IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE TOWERS PROVIDING SERVICE TO [redacted] THAT IS STORED AT PREMISES CONTROLLED BY VERIZON WIRELESS	**Case No. 21-sc-59** **Filed Under Seal**

MEMORANDUM OF AUTHORITY IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS FOR CELL TOWER DATA

The United States respectfully submits this memorandum in support of its application for four related cell tower data (sometimes called "tower dump") search warrants to four major cellular service providers (the "Service Providers"). The proposed warrants have ample probable cause: [redacted]. Moreover, the warrants are sufficiently particular: they define specific times and places to be searched at each Service Provider: all cell tower location data records for three brief time periods (totaling less than two hours) within three narrowly-drawn geographic areas [redacted]. These warrants are in line with precedent and warrants issued by other Courts and have no Constitutional (or statutory) defect.

Procedural History

On Saturday, January 9, the government submitted its initial proposed search warrant for

each of four service providers. That day, AUSAs handling the matter had a telephone conference with Magistrate Judge Harvey about his concerns regarding the proposed warrants. To address those concerns, on Sunday, January 10, the government submitted a second proposed search warrant. That day, the lead AUSA had a telephone conference with Magistrate Judge Harvey, who continued to express concerns regarding the proposed warrants. In response, on Tuesday, January 12, the government submitted a third proposed search warrant. In another telephone conference that day, Magistrate Judge Harvey expressed concerns regarding the proposed warrants. At the request of Magistrate Judge Harvey on January 13, 2021, the government filed an application for the issuance of a search warrant and related documents, all of which are substantively identical to what will be submitted to the Court for its consideration. Concurrent with submitting this brief to the Court, the government understands that Magistrate Judge Harvey has filed or will be filing a denial of the government's application for this search warrant.

Legal Authority

Magistrate judges are assigned certain duties and powers to handle criminal matters before a case is assigned to a district judge. D.D.C. CRIM. R. 57.17(a); *see also* 28 U.S.C. § 636(b)(3) (permitting district courts to "assign[] . . . additional duties [to magistrate judges] as are not inconsistent with the Constitution and laws of the United States"). When a party requests review of a magistrate judge's order issued pursuant to one of those powers, that order "may be accepted, modified, set aside, or recommitted to the magistrate judge with instructions, after de novo review by the Chief Judge." D.D.C. CRIM. R. 59.3(b); *see also United States v. Wheeler*, 746 F. Supp. 2d 159, 161 (D.D.C. 2010) (Lamberth, C.J.) (reviewing *de novo* same magistrate judge's order dismissing a criminal complaint for violations of the STA, without addressing magistrate judge's power to exercise this authority).

Probable cause amply supports the search warrants[1] at issue here, sometimes referred to as

---

[1] The government applied for the warrants here out of an abundance of caution. Although (as described herein) the basis to issue a warrant is met, a search warrant is *not* required to obtain the non-content location data at issue which involves a request for less than two hours of location information. The plain terms of the Stored Communications Act ("SCA") authorize the government to obtain by court order (that is, a § 2703(d) order) "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." 18 U.S.C. §§ 2703(c)(1), (d). The location information at issue is not "contents of communications."

Other Courts have found this information may be obtained by a SCA § 2703(d) order, and that doing so raises no Fourth Amendment issue. *See United States v. Walker*, Case No. No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *7-8 (E.D.N.C. July 20, 2020) (distinguishing *Carpenter v. United States*, 138 S. Ct. 2206 (2018), finding that cell tower location data for a particular place and time was properly obtained under § 2703(d) orders, and thus there was "no basis for attaching a Fourth Amendment interest to tower dump CLSI"). Pre-*Carpenter*, other courts also so held. *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) ...*, 42 F. Supp. 3d 511, 512-14 (S.D.N.Y. 2014) (M.J. Francis) (cell tower data available via 2703(d) order); *see also id.* at 515 (rejecting ACLU argument that "the Government's application here raises the spectre of 'wholesale surveillance' .... Such concerns center on the possibility of the Government tracking an individual's (or a number of individuals') every movement over a period of time."); *In the Matter of Application for Cell Tower Records Under 18 U.S.C. § 2703(D)*, 90 F. Supp. 3d 673, (S.D. Tex. 2015) (concurring with M.J. Francis, "conclud[ing] that the SCA authorizes the compelled disclosure of cell tower log data" under § 2703(d) under Fifth Circuit precedent); *but see In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770-71 (S.D. Tex. 2013) (finding such request required a warrant after denying § 2703(d) order).

