



No. 3:25-CR-38

**IN RE FOUR APPLICATIONS FOR SEARCH
WARRANTS SEEKING INFORMATION ASSOCIATED
WITH PARTICULAR CELLULAR TOWERS A/K/A
TOWER-DUMP WARRANTS**

ORDER

Before CARLTON W. REEVES, *District Judge*.

Digital surveillance has been a huge boon to the government. By leveraging time-and-location data from cellular devices, agents can ascertain the identities of previously unknown suspects.¹ This technique has enhanced law enforcement's

¹ See, e.g., April Rubin, *Bank, Cell Records Led FBI to Suspect in Jan. 6 Eve Pipe Bomb Case*, Axios (Dec. 4, 2025), <https://www.axios.com/2025/12/04/fbi-pipe-bomb-rnc-dnc-arrest>; Tim Stelloh, *Cellphone Data Helped Solve a Michigan Singer's Murder, but Experts Say the Tool Will Soon Be Off-Limits*, NBC News (Mar. 22, 2024, at 9:53 CDT), <https://www.nbcnews.com/news/us-news/cell-phone-data-helped-solve-egypt-covingtons-murder-experts-say-tool-rcna144651>; Daniel Miller et al., *Inside the Brink's Heist Probe: How*

ability to investigate and prosecute crime.² But digital surveillance can also provide the government with *unfettered* access into individuals' lives. Such intrusions would have been unthinkable to those 55 men gathered in Philadelphia in 1787. Therein lies the problem—the technological resources at the government's disposal unlock efficient and effective ways to solve crime in the twenty-first century, but they also expose individuals' whereabouts at all times, including in sensitive places. The government now has the capacity to identify any individual with a cell phone, at any public or private location. As technology continues to evolve, open questions remain about what surveillance actions meet constitutional muster. The Fourth Amendment's protection against expansive government surveillance, nevertheless, must stay true to the Founders' core principles.

Law enforcement, in this matter, is investigating a series of violent crimes that were committed in Jackson, Mississippi. Some suspects' identities are known. Others are not. To identify all those potentially involved, the Government applied for search warrants. These warrants would permit law enforcement to use "tower dumps" to access the time-and-location-data of all devices that connected to cell towers around

Alleged Burglars Behind \$100-Million Theft Were Caught, L.A. Times (Oct. 16, 2023, at 3:00 PST), <https://www.latimes.com/california/story/2025-10-16/brinks-heist-investigation>.

² See Brief of *Amici Curiae* the Local Government Legal Center in support of Respondent at 5-10, *Chatrie v. United States*, 609 U.S. ----, 146 S. Ct. 2193 (2026) (No. 25-112), 2026 WL 973491, at *5-10 (Apr. 1, 2026) (explaining how geofence warrants are useful as crime solving tools, helping to "fill a gap no other technique to date can").

the area where these crimes allegedly occurred. With this information, the Government asserts that it will be able to identify all potential suspects. Even so, law enforcement would also have access to the cellular records of countless individuals, the vast majority of whom were merely passing by a location at the “wrong” time.³ That is an unreasonable search under the Fourth Amendment. To uphold core constitutional principles, this Court finds that tower dumps are *per se* unconstitutional. The Government’s request to reverse the Magistrate Judge’s decision denying its applications for search warrants is denied.

I.

Factual and Procedural History

A. Background⁴

Federal law enforcement has long been investigating gang activity in the Jackson metropolitan area. The Government alleges that a series of violent crimes transpiring over a 14-month period were related to one another and carried out by members of a gang and its rivals. The specific identities of all

³ See, e.g., Evan Perez, *Stumbles in the Search for a Brown University Shooter Led to the Wrong Man*, CNN (Dec. 17, 2025), <https://www.cnn.com/2025/12/17/politics/stumbles-search-brown-university-shooter-wrong-man> (discussing how cellular tower records identified the wrong suspect).

⁴ Due to an ongoing criminal investigation, the subject warrants and supporting documents, Docket Nos. 1-5, 16-18, and the Government’s memorandum in support of its motion for review of the denial of search warrant applications, Docket No. 40, are filed under seal. As a result, the specific details—identifying potential gang members and the target locations—will not be discussed in this published Order.

those involved elude the Government. To detect who was present at the respective crime scenes, the Government initially applied for four search warrants, the “February warrant applications.” February Warrant Applications, Docket Nos. 1-4. The February warrant applications, sharing a common affidavit, seek time-and-location data from the four cellular providers that control the cell towers near the nine locations where these crimes occurred. The Government argues that gang members commonly use cell phones to communicate and carry out illicit activity, and so by acquiring cellular data through tower dumps, all the perpetrators will become known. Magistrate Judge Harris denied the Government’s February warrant applications, holding that tower dumps are impermissible general warrants under the Fifth Circuit’s *United States v. Smith*.⁵ *In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers a/k/a Tower-Dump Warrants*, No. 3:25-CR-38-CWR-ASH, 2025 WL 603000, at *8 (S.D. Miss. Feb. 21, 2025).

