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 310 FIRST STREET, SE, WASHINGTON, D.C., 430 SOUTH CAPITOL STREET, SE #3, WASHINGTON, D.C., AND THE VICINITY BETWEEN THEM ON JANUARY 5, 2021 THAT IS STORED AT PREMISES CONTROLLED BY VERIZON WIRELESS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE TOWERS PROVIDING SERVICE TO 310 FIRST STREET, SE, WASHINGTON, D.C., 430 SOUTH CAPITOL STREET, SE #3, WASHINGTON, D.C., AND THE VICINITY BETWEEN THEM ON JANUARY 5, 2021 THAT IS STORED AT PREMISES CONTROLLED BY AT&T CORPORATION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE TOWERS PROVIDING SERVICE TO 310 FIRST STREET, SE, WASHINGTON, D.C., 430 SOUTH CAPITOL STREET, SE #3, WASHINGTON, D.C., AND THE VICINITY BETWEEN THEM ON JANUARY 5, 2021 THAT IS STORED AT PREMISES CONTROLLED BY SPRINT CORPORATION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR TELEPHONE TOWERS PROVIDING SERVICE TO 310 FIRST STREET, SE, WASHINGTON, D.C., 430 SOUTH CAPITOL STREET, SE #3, WASHINGTON, D.C., AND THE

Case Nos. 21-sc-59, 21-sc 60, 21-sc-61, 21-sc-62 (GMH)

Chief Judge Beryl A. Howell

FILED UNDER SEAL

VICINITY BETWEEN THEM ON JANUARY 5, 2021 THAT IS STORED AT PREMISES CONTROLLED BY T-MOBILE, US

MEMORANDUM OPINION AND ORDER

On January 6, 2021, a joint session of the United States Congress convened at the United States Capitol, with Vice President Mike Pence presiding, to carry out the constitutional duty of certifying the vote count of the Electoral College of the 2020 Presidential Election. Shortly before this ritual of democracy was disrupted by a rioting mob that breached the Capitol, two suspected improvised explosive devices ("IEDs") with wires were detected at the headquarters of both the Republican National Committee ("RNC") and the Democratic National Committee ("DNC"), several blocks from the Capitol. In the ensuing investigation to find the person or persons responsible for placing these IEDs at those locations, video footage collected from near the RNC and DNC revealed a potential Subject, who was observed in the vicinity of both buildings on the evening of January 5, 2021, the day before the IEDs were found. This Subject's identity is unknown to law enforcement agencies.

To further the Federal Bureau of Investigation ("FBI")'s efforts to identify the Subject and those responsible for committing possible violations of 18 U.S.C. § 2332a (Use of Weapons of Mass Destruction) and 26 U.S.C. § 5861(d) (Possession of Unregistered Firearm (Destructive Device)), the government seeks to obtain data about communications (not including the contents of communications) initiated in a one-hour period in the relevant area where the Subject was observed, using cellular telephone towers ("cell towers") operated by four major cellular service providers: Verizon Wireless, AT&T Corp., Sprint Corp., and T-Mobile US, Inc. (the "Service Providers"). On January 13, 2021, a Magistrate Judge denied the government's applications for

four related search warrants requiring the Service Providers to disclose the unique cell numbers and identifiers of cellular devices used for a brief period of one hour on the night of January 5, 2021, in the small geographic areas where the Subject was observed. *See* Order at 8, *In the Matter of the Search of Info. Associated with the Cellular Tel. Towers Providing Serv. to 310 First St., SE, Wash., D.C., 430 S. Capitol St., SE #3, Wash., D.C., & the Vicinity Between Them on Jan. 5, 2021 that Is Stored at Premises Controlled by AT&T Corp.,* Case No. 21-sc-60 (GMH) (D.D.C. Jan. 13, 2021) ("MJ Order"), ECF No. 9.[1] The government appealed the MJ Order the same day it was issued, and renewed the applications for issuance of all four warrants by the undersigned Chief Judge. *See* Gov't's Mem. Authority Appls. Search Warrants for Cell Tower Data ("Gov't's Mem.") at 2, ECF No. 5; Appl. for Warrant by Tel. or Other Reliable Elec. Means ("Warrant Appl."), ECF No. 6.[2] For the reasons set forth below, the warrants were approved on January 13, 2021, *see* Search & Seizure Warrant, ECF No. 10, with this Memorandum to follow.

[1] The government submitted substantially similar applications and additional filings in all four cases at issue, and the Magistrate Judge issued a single Order denying all four applications. *See* MJ Order. For clarity, except where otherwise noted, the Court cites only to the filings entered in *In the Matter of the Search of Info. Associated with the Cellular Tel. Towers Providing Serv. to 310 First St., SE, Wash., D.C., 430 S. Capitol St., SE #3, Wash., D.C., & the Vicinity Between Them on Jan. 5, 2021 that Is Stored at Premises Controlled by AT&T Corp.,* Case No. 21-sc-60 (GMH) (D.D.C.).

