

VIA E-MAIL

July 2, 2019

Kevin Krebs
Assistant Director, FOIA/Privacy Unit
Executive Office for United States Attorneys
Department of Justice
175 N Street, NE, Suite 5.400
Washington, DC 20530-0001
USAEO.FOIA.REQUESTS@usdoj.gov

Dear Mr. Krebs:

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Executive Office for United States Attorneys (“EOUSA”).

EPIC seeks records related to the federal use of 18 U.S.C. § 2703(d) orders and warrants to obtain cell site location information (“CSLI”). 18 U.S.C § 2703(d) authorizes the government to compel an electronic communication service provider to disclose certain records using a court order if there are “reasonable grounds to believe” that the records are “relevant and material to an ongoing criminal investigation.”¹ Recently, the Supreme Court held that cell phone location records are protected by the Fourth Amendment and are inaccessible without a warrant.²

Documents Requested

The first page of all § 2703(d) orders and warrants for production of cell site location information during the following calendar years: 2017, 2018, and 2019.

EPIC requests that the EOUSA search for responsive records in each U.S. Attorney’s Office separately.

Background

Enacted in 1986, the Electronic Communications Privacy Act (“ECPA”) protects a wide range of electronic communication in transit and at rest.³ 18 U.S.C. § 2703(d), which is part of ECPA’s Stored Communications Act,⁴ authorizes the government to compel an electronic

¹ 18 U.S.C. § 2703(d) (2019).

² *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

³ 18 U.S.C. §§ 2510–2523 (2019).

⁴ 18 U.S.C. § 2701–2712 (2019).

communication service provider to disclose customer records.⁵ In contrast to warrants that require a showing of “probable cause,” § 2703(d) orders only required a showing of “specific and articulable facts” that the records are “relevant” to an ongoing investigation, a lower burden of proof.⁶

Prior to the *Carpenter* decision, law enforcement agencies used § 2703(d) orders to collect detailed CSLI—“the information collected as a cell phone identifies its location to nearby cell towers”⁷—to pinpoint the location of individuals. In some cases, the government has compiled as much as 221 days’ worth of CSLI, all without obtaining a warrant.⁸

Giving law enforcement access to CSLI implicates the privacy interests of almost all individuals in the United States. Today, cell phones are ubiquitous and “unless a person is willing to live ‘off the grid,’ it is nearly impossible to avoid” generating CSLI simply by “navigat[ing] daily life.”⁹ Over 95% of all Americans own a cell phone¹⁰ and there are 396 million cell phone service accounts for a nation of 326 million people.¹¹ Most cell phone owners keep their phones in close proximity to them at all times.¹² As a result, CSLI can reveal the most intimate details of everyday life: trips to a place of worship, attendance at a political protest, or visits to a medical specialist. Cell site location records obtained by the government are incredibly comprehensive and this precision will only increase as technology advances.

In 2018, the Supreme Court held in *Carpenter v. United States* that CSLI is protected by the Fourth Amendment.¹³ The Court stated that “an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records.”¹⁴ Because giving government access to cell-site records contravenes a “reasonable expectation of privacy,”¹⁵ the Government is obligated to get a warrant “[b]efore compelling a wireless carrier to turn over a subscriber’s CSLI.”¹⁶ It is important to note that *Carpenter* does not prevent law enforcement from accessing CSLI. Instead, it requires that law enforcement obtain a warrant before doing so. Thus, it remains crucial that key information about the government’s use of § 2703(d) orders pre-*Carpenter*, and warrants post-*Carpenter* including the frequency with which the orders are obtained—especially in light of *Carpenter*—is revealed to the public.

⁵ 18 U.S.C. § 2703(c)(1) (2019).

⁶ 18 U.S.C. § 2703(d) (2019).