Notably, *Carpenter* held only that individuals have a reasonable expectation of privacy in "historical cell phone records that provide a comprehensive chronicle of the user's past movements," 138 S. Ct. at 2212 – not information that indicates their presence only at a particular location during a narrow time frame. *See id.* at 2217 n.3 (declining to "decide whether there is a limited period for which the Government may obtain an individual's historical [Cell Site Location Information ("CSLI")] free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."); *id.* at 2220 ("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)."). As the Supreme Court emphasized, its decision was "narrow," *id.* at 2217, and "this case is not about 'using a phone' or a person's movement at a particular time." *Id.* at 2220 (emphasis added). As the Seventh Circuit explained in another cell tower data robbery case, *Carpenter* "did not invalidate warrantless tower dumps which identified phones near one location (the victim stores) at one time (during the robberies)." *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019). The Seventh Circuit

cell tower data warrants, and they are drawn with sufficient particularity.

A. Probable Cause

A valid search warrant must be supported by probable cause, which exists when the information provided to the judge demonstrates "a fair probability" that contraband or evidence of a crime will be found in the particular place to be searched. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). This "practical, common-sense decision" is made based on the "totality of the circumstances." *Gates*, 462 U.S. at 238. Similarly, search warrant applications should be read in a realistic, common-sense fashion, and not in a grudging, hyper-technical manner. *See, e.g., Gates*, 462 U.S. at 236.

"Probable cause 'is not a high bar.'" *Dist. of Columbia v. Wesby*, 136 S. Ct. 577, 586 (2018) (quoting *Kaley v. United States*, 134 S. Ct. 1090, 1103 (2014)). "Probable cause" simply means that there is "a fair probability that contraband or evidence of a crime will be found in the

---

concluded that *Carpenter* "does not help" a robbery defendant who has challenged the cell tower data used to identify him. *Id.*; *see also United States v. Yang*, 958 F.3d 851, 862 (9th Cir. May 4, 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for defendant was not a search under Carpenter because "the information in the database did not reveal 'the whole of [the defendant's] physical movements.'"). In short, because one-time cell tower data information does not fall within the scope of *Carpenter*'s protection for long-term, comprehensive location information, it remains subject to the long-standing principle that an individual retains no reasonable expectation of privacy in information revealed to a third party and then disclosed to the United States. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

More generally, a request for such cell tower location data is like other investigative techniques—such as review of surveillance videos or highway toll information—in which investigators collect information from witnesses to determine who was in the vicinity of a crime. Here, the Service Providers (through their cell towers) observed the location of phone users present near the offenses, and the government is calling upon those companies to disclose their observations. Put simply, collecting information from such a witness – like a homeowner with a home security camera – is not a search.

location to be searched." *United States v. LaMorie*, 100 F.3d 547, 552 (8th Cir. 1996). "[A] warrant is proper so long as the evidence as a whole creates a reasonable probability that the search will lead to the discovery of evidence." *United States v. Smith*, 266 F.3d 902, 904 (8th Cir. 2001) (quoting *United States v. Humphrey*, 140 F.3d 762, 764 (8th Cir. 1998)). The determination of probable cause "turn[s] on the assessment of probabilities in particular factual contexts, not readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 238. After all, an "affidavit need only establish the probability of criminal activity . . . not proof beyond a reasonable doubt." *United States v. Brown*, 584 F.2d 252, 257 (8th Cir. 1978); *see United States v. Reivich*, 793 F.2d 957, 963 (8th Cir. 1986) (noting that the "touchstone is 'probability,' and not 'certainty'"); *Gates*, 462 U.S. at 243-44, n.13.). In other words, the probable cause standard requires only that there be a fair probability that evidence will be found at the place to be searched.

"A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched – the so-called 'nexus' element." *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (quoting *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999)).