[2] The provider-specific applications filed by the government in each of the four cases are materially similar and rely on the same affidavit. *See* Appl. for Warrant by Tel. or Other Reliable Elec. Means, *In the Matter of the Search of Info. Associated with the Cellular Tel. Towers Providing Serv. to 310 First St., SE, Wash., D.C., 430 S. Capitol St., SE #3, Wash., D.C., & the Vicinity Between Them on Jan. 5, 2021 that Is Stored at Premises Controlled by Verizon Wireless*, Case No. 21-sc-59 (GMH) (D.D.C. Jan. 13, 2021), ECF No. 4; Appl. for Warrant by Tel. or Other Reliable Elec. Means, *In the Matter of the Search of Info. Associated with the Cellular Tel. Towers Providing Serv. to 310 First St., SE, Wash., D.C., 430 S. Capitol St., SE #3, Wash., D.C., & the Vicinity Between Them on Jan. 5, 2021 that Is Stored at Premises Controlled by Sprint Corp.*, Case No. 21-sc-61 (GMH) (D.D.C. Jan. 13, 2021), ECF No. 6; Appl. for Warrant by Tel. or Other Reliable Elec. Means, *In the Matter of the Search of Info. Associated with the Cellular Tel. Towers Providing Serv. to 310 First St., SE, Wash., D.C., 430 S. Capitol St., SE #3, Wash., D.C., & the Vicinity Between Them on Jan. 5, 2021 that Is Stored at Premises Controlled by T-Mobile US*, Case No. 21-sc-62 (GMH) (D.D.C. Jan. 13, 2021), ECF No. 4.

I. BACKGROUND

A. Factual Background

Two months after the November 3, 2020 presidential election, on January 6, 2021, a joint session of the United States Congress convened at the United States Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election. Warrant Appl., Aff. Supp. Appl. for Search Warrant ("Aff.") ¶ 6, ECF No. 6. The joint session began at approximately 1:00 p.m., with Vice President Mike Pence presiding. *Id.* By 1:30 p.m., the United States House of Representatives and the United States Senate adjourned to separate chambers within the Capitol to resolve an objection raised in the joint session. *Id.* Vice President Pence continued to preside in the Senate chamber. *Id.* Shortly after, "[h]undreds" of "[r]ioters breached the Capitol . . . as both the House and Senate [met]," and mayhem broke out inside the building, putting a temporary halt to the electoral vote count. Rachael Levy et al., *Pro-Trump Mob Force Way into Capitol; D.C. Orders Curfew*, WALL ST. J. (Jan. 6, 2021, 5:45 PM), https://www.wsj.com/articles/as-rioters-again-dispute-trumps-defeat-d-c-police-make-arrests-11609945368?reflink=mobilewebshare_permalink; *see also, e.g.*, Nicholas Fandos & Emily Cochrane, *After Pro-Trump Mob Storms Capitol, Congress Confirms Biden's Win*, N.Y. TIMES (Jan. 6, 2021), https://nyti.ms/3ns7D17 (reporting that, at "about 2:15 p.m., as the House and Senate separately debated the objection [raised in the joint session], security rushed Mr. Pence out of the Senate chamber and the Capitol building was placed on lockdown after the demonstrators surged past barricades and law enforcement toward the legislative chambers").

Just minutes before these events disrupted the certification of the result of the 2020 Presidential Election, according to the government, multiple law enforcement agencies in the Washington, D.C. area received reports concerning two separate suspected IEDs. Aff. ¶¶ 7–8. At approximately 1:00 p.m., a suspected IED was reported at RNC headquarters, located at 310

First Street, SE, in Washington, D.C. *Id.* ¶ 7. Fifteen minutes later, at approximately 1:15 p.m., a second suspected IED with a similar description was reported at DNC headquarters, located at 430 South Capitol Street, SE #3, also in Washington, D.C. *Id.* ¶ 8. The timing, to align with the opening of the joint session, and the locations at which the devices were found, blocks away from the Capitol, raise the suspicion that the IEDs may have been strategically placed to distract and divert law enforcement from the impending mob rush at the Capitol. The two suspected IEDs were similar in appearance; both featured "protruding wires" as well as "an object that resemble[d] the face of a timer." *Id.* ¶ 9. Photographs of the devices indicate that they were made, at least in part, "of property used in interstate commerce including manufactured wires and pipes." *Id.* ¶ 11. Fortunately, the U.S. Capitol Police Hazardous Devices Section responded to the reports and successfully detonated and neutralized both devices before they caused any harm. *Id.* ¶ 10.