⁷ *Cell Phone Location Tracking*, Nat’l Ass’n of Criminal Def. Lawyers (June 7, 2016), [https://www.nacdl.org/uploadedFiles/files/criminal_defense/fourth_amendment/2016-06-07_Cell%20Tracking%20Primer_Final\(v2\)%20\(2\).pdf](https://www.nacdl.org/uploadedFiles/files/criminal_defense/fourth_amendment/2016-06-07_Cell%20Tracking%20Primer_Final(v2)%20(2).pdf).

⁸ In *United States v. Graham*, the government collected around 29,000 location data points per defendant. 824 F.3d 421 (4th Cir. 2016) at 446–47 (Wynn, J., dissenting).

⁹ *United States v. Davis*, 785 F.3d 498, 525 (11th Cir. 2015) (en banc) (Rosenbaum, J., concurring).

¹⁰ *Mobile Fact Sheet*, Pew Research Center (Feb. 5, 2018), <https://www.pewinternet.org/fact-sheet/mobile/>.

¹¹ *Carpenter*, 138 S. Ct. at 2211.

¹² *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

¹³ *Carpenter*, 138 S. Ct. at 2217.

¹⁴ *Id.* at 2221.

¹⁵ *Id.* at 2217.

¹⁶ *Id.* at 2221.

Request for Expedition

EPIC is entitled to expedited processing of this request under FOIA and the DOJ's FOIA regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(e)(1). Specifically, this request is entitled to expedited processing because (1) there is an “urgency to inform the public about an actual or alleged Federal Government activity,” and (2) the request is “made by a person who is primarily engaged in disseminating information.” 28 C.F.R. § 16.5(e)(1)(ii).

First, there is an “urgency to inform the public about an actual or alleged federal government activity.” *Id.* The “actual . . . federal government activity” is federal law enforcement's access to CSLI under 18 U.S.C. § 2703(d). This activity is not in dispute. Numerous court rulings have concerned the federal use of § 2703(d) orders to obtain CSLI.¹⁷ *Carpenter* itself stems from the issuance of two § 2703(d) orders by federal magistrate judges.¹⁸

There is also a clear “urgency to inform the public” about the extent of federal law enforcement's warrantless access to CSLI under § 2703(d) because the public deserves to know how often law enforcement is seeking cell site data. Surveys show that Americans are acutely concerned about the privacy of their personal data and desire limits on location data tracking.¹⁹ However, only 52% of individuals surveyed understood “that turning off the GPS function of a smartphone *does not* prevent all tracking of that device.”²⁰

The practice of obtaining § 2703(d) orders and CSLI warrants is prevalent. In 2017 alone, four major cell phone service providers—Verizon, AT&T, T-Mobile, and Sprint—received 172,710 orders and 104,464 search warrants from law enforcement.²¹ Over the years, as the number of orders requested has gone down, the number of warrants requested has gone up. In the second half of 2017 for example, law enforcement requested 28,817 orders and 10,631 warrants from Verizon.²² In the first half of 2018, law enforcement requested 25,929 orders, a 2,888 decrease, and 13,552 warrants, a 2,921 increase, from Verizon.²³ Though the four major service providers have released reports, their reports are limited. They do not distinguish between

¹⁷ See e.g. *United States v. Korte*, 918 F.3d 750, 758 (9th Cir. 2019); *United States v. Goldstein*, 914 F.3d 200, 202 (3rd Cir. 2019); *United States v. Curtis*, 901 F.3d 846, 848 (7th Cir. 2018); *United States v. Joyner*, 899 F.3d 1199, 1204 (11th Cir. 2018).

¹⁸ *Carpenter*, 138 S. Ct. at 2212.

¹⁹ *Mobile Fact Sheet*, Pew Research Center (Feb. 5, 2018), <https://www.pewinternet.org/fact-sheet/mobile/>.

²⁰ 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/>.

