

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue, N.W.
Washington, D.C. 20036,

Plaintiff,

v.

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

Defendant.

Civ. Action No. 18-1814

FIRST AMENDED COMPLAINT FOR INJUNCTIVE RELIEF

1. Plaintiff Electronic Privacy Information Center (“EPIC”) pursues this action against the Executive Office for United States Attorneys (“EOUSA”), a subcomponent of the Defendant U.S. Department of Justice (“DOJ”), under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552.

2. EPIC seeks the release of records related to the DOJ’s collection of cell site location information (“CSLI”) in 2016, 2017, 2018, and 2019. EPIC has submitted three separate FOIA requests to the DOJ (“EPIC’s 2016 CSLI FOIA Request,” “EPIC’s 2017 CSLI FOIA Request,” and “EPIC’s 2019 CSLI FOIA Request”). In this Complaint, EPIC challenges (1) the DOJ’s failure to make a timely decision about EPIC’s FOIA requests; (2) the DOJ’s failure to release records responsive to EPIC’s FOIA requests; and (3) the DOJ’s unlawful policy and practice of refusing to conduct searches for responsive records held by U.S. Attorney’s Offices (“USAOs”). 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.

8. Defendant DOJ is in possession, custody, and control of the records requested by Plaintiff, which are the subject of this action.

¹ See EPIC, *About EPIC* (2019), <https://epic.org/epic/about.html>.

Facts

9. The Supreme Court's recent decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), has raised important questions about the use of cell site location information by law enforcement agencies. In that case, the Court held that the acquisition of cell-site records was a Fourth Amendment search.

10. 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 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.

11. Through EPIC's 2016 CSLI FOIA Request, EPIC's 2017 CSLI FOIA Request, EPIC's 2019 CSLI FOIA Request, and future requests EPIC seeks to evaluate the use, effectiveness, cost, and necessity of the collection and use of cell site location information by law enforcement. These records will enable EPIC, the public, lawmakers, and the courts to have a better understanding of how this surveillance authority is being used and how broadly these techniques impact the privacy of Americans.

12. Today, cell phones are as necessary as they are ubiquitous for Americans. Spanning a wide range of demographic groups, an estimated 95% of Americans own a cell phone.² Modern cell phones generate precise location records that can be used to track an individual's movements over time. Telecommunication companies routinely collect and store this data, and law enforcement seeks access to this data with increasing frequency.

13. Surveys show that Americans are acutely concerned about the privacy of their personal data, skeptical about companies' data collection practices, and desire limits on location data

² *Mobile Fact Sheet*, Pew Research Center (Feb. 5, 2018), <http://www.pewinternet.org/fact-sheet/mobile/>.

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% of those surveyed understood “that turning off the GPS function of a smartphone *does not* prevent all tracking of that device.”⁵

14. 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.*

Orders Under the Stored Communications Act—18 U.S.C. § 2703(d)

15. 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”).

16. Enacted in 1986, the Electronic Communications Privacy Act (“ECPA”) protects a wide range of electronic communications in transit and at rest.⁶ ECPA updated the federal Wiretap

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.*

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).

Act, and created new legal protections for stored communications, *See* 18 U.S.C. §§ 2701–2712 (the Stored Communications Act (“SCA”)). The SCA makes it unlawful to access electronic communications without authorization when those communications are held by a service provider in electronic storage. The SCA also requires law enforcement to obtain a court order or subpoena to access certain subscriber records. 18 U.S.C. § 2703(d).

17. Section 2703(d) permits the government to compel a provider of electronic communication services to disclose certain subscriber records through a court order. 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

18. 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

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 Jajszczyk ed., 2d ed. 2011)

¹⁰ Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* 104 (2010).

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 the device, and consequently, the location of the person using the phone. Called “Cell Site Location Information”—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

19. Law enforcement typically uses CSLI records in an investigation to pinpoint the location of individuals and to 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).