In the course of its investigation of who was responsible for the IEDs, the FBI reviewed "video footage collected from locations near the RNC and DNC" and identified a Subject who, the evening before the events of January 6, 2021, was in the vicinity of both locations where the IEDs were found. *Id.* ¶¶ 12–15. The footage shows that, between approximately 7:30 p.m. and 8:00 p.m. on January 5, 2021, the Subject was seated on a bench near DNC headquarters, next to the location where one of the two IEDs was found the next day. *Id.* ¶ 13. He appears to be reaching in and around a backpack. *Id.* Notably, at approximately 7:48 p.m., the Subject can be observed either looking at or using a cell phone while at the intersection of Canal Street, SE and South Capitol Street, SE, close to the DNC. *Id.* Additional video from the same half-hour period captures the Subject traveling, at 7:35 p.m. and again at 7:59 p.m., between the location of the IED later found at the DNC and the location of the IED later found at the RNC. *Id.* ¶ 14.

These recordings indicate that, between 7:30 p.m. and 8:00 p.m., the Subject twice passed through a 3,660 square meter (0.5 square miles) geographical area, demarcated by coordinates, consisting of "a mix of government and business locations." *Id.* Footage recorded slightly later in the evening, between 8:00 p.m. and 8:30 p.m., shows the Subject in the vicinity of the location at the RNC where the IED was found the following afternoon. *Id.* ¶ 15.

B. The Requested Warrants

Drawing on the Subject's use of a cell phone near the DNC, the FBI now seeks to further its investigation into the identity of this individual by obtaining cell tower data. To that end, the government requested four related search warrants that would require the Service Providers to disclose data for thirty-minute periods from cell towers in each of three categories: (1) towers that provided cellular service to 430 South Capitol Street, SE #3 (the location of DNC headquarters), between 7:30 p.m. and 8:00 p.m. on January 5, 2021; (2) towers that provided cellular service to 310 First Street, SE (the location of RNC headquarters) between 8:00 p.m. and 8:30 p.m. on January 5, 2021; and (3) towers that provided cellular service to the 3,660 square meter geographical area through which the subject traveled between 7:30 p.m. to 8:00 p.m. on January 5, 2021. Warrant Appl., Attach. A-2. In particular, the warrants seek "the telephone call number and unique identifiers for each wireless device in the vicinity" of the cell towers during the relevant time periods, *id.*, Attach. B at Part I(A), on the theory that, because the Subject was seen on video to have had possession of a cell phone at the times in question, "there is a strong basis to believe the phone will have connected with a cell tower . . . and thus that the presence of the [S]ubject's phone will be recorded among the cell tower data," Gov't's Mem. at 5.

The technical process by which the cell tower data sought by the government would be collected and processed explains how such evidence may enable the FBI to identify the Subject. Cellular providers maintain records about the wireless devices using cell towers on the

provider's network to send or receive communications, which records may include (1) "the telephone call number and unique identifiers of the wireless device[s]" connecting to a cell tower to send or receive communications; (2) the cell tower and sector (*i.e.*, face of the tower) used for the connections; (3) "the date, time, and duration of the communication"; and (4) "the type of communication (e.g., phone call or SMS text message)" and "the source and destination telephone numbers associated with the communication." Aff. ¶ 26. These records for each cell tower may be "dumped" and "analyzed to identify common cellular numbers utilizing cell towers/sectors consistent with the geographic area and/or locations of interest." *Id.* ¶ 28.

To "provide 360 degrees of coverage," each cell tower has multiple sectors, each of which faces in a different direction. *Id.* ¶ 23. The FBI, in searching the "0.5 mile square of the locations of interest" to the investigation, and based on the total number of cell towers of the Service Providers in the small area, identified "approximately 337 unique cell sectors" that could possibly relate to the investigation, with Verizon Wireless controlling approximately 121 cell sectors; AT&T controlling approximately 143 cell sectors; T-Mobile controlling approximately 42 cell sectors; and Sprint controlling approximately 31 cell sectors. *Id.* ¶ 24. In additional representations made to the Court prior to issuance of the warrants, the government clarified that cell service providers, when asked for cell tower information, typically provide large Excel spreadsheets with the relevant tower, time, location, and connection information organized by connecting device, and that the government takes this raw data and processes it through proprietary software to limit review and analysis to the device data "temporally and geographically [relevant] to the specific offenses at issue." Gov't's Mem. at 10. Additional court orders would be sought for disclosure of information linking the relevant device identifiers

to subscribers and other investigative techniques would be utilized to link the cell tower data to the potential Subject.