The Government refashioned the February warrant applications and subsequently applied for three new warrants, the “June warrant applications,” concerning the same investigation into a street gang. June Warrant Applications, Docket Nos. 16-18. In the June warrant applications, the Government requests tower dump data from cellular towers near six different locations in Jackson that are more narrowly associated with where a homicide, vehicular theft, and two shootings took place over a two-day period in early 2024. In total, the warrant applications seek 30 minutes of cell-site records for

⁵ The *Smith* decision held that geofence warrants are categorically unconstitutional. 110 F.4th 817 (5th Cir. 2024).

two locations, 20 minutes for another two locations, and 10 minutes for the remaining two locations. Unlike the February warrant applications, the June warrant applications only request information from the cellular devices that connected to two or more of the six tower locations during the subject time period. Magistrate Judge Harris, nonetheless, declined to approve the June warrant applications based on the same reasoning he relied on to deny the February warrant applications. *In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers a/k/a Tower-Dump Warrants*, No. 3:25-CR-38-CWR-ASH, 2025 WL 1792841, at *1 (S.D. Miss. June 27, 2025).

The Government seeks review of Magistrate Judge Harris's denial of the June warrant applications and contends that the February warrant applications, too, are constitutional. Government's Motion, Docket No. 40.⁶

B. Tower Dumps: A Primer

Law enforcement agencies have used tower dumps as an investigative tool for over a decade. *See* June Warrant Application, Docket No. 16 at 30, Aff. ¶ 63. Though the tool has been at the government's disposal, its constitutionality has come in doubt following the Supreme Court's landmark *Carpenter* decision on the constitutionality of historical cell-site location

⁶ The National Association of Criminal Defense Lawyers, American Civil Liberties Union, American Civil Liberties Union of Mississippi, Electronic Frontier Foundation, and the Office of the State Public Defender filed a Brief of *Amici Curiae*. Docket No. 37.

information (CSLI).⁷ See 585 U.S. 296 (2018). Courts throughout the country are divided on how to apply *Carpenter*'s "narrow" holding to other surveillance techniques like tower dumps, as well as geofencing and real-time CSLI. See *id.* at 316; *Savage*, 2024 WL 3295586, at *2. To understand how tower dumps resemble and differ from the CSLI technology at the center of *Carpenter*, the Court provides a succinct explanation of how tower dumps operate.

Cell phones are everywhere in the United States. Nearly all American adults own a cell phone, and 91 percent own smartphones. William Bishop et al., Pew Rsch. Ctr., *Mobile Fact Sheet* (Nov. 20, 2025), <https://www.pewresearch.org/internet/fact-sheet/mobile/>. "Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called 'cell sites.'" *Carpenter*, 585 U.S. at 300. These cell sites are typically located on cell towers, but they also are on top of other fixtures, like light posts, flag poles, sides of buildings, and even on church steeples. *Id.* Cell sites, generally, "have several directional antennas that divide the covered area into sectors." *Id.* These sectors each cover approximately a 120-degree angular area. Government's Motion, Docket No. 40 at 10.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most

⁷ See *United States v. Savage*, No. 23-454, 2024 WL 3295586, at *2 (E.D. Pa. July 3, 2024) ("[I]n the years since [*Carpenter*], litigation has largely focused on whether tower dumps are searches at all for Fourth Amendment purposes, or if police may access CSLI data via mechanisms other than a search warrant[.]").

modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites [e.g., in urban areas], the smaller the coverage area.

Carpenter, 585 U.S. at 300-01.

Cellular providers, like AT&T, Verizon, Sprint, T-Mobile, and C-Spire, track when a device connects to a cell site—"noting the cell site used, the phone's identifier, and the start, end, origination and length of the communication[.]" Brief of *Amici Curiae*, Docket No. 37 at 13. This "time-stamped record [is] known as cell-site location information (CSLI)." *Carpenter*, 585 U.S. at 301.

Since most residents of the United States own cell phones—and carry them throughout daily life—access to CSLI can reveal individuals' whereabouts efficiently and rather accurately. In *Carpenter*, law enforcement acquired access to days of historical CSLI that tracked a specific suspect's past movements to tie him to a crime, but CSLI can be used in other ways. When it is known where and when a crime occurred, law enforcement can use CSLI to uncover what cellular devices connected to nearby cell towers during the time in question. See Beth W. Jantz, *Simulating More Particularity: Ideas for*

Approaching Search Warrants for Geofences, Tower Dumps, and Cell-Site Simulators, 16 Fed. Cts. L. Rev. 9, 14 (2024); *United States v. Medina*, 712 F. Supp. 3d 226, 237-38, *vacated and remanded on other grounds*, 125 F.4th 310 (1st Cir. 2025) (explaining the differences between tower dumps and historical CSLI). This process of gathering CSLI from cellular providers is a “tower dump.” A tower dump, simply put, is a “request seeking to obtain a list of all phones that connected to a single cell site during a particular window, allowing law enforcement to infer that the owners of those devices most likely were present in that site’s coverage area during that time.” *Savage*, 2024 WL 3295586, at *1 (cleaned up) (emphasis in original).

