UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	**Crim. No. 23-CR-184 (RDM)**
JARED LANE WISE,	:	
	:	
Defendant.	:	

GOVERNMENT'S RESPONSE TO SUPPLEMENTAL ARGUMENT SUPPORTING DEFENSE'S MOTION TO SUPRESS EVIDENCE

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits its Opposition to defendant Jared Wise's Supplemental Argument Supporting Defense's Motion to Suppress Evidence. ECF No. 101. Jared Wise ("Wise" or "the defendant") challenges a search warrant issued on January 22, 2021 to obtain cell-tower information from AT&T ("AT&T Cell-Tower Warrant"). The defendant devotes extensive factual background and argument in his supplement on two issues: (1) a geofence-related opinion in *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), a non-binding decision from a different jurisdiction issued more than three years after the government obtained search warrants for location records for devices detected to be inside the United States Capitol building on January 6, 2021; and (2) a fundamental and factual misunderstanding of legal process in this case and the January 6 prosecution overall.

The government now seeks to correct such misunderstandings and provide a comprehensive overview of the timeline in this case, as it relates to this defendant. The defendant's reliance on *Smith* is misplaced because the AT&T Cell-Tower Warrant is not a geofence warrant and the opinion is otherwise not applicable to the facts of this case and the warrants in the January 6 prosecution. Moreover, the AT&T Cell-Tower Warrant, as well as the warrants specific to

defendant Wise, were supported by probable cause and sufficiently particular. The warrants specific to Wise included information about the AT&T Cell-Tower Warrant and accurately described when the government began its investigation into Wise. Furthermore, law enforcement reasonably relied, in good faith, on those warrants to seize evidence. The Court should reject the defendant's arguments without the need for an evidentiary hearing.

I. Background

A. Procedural History

For an exhaustive recitation of the facts related to the defendant's conduct on January 6, 2021, the May 5, 2022 AT&T warrant, the November 23, 2022 AT&T warrant, and the applicable law, the United States respectfully incorporates the United States' Opposition to Motion to Suppress Evidence, ECF No. 56.

B. AT&T Cell-Tower (*i.e.*, "Tower Dump") Warrant

In January 2021, the government sought and obtained a "tower dump" warrant for records kept by AT&T Corporation ("AT&T"), among other cell-phone service providers. A tower dump warrant, as the Court is aware, seeks "records of phones connected to a particular cell tower over a given period." *United States v. Chatrie*, 107 F.4th 319, 329 (4th Cir. 2024).[1]

A warrant affidavit submitted in support of the government's warrant application summarized the government's investigatory steps. It noted that "video footage … appeared to be

[1] The government also sought a geofence warrant to obtain certain mobile-device location information from Google. *See, e.g. United States v. Easterday*, No. 22-cr-404 (JEB), 2024 WL 195828 (D.D.C. Jan. 18, 2024) (denying motion to suppress identification evidence from Google geofence warrant and "conclud[ing] that the warrant process complied with the Fourth Amendment."). *See also United States v. Rhine*, No. 21-cr-0687 (RC), 652 F. Supp. 3d 38 (D.D.C. 2023); *United States v. Cruz*, No. 22-cr-64 (RBW). The Google geofence warrant is not at issue in the instant case.

captured on mobile devices of persons present" at the Capitol on January 6 "depict[ing] evidence of violations of local and federal law." ECF No. 102-3 at ¶ 28. In addition, news footage displayed "[m]any subjects … using a cell phone in some capacity." *Id.* at ¶ 30. The affidavit accordingly concluded that "evidence of the cell-site activity in the towers that are closest to the [Capitol Building] may provide information regarding individuals who were in close proximity to the area of the target offenses." *Id.* at ¶ 32.

The affidavit noted that the Capitol Building has a distributed-antenna system that strengthens and enhances cell coverage within the building. *Id.* at ¶ 34. This system provides no cell service outside the building. *Id*. The affidavit further stated that "cellular providers … routinely and in their regular course of business maintain historical records that allow them to determine which wireless devices used cellular towers on the cellular provider's network to send or receive communications." *Id.* at ¶ 38. The affidavit thus found "reason to believe that the[se] records … would identify which wireless devices were in the vicinity of the riot that occurred at the [Capitol], on January 6, 2021." *Id.* at ¶ 44.

