UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION

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

CRIMINAL NO. 3:25-CR-38-CWR-ASH

ORDER

Before the Court are four search-warrant applications for location-and-time based cell-tower data, also known as tower-dump or tower-extraction warrants. The applications seek to obtain from four separate cellular service providers a list of phone numbers and identifiers for cellular devices that connected to cell towers covering nine locations during specific windows of time ranging from ten minutes to one hour for each location. The applications also request information about all communications made using those towers during the specified times.[1] The time windows and locations correspond to crimes the Government suspects were committed by members of a violent street gang. Based on the Fifth Circuit's recent decision in *United States v. Smith*, 110 F.4th 817, 820 (5th Cir. 2024), in which the court concluded that geofence warrants are per se "unconstitutional under the Fourth Amendment," the Court concludes these tower-dump search warrants cannot be issued consistent with the Fourth Amendment. For the reasons explained below, the Court therefore declines to issue the warrants.

I. Background

According to the four identical affidavits of an FBI Special Agent supporting the search-warrant applications, law enforcement suspects the involvement of various members of a violent

[1] The applications also seek information for communications beginning before or ending after the specified intervals if any portion of the communications occurred within the requested windows of time.

street gang—including seven named in the applications—in numerous homicides, shootings, and vehicle thefts occurring over a 14-month period in urban and suburban areas. *See generally* Aff.

The Government has asked the Court to authorize the collection of data from every user of a cellular device that connected to any of the cell towers providing service to the locations of those nine incidents "to help identify or eliminate suspects" by pinpointing individuals whose devices "were in the general vicinity of" the crime scenes. Aff. ¶ 58.[2] In particular, for each cell tower providing service to the described locations,[3] the Government seeks

> records and other information (not including the contents of communications) about all communications made using the cellular tower(s) . . . during the corresponding timeframe(s) listed . . . , including records that identify:
>
> a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower ("the locally served wireless device") that registered with the cell tower . . . ;
>
> b. for each communication, the "sector(s)" (i.e. the face(s) of the tower(s)) that received a radio signal from the locally served wireless device;
>
> c. the date, time, and duration of each communication; . . .
>
> d. the source and destination telephone numbers associated with each communication (including the number of the locally served wireless device and the number of the telephone that transmitted a communication to, or to which a communication was transmitted by, the locally served wireless device; and
>
> e. the type of communication transmitted through the tower (such as phone call or text message).

[2] "[C]ellular service providers maintain antenna towers ('cell towers') that serve and provide cellular service to devices that are within range of the tower[s'] signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data." Aff. ¶ 54.

[3] Following submission of its memorandum, the Government explained in response to the Court's question that it is possible that multiple towers for a given provider may service devices in a particular location, but that a cellular device typically connects to the tower providing the strongest signal. A device, however, "does not always utilize the cell tower that is closest to it." Aff. ¶ 54.

Id. at Attachment B. Thus, while the Government's aim is to identify or rule out suspects in the crimes that took place at each location, it is asking the Court to give it access to information about every communication in the covered time and area made by every person, including more detailed location data (beyond the address serviced by a given tower) that the "sector" information will provide. In terms of the temporal scope of the Government's request, each warrant application seeks data for devices connecting to the towers serving the nine locations for a combined total of 220 minutes. So the Government wants the Court to require the four cellular providers to provide data for a total of 880 minutes—or more than 14 hours—for every device connecting to any of the towers serving those locations.

The applications confirm that "[t]he records obtained by the government through these warrants will likely be voluminous and will include the cellular telephone identifiers of otherwise innocent and uninvolved individuals." *Id.* ¶ 59. The Government states that it will retain this information through the conclusion of any prosecutions (including through final appeals), at which time it will "dispose of any extraneous records pertinent to uninvolved, innocent third parties." *Id.* It also states that it will make no investigative use of that innocent-party information absent a court order. *Id.* The Government does not seek the contents of any communications. *Id.* at Attachment B.

The Court requested that the Government address the Fifth Circuit's recent *Smith* decision. The Government submitted a memorandum briefing its position. That memorandum is filed in the record along with the four applications.[4]

[4] The applications involve an ongoing investigation so those applications and the Government's memorandum are filed under seal.