“There are different ways to delineate a location, but none of them precisely describe the boundaries of the geographic area to be searched. Police can request data from all towers in the vicinity of a street address; they can request it from all towers providing service to that address; and they can specify the towers or antennae most likely to have served any phones in the target area.” Brief of *Amici Curiae*, Docket No. 37 at 15. “Because the Government, at the time of serving a tower dump warrant, specifies no suspect phone or individual human target, they must issue a warrant for every cellular provider serving the area of the crime.” *Id.* As a result, tower dumps produce mounds of records—one warrant request may result in a list of thousands or hundreds of thousands of records on individual devices that were “in the vicinity of a cell tower around the time of the crime.” *Id.* at 16-17. “This location information, now in the possession of the government, could include not only public places (roads and bridges), but more importantly non-public places, such as

homes, businesses, churches, mosques, hospitals, and political offices.” *Matter of Tower Dump Data for Sex Trafficking Investigation*, No. 23-M-87, 2023 WL 1779775, at *2 (N.D. Ill. Feb. 6, 2023). Tower dumps “implicate[] privacy concerns of those uninvolved in any criminal activity, who are merely going about their daily lives and presumably do not want their movements tracked by the government, particularly in private and sensitive places.” *Id.* (citation omitted). “Awareness that the government may be watching chills both expression and association.” *Id.* (citations omitted).

Tower dumps, though, can be uniquely effective when law enforcement believes that the same individual or individuals committed crimes across more than one location. “By requesting subscriber information for multiple locations, the Government can cross-reference the data to identify who was present at the crime scene.” *Medina*, 712 F. Supp. 3d at 237-38 (citations omitted). This, presumably, narrows the pool of cellular records so that the suspects can be identified. Across the country, tower dumps have been used effectively for this purpose. *See Jantz, Simulating More Particularity*, at 24-25 (collecting cases).

II.

Legal Standard

Under 28 U.S.C. § 636(b)(3), “[a] magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States.” These additional duties include resolving certain criminal pretrial matters. *Gomez v. United States*, 490 U.S. 858, 868 n. 16 (1989) (citation omitted). “A table in a Committee Report listed the following

as criminal pretrial matters handled by magistrates: arrest warrants, search warrants, bail hearings, preliminary examinations, removal hearings, postindictment arraignments, pretrial conferences, and pretrial motions.” *Id.* Section 636(b)(1)(A) of the Federal Magistrates Act grants a judge of the court power to “reconsider any pretrial matter under [the Act’s] subparagraph (A) where it has been shown that the magistrate judge’s order is clearly erroneous or contrary to law.” Thus, “factual findings [are reviewed] under a clearly erroneous standard, while legal conclusions are reviewed *de novo*.” *Moore v. Ford Motor Co.*, 755 F.3d 802, 806 (5th Cir. 2014) (citations and quotation marks omitted).

III.

Discussion

The Fourth Amendment guarantees “[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. Our Founders envisioned the Amendment as an iron-clad protection against the “reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Riley v. California*, 573 U.S. 373, 403 (2014). General warrants, notably, “specify only an offense, leaving to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.” *Smith*, 110 F.4th at 836 (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981)) (cleaned up). That is why the Fourth Amendment requires that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const.

amend. IV. Probable cause and particularity “safeguard the privacy and security of individuals against arbitrary invasions by government officials.” *Carpenter*, 585 U.S. at 303 (quoting *Camara v. Mun. Ct. of City and Cnty. of S.F.*, 387 U.S. 523, 528 (1967)).

A. Fourth Amendment Search

The threshold issue is whether tower-dumps constitute a search under the Fourth Amendment. *See Smith*, 110 F. 4th at 830. As Magistrate Judge Harris noted, “[b]y proceeding with applications for search warrants, the Government has arguably conceded that the tower dumps *may* qualify as searches within the meaning of the Fourth Amendment.” *In re Four Applications for Search Warrants*, 2025 WL 603000, at *2 n. 5 (emphasis in original); *see also United States v. Sherod*, No. SAG-24-0120, 2025 WL 1736279, at *3 (D. Md. June 23, 2025) (“[B]ecause the investigators here sought and obtained search warrants for all the tower dump records, this Court need not address this preliminary issue, which has been hotly contested in various courts since the Supreme Court left the question open in *Carpenter*.”). The Government, however, rejects that its warrant applications concede as a point of law that tower dumps are searches. Government’s Motion, Docket No. 40 at 38-40. Magistrate Judge Harris’s point is well-taken. For the purposes of *de novo* review and for clarifying the law more generally,⁸ this Court conducts its own search analysis.