Based on this affidavit, the magistrate judge issued a warrant directing AT&T to search its records pertaining to two cellular towers providing service to the Capitol Building during three periods on January 6, 2021: between 12:00 and 12:15 p.m., between 1:00 and 6:30 p.m., and between 9:00 and 9:15 p.m. January 6. *Id.* at 4-5. For those towers and periods, the warrant directed AT&T to disclose to the government information specifying the telephone call number, the date, time, and duration of each communication, if available. *Id.* at 6. The warrant further provided that

the government would review AT&T's list of devices and identify the accounts for which it sought basic identification and subscriber information.[2] *Id.*

The warrant was signed by the magistrate, and the government served it on AT&T on January 22, 2021.[3]

C. Wise Investigation

From the inception of the January 6 investigation, the FBI has sought the public's assistance in identifying individuals who made unlawful entry into the United States Capitol Building and various other alleged criminal violations, such as destruction of property, assaulting law enforcement personnel, targeting members of the media for assault, and other unlawful conduct, on January 6, 2021, in Washington, D.C.

On or about January 10, 2022, a member of the public contacted the FBI and identified that a former FBI agent entered the Capitol during the January 6 riot. The FBI then interviewed the

[2] The warrant included the 12:00-to-12:15-p.m. and 9:00-to-9:30-p.m. periods as "control" periods – *i.e.*, as periods during which no suspects were unlawfully present within the Capitol – so that any devices present within the Capitol during those periods could be excluded from the target devices for which identifying information was sought at the next step.

[3] Citing a "4/18/2021" "timestamp" in a ".txt file" that summarized AT&T's tower-dump returns pertaining to Wise, Wise speculates that the AT&T Cell-Tower Warrant may have been executed after the execution date specified in the warrant (February 4, 2021). *See* ECF No. 101 at 3-5. As explained above, the AT&T Cell-Tower Warrant was issued on January 22, 2021, and executed on the same date. The printout in Wise's FBI case file reflects a later date because it reflects a query of the Cell-Tower Warrant returns after the tipster in this case provided Wise's phone number. In addition, Wise separately complains (ECF No. 101 at 4) about the timing of the government's discovery production of certain "geofence" materials. That accusation, too, fails for multiple reasons. Wise has failed to identify in any detail which "geofence" materials he is referencing, and, more importantly, "geofence" materials are irrelevant to the AT&T *tower dump* warrant at issue in Wise's case. Finally, and most fundamentally, as Wise acknowledges, January 6 defendants have had access to any "geofence" materials since at least March 2022—more than 13 months before Wise was arrested and more than 14 months before he was indicted.

individual. The member of the public provided identifying information and other information regarding Wise. The individual stated that their last conversation with Wise was in October 2021.[4]

After receiving the tip, the FBI ran Wise's cell phone number (as provided by the tipster) against the returns of the AT&T Cell-Tower Warrant.[5] The text of the document summarizing the initial investigation steps, states that:

> Pursuant to an authorized search warrant, law enforcement obtained records from AT&T for cell towers providing service to the United States Capitol. The target device was identified as having utilized a cell site consistent with providing service to the geographic area that includes the interior of the United States Capitol building in and around the time of the incident.
>
> A record search for telephone number (XXX) XXX-1300 yielded positive results and was active on AT&T towers at approximately 14:15:06, 14:22:06, 14:26:06, and 14:29:16 Eastern Standard Time ("EST") on January 6, 2021.

ECF 102-4.

[4] The defendant states that the individual first provided information to the FBI several months earlier, in October 2021, apparently based on a translation of an interview conducted on or about June 26, 2023. The government's understanding of the conversation is that the individual confirmed that that individual's last conversation with Wise was in October 2021 and the individual contacted the FBI after that time—not that the contact with the FBI took place in October 2021.

[5] Wise repeatedly mischaracterizes the AT&T Cell-Tower Warrant as a "geofence" warrant. Wise's characterization is both incorrect and misleading. As the warrant application and affidavit make abundantly, and as summarized above, the AT&T Cell-Tower Warrant was a tower dump warrant, not a geofence warrant. Tower dump warrants and geofence warrants implicate different data, technologies, and legal analyses. *See infra*. And while the Cell-Tower Warrant information was labeled "Geo Fence Results," in the investigation document as drafted by the investigating agent, that was clearly a clerical error. The evidence provided to the defendant—both in the Relativity database and in discovery provided directly to Wise's counsel—plainly refers to the AT&T Cell-Tower Warrant.