II. Analysis

A. The requested warrants will result in a search under the Fourth Amendment.

The initial question is whether a tower dump is a search within the meaning of the Constitution.[5] The Fourth Amendment guarantees individuals the right "to be secure in their persons, houses, papers, and effects, against *unreasonable searches* and seizures." U.S. Const. amend. IV (emphasis added). "The 'basic purpose of this Amendment' . . . 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" *Carpenter v. United States*, 585 U.S. 296, 303 (2018) (quoting *Camara v. Mun. Ct. of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967)). The Supreme Court has "established that 'the Fourth Amendment protects people, not places,' and expanded [its] conception of the Amendment to protect certain expectations of privacy as well." *Id.* at 304 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Court] ha[s] held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

In *Carpenter*, the Supreme Court found that the government's request for as few as 7 days of the defendant's cell-site location information ("CSLI") from his wireless carriers "provide[d] a comprehensive chronicle of [his] past movements" and "was a search within the meaning of the Fourth Amendment." *Id.* at 300, 316. Prosecutors identified Carpenter as one of several potential suspects in a series of robberies and obtained "two orders directing Carpenter's

[5] By 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.

wireless carriers . . . to disclose 'cell/site sector [information] for [Carpenter's] telephone[] at call origination and at call termination for incoming and outgoing calls' during the four-month period when the string of robberies occurred." *Id.* at 302. Although the Government requested 152 days of CSLI from the first provider and 7 days from the other, the Government was able to obtain only 127 days and 2 days of data respectively from the providers. *Id.*

In considering whether the acquisition of "12,898 location points cataloging Carpenter's movements"—"an average of 101 data points per day"—constituted a search under the Fourth Amendment, the Court first noted that a majority had "already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Id.* at 302, 310 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J. concurring in judgment); *id.* at 415 (Sotomayor, J., concurring)). "The Court then expressed concern with the government having unfettered access to CSLI, noting that this data provides 'an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."'" *Smith*, 110 F.4th at 831–32 (quoting *Carpenter*, 585 U.S. at 311 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring))). The Court noted that, "in contrast to a GPS device attached to a person's car, a cell phone 'faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.'" *Id.* at 832 (quoting *Carpenter*, 585 U.S. at 311). Given all of this, the Court concluded that the defendant in *Carpenter* had a "reasonable expectation of privacy in the whole of his physical movements" such that a Fourth Amendment search had occurred. *Carpenter*, 585 U.S. at 313.

The Court reached this conclusion despite a line of cases holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at

308 (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)). The Court distinguished these third-party-doctrine decisions by pointing out the "world of difference between the limited types of personal information addressed in [those cases] and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.* at 314. The Court also explained that "[c]ell phone location information is not truly 'shared' as one normally understands the term":

> In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley* [*v. California*,] 573 U.S.[373, 385 (2014)]. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates.

Id. at 315. The Court thus concluded that "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." *Id.* (quoting *Smith*, 442 U.S. at 745).

Last year, the Fifth Circuit applied *Carpenter*'s logic to assess whether "the use of geofence warrants . . . is unconstitutional under the Fourth Amendment." *Smith*, 110 F.4th at 820. The court began by describing geofence warrants:

> "[l]aw enforcement simply specifies a location and period of time, and, after judicial approval, companies [such as Google] conduct sweeping searches of their location databases and provide a list of cell phones and affiliated users found at or near a specific area during a given timeframe, both defined by law enforcement."

Id. at 822 (quoting Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2509 (2021)). In *Smith*, the geofence warrant sought location data for a one-hour period "within a geofence covering approximately 98,192 square meters" around the scene of a robbery

in a rural area of DeSoto County, Mississippi. *Id.* at 827. The warrant in *Smith*, which led to Google searching its "592 million accounts[,] returned three anonymous device IDs within the requested parameters." *Id.*

The Fifth Circuit noted that "[m]any of the concerns expressed . . . in . . . *Carpenter* . . . are highly salient in the context of geofence warrants." *Id.* at 832–33. In particular, "[a]s [the *Carpenter* Court] explained, modern cell phones enable the government to achieve 'near perfect surveillance'; 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 (quoting *Carpenter*, 585 U.S. at 311–12). The court further acknowledged that geofence "technology provides more precise location data than either CSLI or GPS." *Id.*

It then explained that it was not the first Court of Appeals to consider "whether geofencing is a 'search' subject to the Fourth Amendment": a panel of the Fourth Circuit concluded it was not in *United States v. Chatrie*, 107 F.4th 319, 332 (4th Cir. 2024) (applying third-party doctrine and concluding that the defendant "knowingly and voluntarily chose to allow Google to collect and store his location information" such that he had no "reasonable expectation of privacy in this information").[6] The Fourth Circuit reached its decision, in part, because Google users must "opt[] in to Location History" to enable Google to "track [their] location[s]." *Id.* at 331. The Fifth Circuit disagreed that this made geofence searches meaningfully different from the search of CSLI data in *Carpenter*: "As anyone with a smartphone can attest, electronic opt-in processes are hardly informed and, in many instances, may not even be voluntary." *Smith*,