⁸ The Court is hesitant to assume that the mere fact of applying for a search warrant means that the Government admits that a Fourth Amendment search would be taking place. In fact, the Court commends the Government and law enforcement for applying for search warrants, as a way of

Here, like in other digital Fourth Amendment cases,⁹ “the antecedent question whether or not a Fourth Amendment ‘search’ has occurred is not so simple[.]” *Kyllo v. United States*, 533 U.S. 27, 31 (2001). *See Chatrue v. United States*, 609 U.S. ----, 146 S. Ct. 2193, 2205 (2026) (“In recent decades, this Court has often confronted the challenge of adhering to those principles in the face of new technologies.”). When the Fourth Amendment was ratified in 1791, the Founders had no awareness of digital surveillance strategies, like wiretapping, GPS trackers, and CSLI. *Id.* (“Innovations in surveillance tools have enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes.”) (cleaned up). The Founders, instead, conceptualized searches, particularly those that are unreasonable under the Constitution, as unfettered law enforcement agents rummaging through the home. Throughout the nineteenth century and well into the twentieth, “Fourth Amendment search doctrine was tied to

ensuring compliance with the law. This Court worries that there are misplaced doctrinal “loopholes” (i.e., the good-faith exception) that easily permit law enforcement to utilize new technologies without inquiring about the legality of their actions. The good-faith exception, in particular, has stymied development of Fourth Amendment law, and in doing so, it has also allowed law enforcement and the government to violate the Fourth Amendment. *See generally* Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, 113 *Geo. L.J.* 551 (2025).

⁹ Other federal courts have examined whether tower dumps require Fourth Amendment protection. *See United States v. Pricop*, 775 F. Supp. 3d 1036, 1039 (D. Ariz. 2025) (collecting cases). Some lower courts found tower dumps to be a search. *See, e.g., United States v. Spurlock*, 778 F. Supp. 3d 1136 (D. Nev. 2025). Others have found no search. *See, e.g., United States v. Williams*, 741 F. Supp. 3d 642 (E.D. Mich. 2024). This Court is only bound by the Supreme Court and the Fifth Circuit.

common-law trespass and focused on whether the Government obtains information by physically intruding on a constitutionally protected area.” *Carpenter*, 585 U.S. at 304 (quoting *United States v. Jones*, 565 U.S. 400, 405, 406, n. 3 (2012)) (cleaned up). That has since changed. Andrew Guthrie Ferguson, *Digital Rummaging*, 101 Wash. L. Rev. 1473, 1504 (2024) (“Over time, as police shifted from the analog surveillance technologies of the twentieth century to the digital investigative systems of the twenty-first century, the Supreme Court had to reassess its approach to the threshold search question.”). No longer are property rights “the sole measure of Fourth Amendment violations.” *Soldal v. Cook Cnty., Ill.*, 506 U.S. 56, 64 (1992).

The Supreme Court, in *Katz v. United States*, clarified that “the Fourth Amendment protects people, not places.” 389 U.S. 347, 351 (1967). Grounded in *Katz* and Justice Harlan’s canonical concurrence, the Supreme Court adopted what has become known as the reasonable expectation of privacy test. *See Smith*, 110 F.4th at 830. That test is “[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.” *Id.* (cleaned up). This two-part approach has allowed courts to apply the Founder’s guiding Fourth Amendment principles—rejection of arbitrary and intrusive government surveillance—to the modern world. *See Chatrpie*, 146 S. Ct. at 2205 (“Whether an expectation of privacy counts as legitimate is less the result of any fixed set of rules than of

‘guideposts’ stretching back to the Fourth Amendment’s beginnings.”) (citation omitted).

To determine whether individuals have a reasonable expectation of privacy in tower-dump data, the Court first turns to *Carpenter*, which is “arguably the most relevant Supreme Court precedent addressing law enforcement’s investigatory use of cellular consumer data.”¹⁰ *Smith*, 110 F.4th at 831. The *Carpenter* Court found that “[t]he Government’s acquisition of the cell-site records [CSLI] was a search within the meaning of the Fourth Amendment.” 585 U.S. at 316. Specifically, the Court examined whether there is a reasonable expectation of privacy in “chronic[ing] a person’s past movements through the record of his cell phone signals.” *Id.* at 309. This now-canonical decision marked a departure from the Supreme Court’s past precedents.

In *Carpenter*, law enforcement arrested four men suspected of robbing Radio Shack and T-Mobile stores. One of the suspects confessed; he named 15 accomplices and disclosed some of their phone numbers. The FBI, then, reviewed call records of the confessing suspect. In doing so, the FBI identified additional phone numbers of those who the suspect had called around when the robberies occurred. Under the Stored Communications Act, the government used this information to apply for court orders that would reveal the cell phone records

¹⁰ But see *Chatrpie*, 146 S. Ct. at 2199, which is a more recent Opinion on digital surveillance and the Fourth Amendment that the Supreme Court handed down at the end of the October 2025-2026 Term. That said, *Carpenter* deals with CSLI, whereas *Chatrpie* focuses on Location History.

of additional suspects, including the defendant in *Carpenter*. The court orders were granted, and they subsequently produced 12,898 location points, averaging 101 data points per day. *Id.* at 302. The *Carpenter* Court, however, departed from precedent and found that those requests for CSLI, “digital data—personal location information maintained by a third-party[,]” constituted a search. *Id.* at 306, 309-10.

Under past Fourth Amendment precedent, namely the third-party doctrine, the defendant’s argument would have been foreclosed in *Carpenter*. *See id.* at 306-10. The defendant, Mr. Carpenter, “continuously reveal[ed] his location to his wireless carrier.” *Id.* at 309. Knowingly exposing information, according to *Smith v. Maryland* and *United States v. Miller*, is not protected under the Fourth Amendment. *Id.* at 308; 442 U.S. 735, 743-44 (1979) (holding that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties”); 425 U.S. 435, 443 (1976) (holding that there is no expectation of privacy “even if the information is revealed on the assumption that it will be used only for a limited purpose”).