²¹ See *Law Enforcement Demands for Customer Data: United States*, Verizon, <https://www.verizon.com/about/portal/transparency-report/us-report/>; *Transparency Report*, AT&T (Feb. 2018), <https://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2018-Transparency-Report.pdf>; *Transparency Report*, T-Mobile, <https://www.t-mobile.com/content/dam/t-mobile/corporate/newsroom/pages/factsheetspdf/TransparencyReport2017.pdf>; *Sprint Corporation Transparency Report*, Spring (Jan. 2018), <https://newsroom.sprint.com/csr/content/1214/files/Transparency%20Report%20January%202018.pdf>.

²² *Law Enforcement Demands for Customer Data: United States*, Verizon, <https://www.verizon.com/about/portal/transparency-report/us-report/>.

²³ *Id.*

§ 2703(d) orders and other court orders, provide no geographic breakdown of where § 2703(d) orders are executed, and provide no details on how many days' worth of CSLI is requested. Smaller telecommunications carriers also do not publish transparency reporting and so the overall number of § 2703(d) orders cannot be fully assessed. Despite *Carpenter*, knowing the extent to which law enforcement has performed § 2703(d) orders remains relevant and crucial for public understanding on law enforcement's access to location information.

Second, EPIC is an organization “primarily engaged in disseminating information.” 28 C.F.R. § 16.5(e)(1)(ii). As the Court explained in *EPIC v. DOD*, “EPIC satisfies the definition of ‘representative of the news media’” entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003). Since *EPIC v. DOD*, EPIC continues to disseminate information and perform activities that satisfies the definition of “representative of the news media.”

In submitting this request for expedited processing, EPIC certifies that this explanation is true and correct to the best of its knowledge and belief. 28 C.F.R. § 16.5(e)(3); 5 U.S.C. § 552(a)(6)(E)(vi).

Request for “News Media” Fee Status and Fee Waiver

EPIC is a “representative of the news media” for fee classification purposes. *EPIC v. DOD*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a “news media” requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.10(c)–(d).

Further, any duplication fees should also be waived because (1) disclosure “would shed light on the operations or activities of the government, (2) disclosure of the requested information is “in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government” and (3) disclosure is “not primarily in the commercial interest” of EPIC, the requester. 5 U.S.C. § 552(a)(4)(A)(iii); 28 C.F.R. § 16.10(k). EPIC satisfies this standard based on the DOJ components' considerations for granting a fee waiver. 28 C.F.R. § 16.10(k)(2)(i)–(iii).

(1) Disclosure of the requested information is likely to shed light on the operations or activities of the government

First, disclosure of the requested documents “would shed light on the operations or activities of the government” because the subject of the request “concern[s] identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated.” 28 C.F.R. § 6.10(k)(2)(i). The subject of this request is self-evidently a federal activity. The § 2703(d) orders are orders requested by federal law enforcement officials in connection to a federal criminal investigation.

(2) Disclosure of the requested information is likely to contribute to the public understanding of the operations or activities of the government

Second, disclosure of the requested documents is “in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government.” 28 C.F.R. § 16.10(k)(2). DOJ components evaluate two factors to determine whether this requirement is met: (A) disclosure “must be meaningfully informative about government operations or activities;” and (B) “disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester.” 28 C.F.R. § 16.10(k)(2)(ii). “Components will presume that a representative of the news media will satisfy [the latter] consideration.” 28 C.F.R. § 16.10(k)(2)(ii)(B).

To the first consideration, disclosure of the requested information would “be meaningfully informative about government operations or activities.” 28 C.F.R. § 16.10(k)(2)(ii)(A). Currently, key information about the government’s use of § 2703(d) orders is not available to the public. The public does not know the frequency with which the orders are obtained nor do they know the scope of a § 2703(d) court order. In court proceedings, § 2703(d) orders often only become public in court proceedings years after they are obtained. For cases that are resolved by plea deals, § 2703(d) orders are never revealed to the public. Given that more than 97% of all criminal cases are resolved by plea deals,²⁴ most § 2703(d) orders are never made public.