C. Procedural History

On January 9, 2021, within three days of the discovery of the IEDs, the government first applied for the four warrants described above. Gov't's Mem. at 1–2. In response to queries from the reviewing Magistrate Judge, the government thereafter submitted three iterations of each of their four requests regarding the Service Providers. *See id.*; Appl. for Warrant by Tel. or Other Reliable Elec. Means, ECF No. 1; Appl. for Warrant by Tel. or Other Reliable Elec. Means ("January 13 Appl."), ECF No. 3. On January 13, 2021, the Magistrate Judge denied the third iterations of all four applications on the grounds first, that "the government ha[d] failed to establish probable cause as required by the Fourth Amendment," MJ Order at 8, and second, that the applications were overly broad with respect to the data sought, *see id.* at 6–7. The government sought review of the MJ Order and renewed its applications for the issuance of the four search warrants and related documents. Gov't's Mem. at 2; Warrant Appl.; *see also* Local Civ. R. 40.7(e) ("[T]he Chief Judge shall . . . hear and determine requests for review of rulings by magistrate judges in criminal matters not already assigned to a district judge."). Following additional responses from the government to queries from the Court, on January 13, 2021, the warrants were approved and issued, with this Memorandum Opinion explaining the Court's reasoning to follow. *See* Search & Seizure Warrant.[3]

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." As this matter

[3] The applications denied by the Magistrate Judge and the approved applications are "substantively identical." Gov't's Mem. at 2; *see also* Warrant Appl., Attachs. A-2, B; January 13 Appl., Attachs. A-2, B.

was not "designate[d]" to a magistrate judge by a district court judge within the meaning of § 636(b)(1)(A) or (B), the order denying the government's application is an exercise of the Magistrate Judge's "additional duties," pursuant to § 636(b)(3), in conjunction with this Court's Local Criminal Rule 57.17(a), under which magistrate judges are granted the "duty and the power" to "[i]ssue search warrants," as well as to "[i]ssue subpoenas . . . or other orders necessary to obtain the presence of parties or witnesses or evidence needed for court proceedings." Local Crim. R. 57.17(a)(3), (10).

Pursuant to Local Criminal Rule 59.3, a "magistrate judge's warrant or order for which review is requested" in a "criminal matter not assigned to a district judge, . . . may be accepted, modified, set aside, or recommitted to the magistrate judge with instructions, after de novo review by the Chief Judge." Local Crim. R. 59.3(a),(b); *see also In re Search of Info. Associated with [redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 U.S. Dist. LEXIS 130153, at *12 (D.D.C. July 31, 2017) (noting that "because this case arises out of the Magistrate Judge's 'additional duties' jurisdiction pursuant to § 636(b)(3), the Magistrate Judge's order is subject to *de novo* review by the district court"). Accordingly, the Magistrate Judge's order is subject to *de novo* review by the district court.

III. DISCUSSION

The government applied for search warrants based on probable cause. Consequently, these requests for cell tower data dumps are evaluated under this standard of the Fourth Amendment, which provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized." U.S. CONST. amend. IV. The government challenges the conclusions underlying the MJ Order denying the applications that, first, the search warrant applications

"fail[] to show there is a fair probability that the requested data will provide evidence in this matter" and therefore do not make the requisite showing of probable cause under the Fourth Amendment, MJ Order at 3, and second, even if probable cause exists, the applications are overly broad and therefore do not meet the Fourth Amendment's particularity requirement for warrants, *see id.* at 6–7. As explained below, the government has presented sufficient evidence to show probable cause, as required by the Fourth Amendment, in support of its requests for the instant search warrants, and these warrants are sufficiently particularized to pass constitutional muster.

After a preliminary review of the current state of the law governing application of the Fourth Amendment to government requests for cell tower data, each of these points is addressed in turn.

A. Fourth Amendment Application to Cell Tower Data

The Fourth Amendment safeguards "'[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.'" U.S. CONST. amend. IV. This right "protect[s] certain expectations of privacy" that arise "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is '. . . reasonable.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). "[O]fficial intrusion into that private sphere [created by a reasonable expectation of privacy] generally qualifies as a search" under the Fourth Amendment and thus "requires a warrant supported by probable cause." *Id.*

At issue in *Carpenter* was the sufficiency, under the Fourth Amendment, of court orders issued pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d), which requires a showing that "falls well short of the probable cause required for a warrant," *id*. at