Here, the probable cause standard is amply met. First, there is a clear nexus to the crime: [redacted]. Second, there is a "fair probability" that the cell tower data – the place to be searched – will contain evidence of the offense. [redacted] Considering such data as

evidence identifying witnesses who could have seen portions of the offense, there is a near certainty that the cell tower data contains relevant evidence.[2]

B. Particularity

In addition to probable cause, the search must be sufficiently particular or definite. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *United States v. Kail*, 804 F.2d 441, 444-45 (8th Cir. 2011). As one district court considering a cell tower data warrant put it:

> "The degree of specificity required in applying the particularity requirement is flexible and may vary depending on the circumstances and the types of items involved." *Id.* at 445 (internal quotation marks omitted). In other words, the particularity requirement is met if the description of things being sought is "as specific as the circumstances and nature of activity under investigation permit."

---

[2] In a similar context – a geofence warrant requiring Google to identify all devices in a defined geographic area – a court noted the identity of witnesses present as evidence which investigators had probable cause to obtain. *See In the Matter of the Search Warrant Application for Geofence Location Data*, Case No. 20 M 525, 2020 WL 6343084, slip op. at *5 (N.D. Ill. Oct. 29, 2020) (M.J. Harjani) ("There is also probable cause that evidence of the crime will be located at Google because location data on cell phones at the scene of the arson, as well as the surrounding streets, can provide evidence on the identity of the perpetrators and witnesses to the crime. Once the location data is produced and reviewed, the government can obtain subscriber information on those cell phones, which will reveal the identifiers of the potential culprits and witnesses to the events.") (record citations omitted); *id.* at *10 ("it is also vital to repeat that the so-called "uninvolved individual" may actually be a witness to the crime."). *But see In the Matter Of The Search Of: Information Stored At Premises Controlled By Google*, Case No. 20 M 392, 2020 WL 4931052, slip op. at *15 (N.D. Ill. Aug. 24, 2020) (M.J. Fuentes) ("Because the proposed warrant here seeks information on persons based on nothing other than their close proximity to the Unknown Subject at the time of the three suspect shipments, the Court cannot conclude that there is probable cause to believe that the location and identifying information of any of these other persons contains evidence of the offense."); *id.* at *17 ("But the proposed warrant would grant the government far greater discretion, namely, to sort through the location information and derivative identifying information of multiple people to identify the suspect by process of elimination. This amount of discretion is too great to comply with the particularity requirement, and the proposed warrant thus suffers from the same fatal particularity flaw as did the proposed warrants in the first two applications.").

> *United States v. Martin*, 866 F.2d 972, 977 (8th Cir. 1989) (internal citation omitted).

United States v. James, Case No. 18-CR-216 (SRN/HB), 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019). "While warrants 'must describe the objects of the search with "reasonable specificity," the Constitution does not insist that they be "elaborately detailed."' Importantly, particularity turns on what is realistic or possible for the investigation at hand." *See In the Matter of the Search Warrant Application for Geofence Location Data*, Case No. 20 M 525, 2020 WL 6343084, slip op. at *7 (N.D. Ill. Oct. 29, 2020) (M.J. Harjani) (quoting, citing *Archer v. Chisholm*, 870 F.3d 603, 616 (7th Cir. 2017)).

In *James*, the district court found the cell tower data warrants sufficiently particular and rejected defendant's suppression argument that the "warrants allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days," *id.* at *3. There, the cell tower data obtained covered the location of ten (10) different robberies. *Id.* at 1. The analysis for the court was simple:

> [T]he search warrant applications seek information that is constrained—both geographically and temporally—to the robberies under investigation. These constraints are justified by the nature of the investigation—multiple robberies in different geographic areas, carried out by an individual utilizing the same modus operandi. The search warrants were not directed at general searches of the data from those towers, nor did they seek data from towers not geographically relevant to the locations of the robberies during the pertinent time periods.

Id. at *3 (record citations omitted). *See also In the Matters of the Search of Cellular Telephone Towers*, 945 F.Supp.2d 769, 771 (S.D.Tex.2013) (in application involving only one crime scene, issuing warrant for cell tower records, noting that affidavit "demonstrated that the subject of the investigation used a cell phone during the criminal activity in furtherance of the offense. Consequently, there is a nexus between the telephone records sought and the criminal activity

being investigated, especially in light of the narrow, specific date and time that are sought."). In short, there, the Court agreed that even a single tower "dump" may be used to identify a set of suspect phones for further investigation.[3]