While *Carpenter* held that cell-site records cannot be accessed without a warrant, the case’s long-term impact is unclear. The majority maintained that *Carpenter* was a “narrow” decision²⁵ and lower courts have readily interpreted it as such.²⁶ Perhaps most strikingly, the Seventh Circuit in *United States v. Adkinson* offered a way to bypass *Carpenter*.²⁷ The Seventh Circuit held that if a private telephone provider hands CSLI to the government with no encouragement, no warrant is required.²⁸ Thus, even after *Carpenter*, there are still concerns about law enforcement access to CSLI. The public has a right to know the frequency and extent to which the government is accessing their CSLI. Disclosing § 2703(d) orders and warrants would provide a better understanding of the scope of law enforcements’ operations.

To the second consideration, disclosure would “contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester” because, as provided in the DOJ’s FOIA regulations, it “shall be presumed that a representative of the news media will satisfy this consideration.” 28 C.F.R. §

²⁴ *The Trial Penalty: The Sixth Amendment Right to Trial on the Verge of Extinction and How to Save it*, Nat’l Ass’n of Criminal Def. Lawyers (July 10, 2018), <https://www.nacdl.org/trialpenaltyreport/>.

²⁵ *Id.* at 2210.

²⁶ See e.g., *United States v. Reyes-Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (claiming that *Carpenter* is restricted to data revealing a “person’s day-to-day movement”); *United States v. Oakes*, 320 F. Supp. 3d 956, 960 (M.D. Tenn., 2018) (“*Carpenter* has not changed that, before Defendant can assert a Fourth Amendment violation, he has to be able to assert a personal connection to the place or object in which he claims a privacy right.”); *United States v. Kay*, 2018 WL 4375183, at *1 (E.D. Wis., 2018) (refusing to extend *Carpenter* to the warrantless search of data collected by a pole camera).

²⁷ See *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019).

²⁸ *Id.* at 610.

16.10(k)(2)(ii)(B). As previously stated, EPIC is a representative of the news media and satisfies this second consideration.

(3) Disclosure of the information is not primarily in the commercial interest of the requester

Finally, disclosure of the information is “not primarily in the commercial interest of the requester.” 28 C.F.R. § 16.10(k)(2)(iii). In determining whether this final requirement is met, DOJ components evaluate the following two considerations: (i) whether “the requester has any commercial interest that would be furthered by request disclosure;” and (ii) whether “any commercial interest is not the primary interest furthered by the request.” 28 C.F.R. § 6.10(k)(2)(iii)(A)–(B).

To the first consideration, EPIC has no “commercial interest that would be furthered by the requested disclosure.” 28 C.F.R. § 6.10(k)(2)(iii)(A). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.²⁹

To the second consideration, a “commercial interest is not the primary interest furthered by the request” because, as provided in the DOJ FOIA regulations, “[c]omponents ordinarily will presume that when a news media reporter has satisfied the requirements of paragraphs (k)(2)(i) and (ii) of this section, the request is not primarily in the commercial interest of the requester.” 28 C.F.R. § 6.10(k)(2)(iii)(B). Again, the Court in *EPIC v. DOD* deemed EPIC to be a “news media” requester. As established above, disclosure would “shed light on the operations or activities of the government,” would likely “contribute significantly to public understanding,” and “the request is not primarily in the commercial interest of the requester.” *Id.*

For these reasons, a full fee waiver should be granted to EPIC’s request.

Conclusion

Thank you for your consideration of this request. EPIC anticipates your determination on its request within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I); 28 C.F.R. § 16.5(e)(4). For questions regarding this request contact Enid Zhou at 202-483-1140 x104 or FOIA@epic.org.

Respectfully submitted,

/s Jessica Hui

Jessica Hui
EPIC Clerk

/s Enid Zhou

Enid Zhou
Open Government Counsel

²⁹ EPIC, *About EPIC*, <https://epic.org/epic/about.html>.