2221, for the government to obtain historical cell-site location information ("CSLI") for a cell phone used by a suspect in a series of robberies, where the responsive CSLI data spanned a period of 127 days from one service provider and seven days from another provider, *id*. at 2212. The Supreme Court considered "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Id*. at 2211. After answering that question affirmatively, the Court further "conclude[d] that the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id*. at 2221. These conclusions were based on the Court's finding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," *id*. at 2217, noting that such data can provide "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years," *id*. at 2220; *see also id*. at 2217 (noting that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts"). Citing the "world of difference between the limited types of personal information" typically collected by third parties for commercial purposes "and the exhaustive chronicle of location information casually collected by wireless carriers today," *id.* at 2219, the Court "decline[d] to extend" to CSLI the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), explaining that "[g]iven the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection," 138 S. Ct. at 2217; *see also id*. at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The

Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."). At the same time, the *Carpenter* Court characterized its holding as "a narrow one," *id.* at 2220, where it "decide[d] no more than the case before [it]," *id*. at 2220 n.4, summarizing the scope of its ruling to be that "accessing seven days of CSLI constitutes a Fourth Amendment search," *id*. at 2217 n.3.

Notwithstanding that the government seeks search warrants in this matter, it suggests that *Carpenter*'s warrant requirement for CSLI applies only when such records "'provide a comprehensive chronicle of the user's past movements,' [] not information that indicates their presence only at a particular location during a narrow time frame." Gov't's Mem. at 3 n.1 (quoting *Carpenter*, 138 S. Ct. at 2212); *see United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (reasoning that *Carpenter* "did not invalidate warrantless tower dumps . . . which identified phones near one location . . . at one time"). *Carpenter*'s cabined ruling certainly may support that limited reading, but leaves open a range of questions about the application of the Fourth Amendment to CSLI, as the *Carpenter* Court itself acknowledged. For example, the *Carpenter* Court expressly declined to decide "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be," 138 S. Ct. at 2217 n.3, and whether individuals have a reasonable expectation of privacy in "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)," *id*. at 2220, such that the government must seek a warrant based on probable cause before obtaining such data. *See also United States v. Green*, 981 F.3d 945, 958 (11th Cir. 2020) (noting question unresolved by Supreme Court of "whether acquiring [real-time tracking data] constitutes a search"); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) (noting

Supreme Court's unresolved questions whether "the government [can] obtain less than seven days' worth of cell-site location information without a warrant," whether "the government [can] collect cell-site location information in real time or through 'tower dumps' not focused on a single suspect" without a warrant, and whether "other [non-CSLI] business records that might incidentally reveal location information" require a warrant (internal quotations and citations omitted)).

In sidestepping these questions to issue a "narrow" holding, the *Carpenter* Court highlighted the context-specific nature of the Fourth Amendment's application. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2223 (noting that, while *Carpenter*'s ruling requires police to "get a warrant when collecting CSLI to assist in the mine-run criminal investigation," the decision "does not limit [law enforcement's] ability to respond to an ongoing emergency"). Indeed, "[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118–19 (2001) (quoting *Wyoming* v. *Houghton*, 526 U.S. 295, 300 (1999)); *see also Maryland v. King*, 569 U.S. 435, 448 (2013) ("This application of traditional standards of reasonableness requires a court to weigh the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual's privacy." (internal quotations, citations, alteration omitted)); *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) ("The Fourth Amendment commands that searches and seizures be reasonable," which "depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself," and thus "[t]he permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's

Fourth Amendment interests against its promotion of legitimate governmental interests." (internal quotations and citations omitted)).

In short, whether a probable cause warrant is required under the Fourth Amendment for the government to obtain "tower dumps," *Carpenter*, 138 S. Ct. at 2220, for short time periods in circumscribed locations where serious criminal conduct occurred, is murky at best, even though this investigative technique may be critical for prompt identification of a perpetrator. To be sure, such tower dumps do not implicate the significant privacy interests in the form of a "comprehensive record" over a lengthy time period of a targeted individual's movements that animated the *Carpenter* Court's holding. *Id.* at 2217. Thus, some courts have concluded, post-*Carpenter*, that an SCA § 2703(d) order, rather than a warrant, remains sufficient to obtain CSLI in tower dumps for limited time periods of less a few hours. *See, e.g., United States v. Walker*, No. 2:18-CR-37-FL-1, 2020 U.S. Dist. LEXIS 126774, at *22–23 (E.D.N.C. July 20, 2020) (finding "no Fourth Amendment violation when officers obtained the orders" for CSLI, pursuant to SCA § 2703(d), for four 60 to 90-minute time periods over the course of two days, and "no basis for attaching a Fourth Amendment interest to tower dump CLSI [sic]" because such dumps only "capture CLSI [sic] for a particular place at a limited time" and therefore "the privacy concerns underpinning the court's holding in *Carpenter* do not come into play"). By contrast, other courts have concluded that, post-*Carpenter*, a probable cause warrant is necessary to obtain CSLI in a tower dump "constrained to an approximately ninety-minute time frame" on the date, and near the location of, a crime. *United States v. James*, No. 18-cr-216 (SRN/HB), 2018 U.S. Dist. LEXIS 210433, at *5 (D Minn. Nov. 26, 2018).