The *Carpenter* Court, however, “decline[d] to extend *Smith* and *Miller* to cover these novel circumstances.” *Id.* at 309. The Supreme Court determined that the third-party doctrine was not applicable “[g]iven the unique nature of cell phone location records, [and] the fact that the information [wa]s held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.” *Id.* The Court, then, expressly stated that “[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the

technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Id.* at 309-10.

That said, *Carpenter* is “narrow.” *Id.* at 316. The Court declined to “express a view on . . . real-time CSLI or ‘tower dumps.’” *Id.* To date, neither the Supreme Court nor the Fifth Circuit has opined on the constitutionality of tower dumps. *See also Spurlock*, 778 F. Supp. 3d at 1142-43. However, the Supreme Court in *Carpenter* and *Chatrie*, as well as the Fifth Circuit in *Smith*, left a trail of breadcrumbs—sprinkling hints—for how lower courts should proceed on these novel Fourth Amendment issues. *See United States v. Fuentes*, No. CR-21-358-RAW, 2024 WL 5494054, at *8 (E.D. Okla. Sept. 3, 2024) (“While the law sometimes struggles to remain relevant in the ever-changing technological landscape, extrapolation of existing precedent may often be justified to arrive at a just result.”). In fact, even Justice Gorsuch, in his *Carpenter* dissent, questions (albeit unfavorably) how the logic of the majority opinion would not extend to technologies like tower dumps:

But what distinguishes historical data from real-time data, or seven days of a single person’s data from a download of *everyone’s* data over some indefinite period of time? Why isn’t a tower dump the *paradigmatic* example of “too permeating police surveillance” and a dangerous tool of “arbitrary” authority—the touchstones of the majority’s modified *Katz* analysis? On what possible basis could such mass data collection survive the Court’s test while

collecting a single person's data does not? Here again we are left to guess.

Carpenter v. United States, 585 U.S. 296, 396 (2018) (Gorsuch, J., dissenting) (emphasis in original).

More broadly, however, *Carpenter* recognizes that while there is not a “single rubric definitively resolv[ing] which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted.” *Id.* at 304-05 (cleaned up). The “basic guideposts” are “that the Amendment seeks to secure ‘the privacies of life’ against ‘arbitrary power’” and “a central aim of the Framers was ‘to place obstacles in the way of a too permeating police surveillance.’” *Id.* at 305 (citations omitted). These two principles are useful for the Court “when applying the Fourth Amendment to innovations in surveillance tools.” *Id.* With these new technologies, the Court “has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Id.* (quotation marks and citation omitted). To uphold these protections, the Court found that “[a]llowing government access to cell-site records contravenes that expectation.” *Id.* at 311. The Court, thus, clarified that under the reasonable expectation of privacy test, “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.” *Id.* at 310. *Carpenter*, in short, counsels against technologies that give the government unfettered, arbitrary, and intrusive access to individuals’ movements.

In the Supreme Court’s latest Fourth Amendment case, *Chatrrie v. United States*, the Court builds upon its holding in *Carpenter* by applying its previous reasoning to geofencing and Location History. See *Chatrrie*, 146 S. Ct. at 2206. The Court, once again, held that an individual has a reasonable expectation of privacy in their cellular data. But the Court went a step further and clarified that “police invade that expectation [of privacy in cellular information], and thus conduct a search, when they acquire that information, even though for only a limited period of time and even though via a third-party tech company.” *Id.* The *Chatrrie* Court, thus, filled an important gap in *Carpenter* by expressly determining that the temporal aspect of a search has no bearing on whether or not a search occurred. *Id.* at 2209-12; see specifically *id.* at 2210 (“[T]he durational bounds on the data actually acquired do little to address the Fourth Amendment’s concern about ‘a too permeating police surveillance.’”) Put simply, a search is search, regardless of its duration.

The Court now turns to *United States v. Smith*, the leading Fifth Circuit case on digital surveillance technologies. Drawing on *Carpenter*’s logic the Fifth Circuit determined that geofence warrants¹¹ are “unconstitutional under the Fourth Amendment.” 110 F.4th at 820.

In reaching its conclusion, the Fifth Circuit relied largely on *Carpenter*. See *id.* at 832-34. The court recognized “[m]any of the concerns expressed . . . in [] *Carpenter* are highly salient in the context of geofence warrants.” *Id.* at 832-33. Geofences,

¹¹ For a primer on geofence warrants, see *Smith*, 110 F.4th at 821-26.

like CSLI, can provide for “permeating police surveillance” because “carrying one of these devices is essentially a prerequisite to participation in modern society, and users ‘compulsively carry cell phones with them all the time.’” *Id.* at 833 (citation omitted). In fact, the court argued that “[g]eofences also exemplify the Court’s concern with pinpoint location data—this technology provides more precise location data than either CSLI or GPS.” *Id.* (citation omitted). Such data, “like obtaining data through CSLI, is also remarkably cheap, easy, and efficient compared to traditional investigative tools.” *Id.* (quotation marks and citation omitted). For these reasons, the Fifth Circuit saw “parallels between CSLI and Location History data.” *Id.*