[6] Notably, the Fourth Circuit has granted a petition to rehear *Chatrie* en banc. *United States v. Chatrie*, No. 22-4489, 2024 WL 4648102 (4th Cir. Nov. 1, 2024). In *Smith*, the Fifth Circuit denied the Government's petition for rehearing en banc. *United States v. Smith*, No. 23-60321, Order on Petition for Rehearing En Banc (5th Cir. Jan. 14, 2025). *Smith* is binding precedent in the Fifth Circuit.

110 F.4th at 835. The court thus concluded that "*Carpenter*'s application to the third-party doctrine in this case is straightforward": "while cell phone data is held by private corporations, on a practical level, it 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.* at 834 (citing *Carpenter*, 585 U.S. at 315). In other words, the court concluded that the third-party doctrine did not take the Government's acquisition of data from Google outside the ambit of the Fourth Amendment.

Following *Carpenter*'s logic, the Fifth Circuit in *Smith* ultimately held that a search within the Fourth Amendment had occurred pursuant to the geofence warrants: "Given the intrusiveness and ubiquity of Location History data," the defendants had "a 'reasonable expectation of privacy' in their respective data" such that "law enforcement . . . *did* conduct a search when it sought Location History data from Google." *Id.* at 836.

Applying the rationale the Supreme Court articulated in *Carpenter* as interpreted by the Fifth Circuit in *Smith*, the Court concludes that a tower dump is a search under the Fourth Amendment. The warrant applications here seek information identical to that sought in the geofence warrant in *Smith*: "a list of cell phones and affiliated users found at or near a specific area during a given timeframe, both defined by law enforcement." *Id.* at 822 (quoting Note, *Geofence Warrants*, 134 Harv. L. Rev. at 2509).[7] Just as an individual has "a legitimate

[7] In its memorandum, the Government attempts to distinguish *Smith* by noting that "[f]or Google to comply with the geofence warrant, it had to 'search each account in its entire [database]—all 592 million—to find responsive user records.'" Mem. at 2 (quoting *Smith*, 110 F.4th at 824). But the invasiveness of geofence location data in *Smith* was not tied to the breadth of the search Google performed to identify responsive records. Instead, the Fifth Circuit concluded that "[g]iven the intrusiveness and ubiquity of Location History data, [the defendants] ha[d] a reasonable expectation of privacy in their respective data." *Smith*, 110 F.4th at 836 (internal quotation marks omitted). Those same concerns are present here and give rise to cellular device users' reasonable expectation of privacy in their data that would be revealed by

expectation of privacy in the record of his physical movements as captured through CSLI," he has a reasonable expectation of privacy as to the record of his location at particular moments in time that a tower dump would reveal.[8] *Carpenter*, 585 U.S. at 310; *see Smith*, 110 F.4th at 833.

Carpenter did not directly address whether a request for *less* data would constitute a search. Neither the Government's warrant applications nor the warrant in *Smith* span the same amount of time as the location data collected in *Carpenter*—as many as 129 combined days or as few as 2 days considering the narrower request. *Carpenter*, 585 U.S. at 302.[9] *Smith*, however, teaches that the *quantity* of location data points does not control: "While 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. "Plus, such location tracking can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences." *Id.*

---

the Government's requested warrants.

[8] The Government argues that it is not seeking users' location data in the same way the prosecutors in *Smith* and *Carpenter* did. But the data the Government wants from the cellular providers is tied to particular locations and seeks tower sector data to more narrowly pinpoint users' whereabouts. The warrant in *Smith* specified the point of origin for Google's geofence, and so too the Government's warrant applications specify nine points of origin for the tower dumps. The affidavits supporting the applications indicate that the data "will permit investigators to determine . . . the path of travel of the suspects," which further confirms that the Government seeks location data. Aff. ¶ 52. The fact that the Government may get less precise data in this case than it received in *Smith* does not alter the analysis. Improvements in location-tracking technology do not erase the concerns *Carpenter* raised about CSLI data. And *Smith*'s reasoning about the privacy implications of even a snapshot of data apply equally here. The Court concludes the Government is seeking location data and its warrants therefore implicate the privacy concerns embodied in *Carpenter* and *Smith*.