In issuing a geofence search warrant (a similar context), Magistrate Judge Harjani found the warrant sufficiently particular, noting that it "particularly describes the place to be searched because it narrowly identifies the place by time and location and is also not overbroad in scope." *Geofence Location Data*, 2020 WL 6343084, slip op. at *7. The warrant was "limited in time" because "the government has identified an approximately 15-30 minute time frame for each [of six] target location[s] where it believes location data will reveal evidence of the crime" and "does not seek location data for days or even hours to track the whereabouts of the perpetrators but rather location data that is tailored and specific to the time of the [offense] incidents only." *Id.* at *7. Similarly, the warrant was "limited in its location" because "[t]he target locations have been narrowly crafted to ensure that location data, with a fair probability, will capture evidence of the crime only." *Id.* at *7. The Court also discussed at length how the warrant was limited in scope, that is, that it been shaped – as here – by the investigation (*i.e.*, identifying particular dates and

---

[3] *Cf. United States v. Walker*, Case No. No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *8 (E.D.N.C. July 20, 2020) (rejecting a suppression motion aimed at two different § 2703(d) orders to obtain cell tower data, noting that "the orders capture CLSI not for one targeted individual for an extended time, chronicling that individual's private life for days, but rather capture CLSI for a particular place at a limited time.") (emphasis in original); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) ...*, 42 F. Supp. 3d 511, 515 (S.D.N.Y. 2014) (approving § 2703(d) order for cell tower data, noting that the government's application "seeks to retrieve phone numbers used during a particular time period in a particular area"); *id.* at 515-16 (noting that "[t]here is no possibility that widespread tracking of the locations of individuals could ensue if the application is granted" and contrasting a particular time and area with "cumulative cell-site location records," such as those that covered two weeks or more).

times). *Id.* at *8 ("Thus, through on-site investigation, open source searches, and surveillance footage, the government has satisfied overbreadth considerations by ensuring that there is probable cause that location data of perpetrators, co-conspirators and witnesses will be collected from Google, and that the scope of the warrant would not result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause."). In sum, the geofence warrant (akin to a cell tower data warrant) could meet particularity requirements when set (as here) to cover defined periods and places directly associated with the crime and narrowed insofar as possible (as here) to avoid any excess coverage of residential areas.[4]

Here, the proposed warrants are narrowly constrained based on the specific dates and locations of the offenses [redacted] and seek data for only a narrow window of time around the specific times the offenses [redacted]. [redacted] Indeed, the Court can reasonably infer that the subject committed the crime of [redacted] at a time when they reasonably

---

[4] *Geofence Location Data* also addressed some common objections raised by commentators. *See, e.g., id.* at *9 ("recogniz[ing] that the target geofence zones drawn have a margin of error" but noting that "the fact that warrants for location data have margins of error does not invalidate them – only reasonableness is required, not surgical precision"). In particular, the opinion noted that "a criticism of geofence warrants is the potential that privacy concerns of uninvolved individuals are impacted, but again the issue is probable cause and particularity, not precision. As an initial matter, the fact that one uninvolved individual's privacy rights are indirectly impacted by a search is present in numerous other situations and is not unusual." *Id.* at- *9. As an example, "when a court authorizes the search of an individual's email account, it includes private emails sent by non-perpetrators that were not intended to be seen by the government, and may contain intimate and personal details, but are nonetheless viewed by government agents in the search for evidence of the crime. . . . In other words, it is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are impacted." *Id.* (citations omitted).

anticipated few people would be present to see them do so. Thus, the warrants are appropriately tailored toward their legitimate and proper investigatory purpose, namely to identify the individual responsible for the offenses. In sum, the search warrants here specifically seek information limited both temporally and geographically to the specific offenses at issue. They are particular; they are not "general" warrants.

Conclusion

WHEREFORE, the Court should issue the requested search warrants.

Respectfully submitted,

MICHAEL R. SHERWIN
ACTING UNITED STATES ATTORNEY
N.Y. Bar Number 4444188

/s/ Stuart D. Allen
Stuart D. Allen
D.C. Bar No. 1005102
Jonathan P. Hooks
D.C. Bar No. 468570
Peter V. Roman
D.C. Bar No. 984996
Assistant United States Attorneys
555 4th Street, N.W.,
Washington, D.C. 20530
Phone: 202-252-7794