The court continued by acknowledging that “[w]hile it is true that geofences tend to be limited temporally, the potential intrusiveness of even a snapshot of precise location data should not be understated.” *Smith*, 110 F.4th at 833. The Fifth Circuit found that time does not necessarily limit the scope of Fourth Amendment protections. That is because “such location tracking can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences.” *Id.* “With just a click of a button,” the government can get access to “highly sensitive information—think a visit to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, or the gay bar[.]” *Id.* (cleaned up) (citation omitted). Even if the government becomes aware that an individual was at one of these locations for only a few minutes, a person’s presence in sensitive location was

nonetheless exposed. Under the Constitution, there is nothing minor about a minor invasion into one's location data. The Fifth Circuit, thus, concluded that "geofence location data is invasive for Fourth Amendment purposes." *Id.* at 834.

Notably, the Fifth Circuit found it determinative that geofencing captures the location of an individual, "regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection." *Id.* Geofencing allows completely innocuous individuals to get swept up. For the reasons the Supreme Court articulated in *Carpenter*, the Fifth Circuit found that the unconstitutionality of geofencing is not redeemed by the third-party doctrine. "[I]t is unreasonable to think of cell phone users as voluntarily assuming the risk of turning over comprehensive dossiers of their physical movements to third parties." *Id.* The Fifth Circuit recognized that "the third-party doctrine is ill suited to the digital age, in which people reveal a great deal of information about themselves in the course of carrying out mundane tasks." *Smith*, 110 F.4th at 834-35 (quotation marks and citation omitted). That is the case even though individuals opt in to Location History. *Id.* at 835. For the Fifth Circuit, "the intrusiveness and ubiquity of Location History data" triggers a "reasonable expectation of privacy in their respective data." *Id.* at 836.

The Fifth Circuit applied *Carpenter's* logic to geofencing; likewise, this Court finds it appropriate to apply the reasoning of *Carpenter*, the recent *Chatrife* opinion, and *Smith* to tower dumps. Not so fast, says the Government. It attempts to

distinguish *Smith*.¹² See Government’s Motion, Docket No. 40 at 30-38. The Government argues that the Fifth Circuit only recognized a “privacy interest in ‘granular’ and ‘comprehensive’ short-term location data that the court explicitly distinguished as being more precise than cell-site location information.” *Id.* at 39. Whereas the proposed tower dumps before the Court, “involve short-term location information that does not track or chronicle a user’s past movements and that will show only a device was in the general area serviced by a cell tower and sector.” *Id.* Short-term location information, under this logic, does not parallel the more detailed Google Location History data that were the subject of *Smith*. *Id.* The Government further notes that the data in *Smith* are far more precise—such data can identify individuals within ten feet of their location—but tower dumps only “provide a snapshot of devices” and so they are more like “surveillance footage from a business or other location showing persons in the area during a defined period[.]” *Id.* at 40. The Court disagrees for two reasons.

First, the Fifth Circuit has recognized that “the potential intrusiveness of even a snapshot of precise location data should not be understated.” *Smith*, 110 F.4th at 833. See also *Chatrie*, 146 S. Ct. at 2209-12 (discussing how the length of the search does not determine whether a search occurred). Though tower dumps provide more limited, less-detailed information than geofencing, the inherent nature of this type of search remains corrosive to individuals’ privacy interests.

¹² The Government more briefly distinguishes *Carpenter*. Government’s Motion, Docket No. 40 at 40-41.

Second, tower dumps are not equivalent to security cameras, pole cameras, or surveillance footage. The Supreme Court has strongly implied as such. *Carpenter* explicitly does not “call into question conventional surveillance techniques and tools, such as security cameras.” 585 U.S. at 316. Yet, in the same decision, the Supreme Court declined to express any view about technology like tower dumps. *Id.* The *Carpenter* Court, itself, found these two technologies to be materially different, which they are. Security cameras, placed on the outside of buildings, record those out in the public. Tower dumps, however, can identify individuals that are *within* buildings, and the produced location data can thereby reveal whether individuals are in a home, as well as in highly other sensitive places like in a voting site, place of worship, doctor’s office, domestic violence shelter, rehab facility, immigration clinic, gun show, or strip club. See Brief of *Amici Curiae*, Docket No. 37 at 15 (citation omitted); see also *Medina*, 712 F. Supp. 3d at 245-46 (“A tower dump is not the same as simply looking at a few minutes of surveillance tape, because the ability to quickly associate vast amounts of data allows law enforcement to see far more than what simple visual surveillance would reveal and extends effortlessly into both public and private spaces.”). That is fundamentally different than the scope of locational information that surveillance footage from pole towers or security cameras produce. “Tower dumps are also intimate and deeply revealing because even a small number of location data points discloses individuals’ private whereabouts and facilitates inferences about their habits of life.” Brief of *Amici Curiae*, Docket No. 37 at 22. This is exactly what *Carpenter*, *Chatrpie*, and *Smith* reject.

Under the reasoning of *Carpenter*, *Chatrie*, and *Smith*, this Court holds that tower dumps are a search under the Fourth Amendment.

