the request.

35. EPIC attempted to contact Mr. Kornmeier on July 12, 2018, July 16, 2018, and July 18, 2018 to ask for a status update. EPIC left voicemail messages, but they were never returned.

EPIC's Constructive Exhaustion of Administrative Remedies

36. Today is the 406th day since the DOJ received EPIC's 2016 CSLI FOIA Request.

37. Today is the 238th day since the DOJ received EPIC's 2017 CSLI FOIA Request.

38. The DOJ has failed to make a determination regarding EPIC's FOIA Requests for expedited processing within the time period prescribed by 5 U.S.C. § 552(a)(6)(E)(ii)(I).

39. Additionally, the DOJ has failed to make a determination regarding EPIC's FOIA Requests within the time period required by 5 U.S.C. § 552(a)(6)(A)(i).

40. EPIC has exhausted all administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply with Statutory Deadlines

41. Plaintiff asserts and incorporates by reference paragraphs 1–40.

42. Defendant DOJ has failed to make a determination regarding EPIC's first FOIA request for 406 days for EPIC's 2016 CSLI FOIA Request and for 238 days for EPIC's 2017 CSLI FOIA Request. Thus, the DOJ has thus violated the deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).

43. Plaintiff has constructively exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count II

44. **Violation of FOIA: Failure to Grant Request for Expedited Processing**

1. Plaintiff asserts and incorporates by reference paragraphs 1–40.

2. Defendant's failure to grant plaintiff's request for expedited processing violated the FOIA, 5 U.S.C. § 552(a)(6)(E)(i).

3. Plaintiff is entitled to injunctive relief with respect to an agency determination on EPIC's request for expedited processing.

Count III

Violation of FOIA: Unlawful Withholding of Agency Records

45. Plaintiff asserts and incorporates by reference paragraphs 1–40.

46. Defendant DOJ has wrongfully withheld agency records requested by Plaintiff.

47. Plaintiff has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

48. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Count IV

Claim for Declaratory Relief

49. Plaintiff asserts and incorporates by reference paragraphs 1–40.

50. Plaintiff is entitled under 28 U.S.C. § 2201(a) to a declaration of the rights and other legal relations of the parties with respect to the claims set forth in Counts I–IV.

Requested Relief

WHEREFORE, Plaintiff requests this Court:

A. Order Defendant to immediately conduct a reasonable search for all responsive records;

B. Order Defendant to take all reasonable steps to release non-exempt records;

C. Order Defendant to disclose promptly to Plaintiff all responsive, non-exempt records;

D. Order Defendant to produce the records sought without the assessment of search fees;

E. Order Defendant to grant EPIC's request for a fee waiver;

F. Award EPIC costs and reasonable attorney's fees incurred in this action; and

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

Respectfully Submitted,

MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

/s/ Alan Butler
ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel
ELECTRONIC PRIVACY
INFORMATION CENTER

1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: August 1, 2018