[9] But there are similarities between the Government's request here and those in *Carpenter*. The CSLI obtained in *Carpenter* averaged to "101 data points per day," which equates to a little over 4.2 per hour. *Id.* This illustrates that the Government's warrant applications here need not obtain more than a few data points per person per half hour to exceed the rate of collection in *Carpenter*.

As a source cited approvingly in *Smith* noted,

> [E]ven a brief snapshot can expose 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," or a location other than home during a COVID-19 shelter-in-place order.

Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 Stan. L. Rev. 385, 408 (2022) (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)), *quoted in Smith*, 110 F.4th at 833. Here, based on a review of publicly accessible maps, the areas within one mile of each of the Government's specified locations[10] include residential neighborhoods, a mall, medical clinics, schools, shopping centers, a supermarket, churches, a courthouse, hotels, interstate highways, a train station, and an airport. It is unclear how *many* people are implicated by the Government's requested tower dumps, but it is plausible the total will easily exceed the three people in *Smith* by hundreds if not thousands given the population density of the covered areas.[11]

[10] In considering a request for location information—whether in the form of CSLI, a geofence, or a tower dump—*Carpenter* is silent about the import (if any) of geographic scope. *Smith* at least provides a point of comparison. The geofence warrant in *Smith* covered approximately 98,192 square meters for a one-hour period. *Smith*, 110 F.4th at 827. Following submission of its memorandum, the Government explained in response to the Court's question that cell tower range is dependent on a number of variables, such as tower strength and geography, but it can be between 1–1.5 miles. Even assuming the lower estimate, this would translate to a circular area comprising approximately 8,136,688 square meters for between 10 minutes to 1 hour for each tower.

[11] The Government argues that its warrant applications are distinguishable from the geofence warrant in *Smith* because they will "yield[] data that is significantly less granular than a geofence." Mem. at 3. But as the Fifth Circuit in *Smith* noted, "the Supreme Court's analysis of whether the government's access of the defendant's CSLI impeded his reasonable expectation of privacy was *not* based on a review of the specific results of the search in that case. Rather, the Supreme Court analyzed the *general capabilities* of CSLI, and asked whether the *ability* for CSLI 'to chronicle a person's past movements through the record of his cell phone signals' created an expectation of privacy." *Smith*, 110 F.4th at 834 n.8 (quoting *Carpenter*, 585 U.S. at 309) (additional citation omitted).

That brings us to the third-party doctrine. An individual's expectation of privacy in the record of his or her physical location is not "overcome" by "the fact that the Government [will] obtain[] the information from a third party" with whom cell phone users share their data. *Carpenter*, 585 U.S. at 315. The Government's tower-dump warrant applications do not implicate the sort of opt-in procedure that split the Fourth and Fifth Circuits in the geofence cases. Instead, the application of the third-party doctrine in this case is governed by *Carpenter*, which concluded the doctrine did not apply "to the collection of CSLI." *Carpenter*, 585 U.S. at 315 (explaining "[c]ell phone location information is not truly 'shared' as one normally understands the term" and that "in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements" (quoting *Smith*, 442 U.S. at 745)). Because cellular device users have a reasonable expectation of privacy in the location data revealed in a tower dump, a tower dump is a search under *Smith*'s interpretation of *Carpenter* and the Fourth Amendment.

B. The requested warrants fail to satisfy the Fourth Amendment.

Having concluded that a tower dump is a search, the Court turns to whether the Government's warrant applications are "supported by probable cause and particularity." *Smith*, 110 F.4th at 836; *see* U.S. Const. amend. IV ("[N]o 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."). The Fourth Amendment was adopted in "response to 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." *Smith*, 110 F.4th at 836 (quoting *Riley*, 573 U.S. at 403); *see id.* ("'General warrants' are warrants that 'specif[y] 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.'" (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981))). To satisfy the Fourth Amendment, "a search or seizure of a person must be supported by probable cause particularized with respect to that person."[12] *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Critically, "[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." *Id.* "[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." *Id.*

With this framework in mind, the Fifth Circuit in *Smith* concluded that "[g]eofence warrants present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Smith*, 110 F.4th at 837 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). The court noted that geofence warrants "*never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search" and concluded "[t]hat is constitutionally insufficient." *Id.* The court quoted favorably from a law review article that supported its conclusion that geofence warrants do not satisfy the Fourth Amendment:

> As professor Stephen Henderson explains in his discussion of CSLI, focusing probable cause on the group rather than the individual "would mean that a larger database is always preferred" by law enforcement, because "by definition there will be evidence of crime in that larger set." 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). Doing so

[12] Probable cause for a search "exists when there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute . . . evidence of a crime." *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006). An affidavit supporting a search warrant "must make it apparent, therefore, that there is some nexus between the items to be seized and the criminal activity being investigated." *Id.*

> leads to an "absurd" understanding of probable cause: "[A] prosecutor confident that *a* bank customer is committing tax fraud could access the combined records of *all* customers of that bank because, somewhere in there, she is very sure is evidence of crime." *Id.* at 41. Henderson argues, 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.*

Smith, 110 F.4th at 837 n.11.

For the reasons the Fifth Circuit articulated in *Smith*, the Court concludes that the Government's tower-dump warrant applications are not supported by probable cause and particularity. For starters, while the Government has some idea of who *may* have been involved in one or more of the crimes—the affidavits supporting the warrant applications list seven potential suspects—the Government has not presented probable cause to believe that any particular individual committed any of the specific crimes described. The warrant applications also arguably present probable cause to believe that the searches will reveal the location data of some *unknown* perpetrators of the crimes. *See* Mem. at 3 (explaining that affidavits describe "the belief that the cell towers will contain evidence of [who committed] the offenses"). But this is not enough. If the Court were to issue the warrants, it would be authorizing the Government to search the data for every cellular *device* (including cell phones) of every single individual near the crime scenes without a showing of probable cause as to each individual. *See Ybarra*, 444 U.S. at 92 n.4 ("[A] warrant to search a place cannot normally be construed to authorize a search of each individual in that place.").[13]

[13] *Carpenter* characterized its decision as "a narrow one": "We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Carpenter*, 585 U.S. at 316. The Supreme Court's reticence to address other technologies does not authorize their use.

Stated another way, the Government is essentially asking the Court to allow it access to an entire haystack because it may contain a needle. But the Government lacks probable cause both as to the needle's identifying characteristics and as to the many other flakes of hay in the stack. And unlike in *Smith*, where only three devices turned up in the geofence in rural DeSoto County, Mississippi, the haystack here could involve the location data of thousands of cell phone users in various urban and suburban areas. As in *Smith*, the tower-dump warrant applications "present the exact sort of 'general, exploratory rummaging' that the Fourth Amendment was designed to prevent." *Smith*, 110 F.4th at 837 (quoting *Coolidge*, 403 U.S. at 467). And because they are "general warrants," they are "categorically prohibited by the Fourth Amendment." *Id.* at 838.[14]

III. Conclusion

This Court is duty-bound to apply *Smith* as binding precedent. *See United States v. Rahimi*, 117 F.4th 331, 334 (5th Cir. 2024) (Ho, J., concurring) (explaining "[i]nferior courts have no such luxury" to adjust or amend precedents, but must follow precedents "whether we agree with them or not—and whether we expect the [higher c]ourt itself to follow them or not"). This is the case notwithstanding the fact that declining to issue tower-dump warrants "will

[14] The warrant applications are also problematic because of the amount of discretion they vest with law enforcement. Officers will not know which cell phone or phones belong to their suspects until they comb through the lists of all phones in the areas of the crimes and cross reference those lists for commonalities. Even then, this cross-referencing may generate false leads if, for example, an innocent person happened to be in more than one tower dump location at the specified times. The Fourth Amendment does not permit law enforcement to rummage through troves of data and themselves determine the existence of probable cause to support the seizure of that data. *See Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979) (finding warrant authorizing search of adult bookstore not supported by probable cause where affidavit said only that "obscene materials" similar to those purchased by undercover officer "would be found at the store," explaining that "warrant left it entirely to the discretion of the officials conducting the search to decide what items were likely obscene and to accomplish their seizure" and concluding that "[t]he Fourth Amendment does not permit such action").

inevitably hamper legitimate law enforcement interests." *Smith*, 110 F.4th at 841 (Ho, J., concurring) ("[H]amstringing the government is the whole point of our Constitution. . . . Our decision today is not costless. But our rights are priceless."). As explained above, the tower-dump search warrants sought by the Government are materially indistinguishable from the geofence search warrant foreclosed by *Smith*. Accordingly, the Court declines to issue the search warrants.

SO ORDERED AND ADJUDGED this the 21st day of February, 2025.

s/ *Andrew S. Harris*
UNITED STATES MAGISTRATE JUDGE