B. General Warrant

After determining that tower dumps require Fourth Amendment protection, the Court must determine whether warrant applications seeking tower dump data, including the present warrant applications, are supported by probable cause and particularity. *See Smith*, 110 F.4th at 836 (citing *Carpenter*, 585 U.S. at 316). Before reaching the question of whether the subject warrants meet the requirements of probable cause and particularity, this Court is compelled—as the Fifth Circuit did in *Smith*—to address whether tower dumps constitute general warrants that are categorically barred by the Fourth Amendment. *See id.*

“It is undeniable that general warrants are plainly unconstitutional. Indeed, ‘it would be a needless exercise in pedantry to review again the detailed history of the use of general warrants as instruments of oppression from the time of the Tudors, through the Star Chamber, the Long Parliament, the Restoration, and beyond.’” *Id.* (quoting *Stanford v. Texas*, 379 U.S. 476, 482 (1965)). Yet, the Court finds it worth noting that the emergence of digital surveillance has the potential to unleash the Founders’ sincere fear. *See, e.g.*, Andrew Guthrie Ferguson, *Digital Rummaging*, 101 Wash. L. Rev. 1473, 1478 (2024) (“The analysis—offered here—about digital rummaging offers an additional theory of Fourth Amendment protection at a time when police power to invade privacy has grown exponentially.”). The Founders worried about the government rummaging through private houses, but their underlying

concern was that “no warrant can authorize the search of everything or everyone in sight.” *Smith*, 110 F.4th at 836 (quotation marks and citations omitted). This worry applies to technologies of today. *Id.* at 837-38.

Relevantly, the Fifth Circuit determined that “[g]eofence warrants present the exact sort of ‘general, exploratory rummaging’ that the Fourth Amendment was designed to prevent.” *Id.* at 837. The court noted that that first step in complying with a geofence warrant “forces the company to search through its *entire* database . . . law enforcement cannot obtain its requested location data unless Google searches through . . . all 592 million individual accounts—for *all* of their locations at a given point of time.” *Id.* (emphasis in original). Though the government argued that the warrants were “limited to specified information directly tied to a particular [crime] at a particular place,” the Fifth Circuit disagreed. *Id.* “While the *results* of a geofence warrant may be narrowly tailored, the *search* itself is not. A general warrant cannot be saved simply by arguing that, after the search has been performed, the information received was narrowly tailored to the crime being investigated.” *Id.* (emphasis in original). The same reasoning applies with equal force here: tower dumps impermissibly conjure a general rummaging that runs afoul of the Fourth Amendment.

Magistrate Judge Harris extrapolated the logic of *Smith*, applied the Fifth Circuit’s reasoning, and concluded that tower dumps fall into the same trap. *See also Spurlock*, 778 F. Supp. 3d at 1145 (“A warrant that authorizes the search of anyone who was in a particular area during a particular time range is

too permeating police surveillance.”). Here, the warrants at issue do not identify specific users or even specify the precise cell sector or towers to be searched. The Government rejects *Smith*’s application and counters this point by arguing that the warrant applications are supported by probable cause and particularity.

“Probable cause is not a high bar.” *District of Columbia v. Wesby*, 583 U.S. 48, 57 (2018) (quotation marks and citation omitted). The Government only needs to show that “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 235, 238 (1983). According to the respective common Affidavits in both the February and June warrant applications, law enforcement identified that “there is a fair probability” that members and associates of a gang carried out a series of related offenses and that it is common for gang members to use cell phones to carry out crimes. This, for the Government, is sufficient to establish probable cause. For other courts—ones outside of the Fifth Circuit—that may be enough. *See United States v. James*, 3 F.4th 1102, 1105 (8th Cir. 2021) (finding that there is probable cause that the suspect used a cell phone in absence of any direct evidence that demonstrates that the suspect used one); *Sherod*, 2025 WL 1736279, at *4 (same). This Court is not so sure. *Compare Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) (requiring that the “search or seizure of a person” requires “probable cause particularized with respect to that person” and that “[t]his requirement cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be”),

with *Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978) (holding that “valid warrants may be issued to search *any* property, whether or not occupied by a third party, at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found”).

The Government’s reliance on *Zurcher* is well-taken—there is a doctrinal difference in searching a person versus searching property. Government’s Motion, Docket No. 40 at 22-26. The Court wonders whether CSLI constitutes a search of a person or property, yet the Court does not need to resolve this issue. If it is the former, then “a person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.” *Ybarra*, 444 U.S. at 91 (citation omitted). If it is the latter, then *Smith*, once again, provides guidance. “[T]he quintessential problem with [geofence] warrants is that they *never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search. That is constitutionally insufficient.” 110 F.4th at 837 (emphasis in original). The Fifth Circuit continues by recognizing that “in the context of CSLI, it must be the case that probable cause is required for ‘each person’s obtained records,’ meaning here ‘each phone number contained within the dump.’” *Id.* at 837 n. 11 (quoting Stephen E. Henderson, Response, *A Rose by Any Other Name: Regulating Law Enforcement Bulk Metadata Collection*, 94 Tex. L. Rev. See also 28, 40-41 (2016)). Nowhere in the Affidavit is there probable cause for each cellular device. Relying on *Smith*, as well as *Ybarra*, this Court too must find that these warrant applications are not supported by probable cause. The Court doubts that *any* tower dump warrant applications could be.