Confronted with *Carpenter*'s unanswered questions and conflicting authority, the government chose to pursue probable cause warrants here, "out of an abundance of caution,"

while also positing that "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." Gov't's Mem. at 3 n.1 (emphasis in original). The government's approach is prudent.

The applications are next evaluated for their satisfaction of Fourth Amendment requirements, mindful of the overarching reasonableness inquiry requiring consideration of "the promotion of legitimate governmental interests," *King*, 569 U.S. at 448 (internal quotation omitted), that makes such evaluation context specific.

B. All Warrant Requirements Are Satisfied

The Fourth Amendment prescribes that "no Warrants shall issue, but upon probable cause," and that the "place to be searched, and the person or things to be seized" be "particularly describe[ed]." U.S. CONST. amend. IV. Upon a showing by the government that its application satisfies these probable cause and particularity requirements, and a corresponding finding that that there exists "a fair probability that contraband or evidence of a crime will be found in a particular place," *Illinois v. Gates*, 462 U.S. 213, 238 (1983), a search warrant may issue. Here, the government's warrants and supporting applications fulfill the probable cause and particularity warrant requirements and thus the warrants may properly issue.

1. The Warrants Are Supported by Probable Cause

"[T]he task of evaluating probable cause [is] 'a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found[.]" *United States v. Cardoza*, 713 F.3d 656, 659 (D.C. Cir. 2013) (quoting *Gates*, 462 U.S. at 238). This "objective standard," informed by "'a . . . totality-of-the-circumstances analysis,'" *United States v. Burnett*, 827 F.3d 1108, 1114 (D.C. Cir. 2016) (quoting *United States v. Vinton*, 594 F.3d 14, 21 (D.C. Cir. 2010)) (citing

Gates, 462 U.S. at 230–32), reflects the reality that "probable cause is a fluid concept—turning 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 232. In the context of a search warrant application, the probable cause inquiry focuses on whether the application provides "a 'substantial basis' for concluding that 'a search would uncover evidence of wrongdoing'" by "demonstrat[ing] cause to believe that 'evidence is likely to be found at the place to be searched'" and "'a nexus . . . between the item to be seized and criminal behavior.'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (first quoting *Gates*, 462 U.S. at 236; then quoting *Groh v. Ramirez*, 540 U.S. 551, 568 (2004); and then quoting *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967)); *see also, e.g., United States v. Glay*, Crim. Action No. 08-213 (JDB), 2009 U.S. Dist. LEXIS 56236, at *5 (D.D.C. June 30, 2009) (same).

The search warrant applications under review meet this probable cause standard. A clear nexus between the CSLI sought in the cell tower dumps and the criminal activity of placing the two IEDs at the RNC and DNC locations is demonstrated by several critical facts in the government's applications. Specifically, the same Subject is captured on video footage at *both* the RNC and DNC locations, where the two IEDs were found, and traveling in between those locations, between approximately 7:30 PM and 8:30 PM on January 5, 2021, one day prior to the discovery of the IEDs. Aff. ¶¶ 12–15. At the DNC location, the Subject is observed sitting on a bench "next to where the suspected IED was found" and "appears to be reaching in and around a backpack." *Id.* ¶ 13. Furthermore, the Subject is observed looking at a cell phone during this hour-long time period. These observations support the reasonable inference that the Subject's cell phone was on and, consequently, that the cell phone likely connected to one of the Service Providers' cell towers in this discrete area.

The nature, timing and location of the Subject's activities on the evening of January 5, 2021, followed by the discovery of the IEDs at RNC and DNC headquarters mid-day on January 6, 2021, provide a substantial basis to believe both that the Subject was responsible for the IEDs and that the requested cell tower dumps will provide evidence helpful in identifying the Subject, associates present or communicating with the Subject during the relevant time period, and/or potential witnesses. *See, e.g.*, *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* ("*In re Geofence Location Data*"), No. 20 M 525, 2020 U.S. Dist. LEXIS 201248, at *17 (N.D. Ill. Oct. 29, 2020) (granting geofence search warrant, which provides the government with the ability to obtain specific location data for all mobile devices within a delineated area, for Google Location History Information to seek "evidence on the identity of the perpetrators and witnesses to the crime" in an arson investigation). The government's legitimate interest in obtaining such information, given the seriousness of the criminal activity under investigation, *see* 18 U.S.C. § 2332a; 26 U.S.C. § 5861(d), cannot be gainsaid, and the privacy interests implicated by the tower dump, if cognizable under *Carpenter*, are minimal, given the warrants' limited temporal and geographic scope. *See Knights*, 534 U.S. at 118–19; *King*, 569 U.S. at 448; *Houghton*, 526 U.S. at 300. The government has demonstrated probable cause for the requested tower dumps.