20. 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 only that in 2017 the company received 16,385 demands for historic CSLI.¹³ Sprint Corporation’s report stated only that in 2017 the company received 29,595 court ordered requests for customer information but did not distinguish which

¹¹ Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013), <http://www.mattblaze.org/blog/celltapping>.

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>.

orders were § 2703(d) orders.¹⁴ T-Mobile’s reports stated only 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 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 CSLI 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*

21. 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.*

22. 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

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 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).

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

EPIC’s FOIA Requests

A. EPIC’s 2017 CSLI FOIA Request

23. 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.

24. 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:

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

25. 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).

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

27. EPIC received no acknowledgement letter from the DOJ.

28. 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.

29. 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.

30. 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

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

32. 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:

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

33. 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).

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

35. EPIC received no acknowledgement letter from the DOJ.

36. 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.

37. 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.

C. EPIC'S 2019 CSLI FOIA Request

38. On July 2, 2019, EPIC submitted a third FOIA request (“EPIC’s 2019 CSLI FOIA Request”) to the DOJ’s Executive Office for United States Attorneys via e-mail.
39. 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:
 - The first page of all 2703(d) orders for production of cell site location information during 2017, 2018, and 2019.
40. 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).
41. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).
42. EPIC received no acknowledgement letter from the DOJ.

EPIC’s Initial Complaint

43. As a result of the DOJ’s failure to comply with the FOIA, EPIC filed a complaint in *EPIC v. Department of Justice*, No. 18-1814, on Aug. 1, 2018. Compl., ECF No. 1.
44. The DOJ submitted its answer on Sept. 19, 2018. Def.’s Answer, ECF No. 5.

Developments Since the Filing of EPIC’s Initial Complaint

45. On September 20, 2018, this Court ordered the parties to:

[M]eet and confer and file a Joint Status Report proposing a schedule for proceeding in this matter. The schedule should address, among other things, the status of Plaintiff’s FOIA request, the anticipated number of documents responsive to Plaintiff’s FOIA request, the anticipated date(s) for release of the documents requested by Plaintiff, whether a motion for Open America stay is likely in this case, whether a Vaughn Index will be required in this case, and a briefing schedule for dispositive motions, if required.
46. The parties were directed to file a Joint Status Report on or before October 19, 2018.
47. EPIC contacted the DOJ on Oct. 5, 2018 to propose a processing schedule. Joint Status Report, ECF No. 6. The DOJ provided copies of two letters it asserted that were previously sent

to EPIC and the parties agreed to discuss further the scope of issues in dispute and agree upon a schedule.

48. On Oct. 10, 2018, the DOJ sent EPIC a letter claiming to be a “final action” on the First FOIA Request. Joint Status Report, ECF No. 8. The letter stated: “Our Data Analysis Staff has searched its database and determined that EOUSA does not track the statute requested.” *Id.*

49. On October 19, 2019, the parties filed an initial Joint Status Report indicating that the DOJ had provided two letters to EPIC and requesting more time to discuss the scope of issues in dispute. *Id.*

50. On October 22, 2018, the Court again entered an Order for the parties to file a status report by November 6, 2018, with the necessary information from the agency. October 22, 2018, Minute Order.

51. On November 6, 2018, EPIC sent the DOJ several questions about its record retention practices pertaining to § 2703(d) orders that would be helpful in identifying responsive records. EPIC proposed to schedule a call to discuss scoping the request and developing a search methodology. The parties also filed a Joint Status Report that indicated that they required additional time to determine the scope of issues in dispute and to agree upon a schedule for further proceedings. Joint Status Report, ECF No. 7.

52. On November 7, 2019, the Court entered an Order reiterating the two previous orders and indicating that the parties should file by November 20, 2018, a status report that includes the necessary information about the agency’s processing of EPIC’s request. November 7, 2018, Minute Order.