Assuming *arguendo* that there is probable cause, there is also a lack of particularity. By requesting cellular records at six locations that relate to law enforcement’s investigation (i.e., the June warrant applications), the Government argues that “the search warrants are sufficiently particular to allow a reasonable officer to identify items subject to seizure and prevent the ‘general, exploratory rummaging’ that is characteristic of prohibited general warrants.” Government’s Motion, Docket No. 40 at 27. This Court is skeptical.¹³

Both the February and June warrant applications identify specific locations that are pertinent to law enforcement’s investigation of gang activity and criminal acts. These applications seek cellular records, including “phone numbers or unique identifiers, date, time, and duration of the connection, type of transaction, and the cell tower and sector on which the transaction took place.” *Id.* For the Government, this level of detail alone—even “without specifically describing ‘all items authorized to be taken’”—is sufficient to meet the particularity requirement. *Id.* (quoting *United States v. Fulton*, 928 F.3d 429, 434 (5th Cir. 2019)). The Government cites a string of cases, none of which are binding, that have found tower dump warrants to be particular enough. *See James*, 3 F.4th at 1106 (90-minute periods); *Matter of Search of Info. Associated with Cellular Tel. Towers Providing Serv. to [Redacted] Stored at Premises*

¹³ The Government also argues that the “February warrant applications” pass constitutional muster, even though those warrants seek any cellular identifier that is part of the time-location request. The Court notes that the February warrant applications raise even more concern regarding particularity.

Controlled by Verizon Wireless, 616 F. Supp. 3d 1, 10-11 (D.D.C. 2022) (three locations and 30-minute periods); *Savage*, 2024 WL 3295586, at *3 (collecting cases). Given the specified time periods and locations, the Government maintains that law enforcement will know what exactly they can seize. The Government further adds that the June warrant applications are definitively particular since they seek only the identifiers of cellular devices found in two or more locations. The Court is unconvinced.

Both the February and June warrant applications seek time-and-location from cellular towers located in the Jackson metropolitan area. The locations listed in the applications cover areas that are highly frequented, including but not limited to major highways that service thousands of drivers daily. *See* Garrett Grove, *Hate Bad Traffic? Avoid These 7 Areas in Jackson Metro*, WJTV (June 26, 2023, at 1:38 CDT), <https://www.wjtv.com/news/local-news/hate-bad-traffic-avoid-these-7-areas-in-jackson-metro/>. Additionally, the specified time periods for some of the locations fall into rush hour and/or evening hours when there may be even more cars on the road. Taken together, the Court notes that the products of these warrant applications could produce thousands if not tens of thousands of cellular records. The Government would have unfettered access to the locations of an unknowable number of individuals and, given the areas targeted by the Government's investigation, individuals could be located near not only highly-frequented areas—hospitals, major highways, the airport—but also highly-sensitive areas—homes, places of worship, and political centers. *See In re Four Applications for Search Warrants*, 2025 WL 603000, at *6. These warrant applications do not “particularly describ[e] the place to be searched, and

the person or things to be seized.” U.S. Const. amend. IV. The Court finds it hard to imagine that any tower dump warrant application can satisfy the particularity requirement.

By requesting only the identifiers that appear in two or more locations in the June warrant applications, the Government contends that the particularity requirement of the Fourth Amendment is satisfied. The Government hoped that this additional layer of specificity could salvage the shortcomings that Magistrate Judge Harris identified in the February warrant applications. That is not the case, even though other courts have agreed with that approach. *See, e.g., Sherod*, 2025 WL 1736279, at *6 (“The overlap of two or more locations would clearly contribute to tying the search results to the fair probability of criminal activity.”). This Court, though, remains unpersuaded. Regardless of whether there is a reduction of identifiers through cross-checking, *Smith* instructs against accepting this as a basis for constitutionality. 110 F.4th at 837-38. Post facto narrowing cannot justify an unparticularized search. *Id.*

For these reasons, this Court holds that tower dumps are *per se* unconstitutional general warrants. In any event, neither the February warrant applications nor the June warrant applications are supported by sufficient probable cause or particularity.

IV.

Conclusion

The Government cannot have “access to an entire haystack because it may contain a needle.” *In re Four Applications for Search Warrants*, 2025 WL 603000, at *8. “This [C]ourt ‘cannot forgive the requirements of the Fourth Amendment in the name of law enforcement.’” *Smith*, 110 F.4th at 838 (quoting *Berger v. New York*, 388 U.S. 41, 62 (1967)). Law enforcement benefits from tower dumps, as evidenced by recent cases, and this decision may thwart certain criminal investigations. But the gentlemen in Philadelphia knew the Fourth Amendment’s protections would come with costs. The cost to law enforcement is the price we pay to be free from arbitrary Government intrusion into our everyday movements.

The Government’s motion is DENIED.

SO ORDERED, this the 5th day of August, 2026.

s/ CARLTON W. REEVES
United States District Judge