2. *The Warrants Meet the Particularization Requirement*

In addition to probable cause, an application for a search warrant must "particularly describe[e]" the scope and object of the proposed search and seizure. U.S. CONST. amend. IV; *see also Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Griffith*, 867 F.3d at 1275. This requirement "ensures that the search will be carefully tailored to its justifications," that is, to the probable cause shown. *Garrison*, 480 U.S. at 84. "Consequently, a warrant with an

'indiscriminate sweep' is 'constitutionally intolerable,'" *Griffith*, 867 F.3d at 1275 (quoting *Stanford v. Texas*, 379 U.S. 476, 486 (1965)), and courts "will hold a warrant invalid when 'overly broad,'" *id.* (quoting *United States v. Maxwell*, 920 F.2d 1028, 1033–34 (D.C. Cir. 1990)). As the proper scope of a warrant is confined to the breadth of the probable cause that supports it, "the requirement of particularity is closely tied to the requirement of probable cause." *Id.* at 1275 (internal quotation and citation omitted). "[A] broader sweep," however, may be permissible "when a reasonable investigation cannot produce a more particular description" prior to obtaining and executing the warrant. *Id.* at 1276 (citing *Andresen v. Maryland*, 427 U.S. 463, 480 n.10 (1976)); *see also, e.g., James*, 2018 U.S. Dist. LEXIS 210433, at *13 (upholding cell tower dump warrants, finding that they met the particularity requirement in light of the "circumstances [and] the nature of the activity under investigation").

Applying this standard in the specific factual context presented here, the warrants are sufficiently particularized as to the location, time, and duration pertinent to the probable cause showing. Each warrant sets out, in Attachment A, the three categories of cell towers from which information is requested, as well as the January 5, 2021 date and thirty-minute time period to which the information should be restricted for each category of cell towers. *See, e.g.*, Warrant Appl., Attach. A-2. The three categories of cell towers are those providing cellular service, on January 5, 2021, to the DNC and RNC and the limited geographic area between them, as delimited by specific coordinates, where the Subject was observed. *Id.* Each warrant further describes, in Attachment B's three sections, the types of information to be seized and how that information will be processed. *See, e.g., id.*, Attach. B. Specifically, the Service Providers are required to disclose, "to facilitate execution of the warrant," *id.*, Attach. B at Part I, the telephone call number and unique identifiers for each wireless device that registered with the tower, along

with the sector (*i.e.*, the face of the towers) receiving a signal from the wireless device, and information indicating the location of the signal within the delimited area set out in Attachment A, *id.*, Attach. B at Part I(A)–(D). The next two sections of Attachment B outline the processing of this disclosed information to focus on identifying evidence of "a person [who] was present at more than one of the dates/times/locations identified in Attachment A (that is, the dates/times/locations of certain offenses under investigation), including evidence that a phone or phone number appeared at more than one of such dates/times/locations," *id.*, Attach. B at Part II(b), plus associates and co-conspirators of the Subject, *id.*, Attach. B at Part II(a), (c), and to weed out information "that does not fall within the scope of" the warrant, which information "will not [be] further review[ed] . . . absent an order of the Court," *id.*, Attach B. at Part III.

In sum, then, the warrants are particularized to cell tower dumps of information from four service providers in a small, discrete geographical area, where the IEDs were discovered and the Subject was observed, and the short distance between those locations, also where the Subject was observed traveling, during the period of 7:30 PM to 8:30 PM on January 5, 2021. The warrants are further particularized and delimited by specific coordinates, totaling 3,660 square meters, with a perimeter of 254 meters, *id.*, Attach. A; Aff. ¶ 14, which coordinates "are drawn to avoid residences and focus on business/commercial areas after the end of the business day," minimizing the capture of data from uninvolved individuals within this targeted radius and individuals outside the half-mile radius, Gov't's Mem. at 9. The warrants thereby focus exclusively on cell tower information collected in the limited relevant area of interest between the RNC and the DNC. *See In re Geofence Location Data*, 2020 U.S. Dist. LEXIS 201248, at *13–14 (finding a proposed geofence warrant sufficiently particular where the government had "structured the geofence zones to minimize the potential for capturing location data for