53. On November 15, 2018, the parties conferred to discuss the agency’s search capabilities and records systems. Mr. Kornmeier participated in the call on behalf of the EOUSA and

acknowledged that the individual USAOs do maintain records that could be responsive to EPIC's request. Mr. Kornmeier indicated that he had contacted two of the larger USAOs (D.C. and the SDNY) and found that they did not have a system for tracking §2703(d) application or orders. He indicated that SDNY might be able to locate the records using a log of items filed with the court, and the agency agreed to follow up with USAO-SDNY.

54. The DOJ did contact the USAO-SDNY but did not ultimately conduct a search for records responsive to EPIC's request. Joint Status Report, ECF No. 12. On Feb. 7, 2019, the agency sent an e-mail to EPIC detailing the issues that the USAO-SDNY claimed would prevent them from conducting a search. In the statement, the Office claimed that "it is impossible for the USAO-SDNY to comply with this request" because it is impossible to use criminal clerk logs, manual search methods, or a system-wide digital search to locate responsive records. Among other issues, the agency claimed that search of the office's digital records would require file indexing that would "crash the system."

55. On Feb. 15, 2019, EPIC proposed a revised search methodology to search several USAOs that might be able to locate responsive records. EPIC proposed that the DOJ would contact three specific U.S. Attorney's Offices—the Eastern District of Oklahoma (a small sized office), the Eastern District of Pennsylvania (a medium sized office), and the Southern District of California (a large sized office)—and determine whether those offices could conduct searches for responsive records. *Id.*

56. On March 13, 2019, the agency agreed to contact the three offices and provide EPIC with a response within 30 days. *Id.* Joint Status Report, ECF No. 12.

1. On April 25, 2019, the DOJ sent an e-mail to EPIC stating that all three USAOs had responded that they "do not track" the information requested. Joint Status Report, ECF No. 13.

The Eastern District of Oklahoma “reported that they do not have access to orders regarding cell site locations.” And the offices indicated that “[t]hey would have to manually search all of their case files for the designated time period to find cases in which a 2703(d) order was requested and granted.” The offices refused to conduct a manual search.

57. The DOJ has still not produced or identified any records in response to EPIC’s FOIA requests or provided an anticipated date of release.

EPIC’s Constructive Exhaustion of Administrative Remedies

58. Today is the 797th day since the DOJ received EPIC’s 2016 CSLI FOIA Request.

59. Today is the 804th day since the DOJ received EPIC’s 2017 CSLI FOIA Request.

60. Today is the 56th day since the DOJ received EPIC’s 2019 CSLI FOIA Request.

61. 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).

62. Additionally, the DOJ has failed to make a determination regarding EPIC’s 2016, 2017, and 2019 CSLI FOIA Requests within the time period required by 5 U.S.C. § 552(a)(6)(A)(i).

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

Count I

Violation of the FOIA: Failure to Comply with Statutory Deadlines

64. Plaintiff EPIC asserts and incorporates by reference paragraphs 1–64.

65. Defendant DOJ has failed to make a determination regarding EPIC’s 2016 CSLI FOIA request for 797 days, EPIC’s 2017 CSLI FOIA Request for 804 days, and for EPIC’s 2019 CSLI FOIA Request 56 days. Thus, the DOJ has violated the statutory deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).

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

Count II

Violation of the FOIA: Failure to Grant Request for Expedited Processing

67. Plaintiff EPIC asserts and incorporates by reference paragraphs 1–64.
68. Defendant DOJ’s failure to grant plaintiff’s request for expedited processing for EPIC’s 2017 CSLI FOIA Request, 2016 CSLI FOIA Request, and 2019 CSLI FOIA Request violated the FOIA, 5 U.S.C. § 552(a)(6)(E)(i).
69. EPIC is entitled to injunctive relief with respect to an agency determination on EPIC’s request for expedited processing.