uninvolved individuals and maximize the potential for capturing location data for suspects and witnesses"). Further, the information sought within this carefully delimited geographic and temporal scope is also particularized and limited to the types of data, *i.e.*, phone numbers and unique device identifiers, that can be used to identify the Subject, associates of that Subject, and potential witnesses in furtherance of the criminal investigation. Finally, the directions as to how the government must handle the tower dump data, including limiting the data that may be seized to the precise terms of the temporal and geographic scope set out in the warrants, provide sufficiently specific guidance that, in these circumstances, satisfies the particularity requirement. *See United States v. Heldt*, 668 F.2d 1238, 1256 (D.C. Cir. 1981) (explaining that "the particularity requirement seeks to assure that 'those searches deemed necessary should be as limited as possible'" and "'nothing is left to the discretion of the officer executing the warrant'" (first quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); and then quoting *Marron v. United States*, 275 U.S. 192, 196 (1927))); *Coolidge*, 403 U.S. at 467 (noting that a main objective of Fourth Amendment particularity requirement is to assure that "searches deemed necessary should be as limited as possible," and the warrant achieves that goal only by directing executing officers to the particular things to be seized).

The MJ Order raised concerns about the warrants' potential overbreadth in capturing "hundreds, if not thousands, of cellphone [sic] identifiers, many of which would not belong to either a suspect or witness." MJ Order at 4–5. This overbreadth concern, which appears to discount both the geographic scope limitations of the warrants, *id*. at 6 (stating "[t]he government has not provided any information on the size of the area served by the over 300 cell sectors"), and the value of the government's effort to analyze the cell tower dump data to identify common

cellular numbers utilizing the cell tower in the relevant area to pinpoint the Subject's movements and identity, *see id*. at 5, is mitigated by two considerations.

First, the small, discrete area from which the data to be seized is largely a commercial area in downtown Washington, D.C., with the data limited to that generated *after* business hours, *see, e.g.*, Warrant Appl., Attach. A-2, and carefully circumscribed with specific geographic coordinates to exclude residences. This necessarily reduces the number of persons whose cell phone identifiers would be subject to collection on nearby cell towers simply because they either reside in the area or work there, particularly in the midst of a pandemic, which has sharply limited the operations of most businesses in the area.

Second, concerns about "what the government is claiming it can do with the data dump," MJ Order at 6, either overlook or reject the effectiveness of the process the government has outlined for analyzing the raw data disclosed by the Service Providers to identify the relevant data for seizure. The warrants demand disclosure of valuable metadata associated with "the telephone number and unique identifiers for each wireless device" connecting to a cell tower, *id.*, Attach. B at Part I(A), to facilitate the government's winnowing from the raw tower dump data to the relevant data subject to seizure. Specifically, the warrants direct that the raw data include date/time/duration information for each wireless device registered with the cell tower as well as important sector information, all of which will enable the government to narrow the raw data to the relevant temporal scope and location where the Subject was observed. Such tailoring of the dataset, as the government clarified to this Court, is accomplished using the FBI's proprietary software, with any data that falls outside of the strict parameters of the warrants' Attachment A to be segregated without further review, absent a court order. *See, e.g.*, *id.*, Attach. B at Part III. As the government advised, Service Providers generally provide cell tower dumps based on the

parameters of date and time periods, without segregating by sector, a task that would require precise investigative details not normally shared with third parties, such as Service Providers.

Finally, the MJ Order's critique that "[t]he government has . . . not provided information about the area of interest," the "size of the area served by the over 300 cell sectors," MJ Order at 6, and the area covered by the cell towers in the given location, *id.* at 7, while correct about the lack of such information, again fails to credit the significance of the metadata associated with the raw tower dump data to help the government narrow the data subject to seizure and analysis, to the extent the Service Providers are unable to limit the raw data production by the circumscribed area in the warrants' Attachment A.

The government has carefully tailored the warrants to the greatest degree possible to obtain cell phone data from the Service Providers to assist in identifying the Subject suspected of leaving two IEDs at the DNC and RNC. Assessing the particularity of the warrants in light of the totality of the circumstances, *Gates*, 462 U.S. at 230, including the seriousness and dangerousness of the criminal activity at issue, the incidental characteristics of the relevant locations, the practical barriers to limiting the information the Service Providers are able to disclose, and the capabilities of the government to segregate from the cell tower dumps the relevant information subject to the warrant, demonstrates that the warrants are sufficiently particularized to provide specific guidance to law enforcement as to what data may be seized and a "fair probability" that evidence of the alleged crime will be discovered through execution of the warrants.

IV. ORDER

For the reasons stated above, the Magistrate Judge's Order is **REVERSED**, and the government's applications for search warrants for cell tower data are **GRANTED**. The

government is **DIRECTED** to review this Memorandum Opinion and Order, and other filings on the Court's docket in this matter, and advise which filings may be unsealed, in whole or in part, with proposed redactions as necessary to protect any ongoing criminal investigations, by May 14, 2021, unless these filings have been unsealed before then.

SO ORDERED.

Date: January 17, 2021

BERYL A. HOWELL
Chief Judge