Count III

Violation of the FOIA: Unlawful Withholding of Agency Records

70. Plaintiff EPIC asserts and incorporates by reference paragraphs 1–64.
71. Defendant DOJ has wrongfully withheld agency records requested by Plaintiff.
72. EPIC has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).
73. EPIC is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Count IV

Violation of the FOIA: Impermissible Policy, Pattern, and Practice of Failing to Conduct a Search in Response to Reasonably Described FOIA Requests

74. Plaintiff EPIC asserts and incorporates by reference paragraphs 1–64.

75. Defendant DOJ's Executive Office for United States Attorneys has adopted and is engaged in a policy, pattern, or practice of violating the FOIA's requirement that agencies search for records in response to a reasonably described request.
76. Under the EOUSA's unlawful policy, pattern, and practice, the agency refuses to conduct a search for records in EPIC's FOIA requests that clearly identified a specific type of record in the agency's possession and limited the request to a specific date range.
77. Under the EOUSA's unlawful policy, pattern, and practice, the agency refuses to conduct a search for records requests even when EPIC agreed to initially limit the search to specific USAOs.
78. Under the EOUSA's unlawful policy, pattern, or practice, the agency's USAOs maintain file management systems in a way, the agency alleges, that makes it impossible to search digital files for reasonably described records subject to release under the FOIA
79. The agency has never claimed that the requested records do not exist or that agency does not have control, custody, or possession of these types of records.
80. The DOJ is violating the FOIA by maintaining a policy, pattern, and practice of refusing to conduct searches reasonably calculated to uncover any records responsive to FOIA requests directed to EOUSA and USAOs.
81. The agency's repeated, unlawful, and intentional actions have harmed, and will continue to harm, EPIC and other similar requesters by indefinitely delaying the processing of their FOIA requests and withholding agency records.
82. The agency's unlawful policy, pattern, and practice of refusing to conduct a search in response to reasonably described FOIA requests like EPIC's FOIA requests will continue absent intervention by this Court.

83. EPIC therefore is entitled to declaratory and injunctive relief to compel the agency to comply with the requirements of the FOIA and to prevent the agency from continuing to apply its unlawful policy, pattern, or practice of refusing to search for responsive records.

Count V

Violation of the FOIA: Impermissible Policy, Pattern, and Practice of Failing to Comply with Statutory Deadlines

84. Plaintiff EPIC asserts and incorporates by reference paragraphs 1–64.
85. Defendant DOJ has failed to make a determination regarding EPIC’s three FOIA requests. Specifically: 797 days for EPIC’s 2016 CSLI FOIA Request; 804 days for EPIC’s 2017 CSLI FOIA Request; and 56 days for EPIC’s 2019 CSLI FOIA Request. Thus, the Defendant has thus violated statutory deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).
86. On information and belief, the DOJ has a policy and practice of failing to comply with the FOIA’s statutory deadlines in connection with the processing of EPIC’s 2016, 2017, and 2019 CSLI FOIA requests.
87. The DOJ’s repeated, unlawful, and intentional actions have harmed, and will continue to harm, EPIC and other requesters by requiring them to file suit against the agency in order to get the agency to process reasonably described FOIA requests.
88. EPIC is being irreparably harmed by the DOJ’s unlawful policy and practice and will continue to be irreparably harmed unless the DOJ is compelled to comply fully with the FOIA’s procedural requirements.

Count VI

Claim for Declaratory Relief

89. EPIC asserts and incorporates by reference paragraphs 1–64.

90. EPIC 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–V.

Requested Relief

WHEREFORE, EPIC requests this Court:

- A. Order the DOJ to immediately conduct a reasonable search for all responsive records;
- B. Order the DOJ to take all reasonable steps to release non-exempt records;
- C. Order the DOJ to disclose promptly to EPIC all responsive, non-exempt records;
- D. Order the DOJ to produce the records sought without the assessment of search fees;
- E. Order the EOUSA to implement recordkeeping practices that enable its offices to conduct digital searches for records requested;
- F. Order the DOJ to grant EPIC’s request for a fee waiver;
- G. Award EPIC costs and reasonable attorney’s fees incurred in this action; and
- H. 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
1519 New Hampshire Avenue, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: August 26, 2019