After the matter was converted to a full investigation, the FBI took additional investigative steps, including using legal process to gather more specific information from AT&T, as discussed below.

D. Subsequent AT&T Warrants

As described in the United States' Opposition to Motion to Suppress Evidence, ECF No. 56, as part of its investigation into Wise, the government sought and obtained search warrants for information held by AT&T and associated with the defendant's telephone account. Those warrants were issued on May 5, 2022 and November 23, 2022 (collectively, the "Subsequent AT&T Warrants").

For both Subsequent AT&T Warrants, the government's supporting affidavits referenced, among other evidence, the fact that Wise's cell phone had hit on the AT&T tower dump returns. Specifically, the affidavit in support of the May 5, 2022 AT&T warrant stated, among other things:

> Pursuant to an authorized search warrant, law enforcement obtained records from AT&T for cell towers providing service to the United States Capitol. The target device was identified as having utilized a cell site consistent with providing service to the geographic area that includes the interior of the United States Capitol building in and around the time of the incident.
>
> A record search for telephone number XXX-XXX-1300 yielded positive results and was active on AT&T towers at approximately 14:15:06, 14:22:06, 14:26:06, and 14:29:16 Eastern Standard Time ("EST") on January 6, 2021.

Government's Exhibit A to ECF No. 56 at ¶¶ 40-41.

Similarly, the affidavit in support of the November 23, 2022 AT&T warrant included the following statement:

> Pursuant to an authorized search warrant, law enforcement obtained records from AT&T for cell towers providing service to the United States Capitol. The target devices were identified as having utilized

> a cell site consistent with providing service to the geographic area that includes the interior of the United States Capitol building in and around the time of the incident.
>
> A record search for telephone number XXX-XXX-1300 revealed that it was active on AT&T towers at approximately 14:15:06, 14:22:06, 14:26:06, and 14:29:16 Eastern Standard Time ("EST") on January 6, 2021, within 15 minutes of the initial breach of the Capitol building and the USCP ordering the evacuation of Vice President Mike Pence and members of Congress.

Government's Exhibit B to ECF No. 56 at ¶¶ 41-42.

The affidavits in support of the Subsequent AT&T Warrants also explained that "[o]n or about January 26, 2022, an individual ("UI"), whose identity is known to the FBI, reported to an FBI Washington Field Office Supervisory Special Agent, that WISE told UI that WISE was inside the United States Capitol building on January 6, 2021." Government's Exhibit A to ECF No. 56 at ¶ 38; *see also* Government's Exhibit B to ECF No. 56 at ¶ 39. The affidavit further stated that the individual provided the defendant's identifiers, including his phone number. *Id.*

In other words, all warrants referenced the AT&T tower dump review.

II. Argument

The defendant's arguments are legally and factually without merit. Conflating the AT&T Cell-Tower Warrant with a geofence warrant, Wise urges this Court to adopt the logic of a recent Fifth Circuit decision involving a geofence warrant—but not that decision's actual holding—and suppress the returns of the AT&T Cell-Tower Warrant, as well as its fruit. Wise's contentions fail for a number of reasons. The AT&T Cell-Tower Warrant at issue in this case implicated collection of records from AT&T via a "tower dump"—not a geofence—and tower dumps have long been deemed not to implicate the Fourth Amendment under a straightforward application of the third-party doctrine. Indeed, the Supreme Court's decision in *Carpenter v. United States*, 585 U.S. 296

(2018)—despite narrowing the scope of the third-party doctrine as applied to *some* cell-phone contexts—specifically disclaimed expressing any view that tower dumps constitute a "search" under the Fourth Amendment. *Id.* at 316. Since *Carpenter*, courts have repeatedly reaffirmed that tower dumps do not implicate the Fourth Amendment.

Nor is there merit to Wise's reliance on *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), which—despite denying suppression under the good-faith exception—opined that a "geofence warrant" was an impermissible "general warrant." *Id.* at 838. Again, this case involves only a tower dump. It does not involve a geofence or Google's "Location History" data. The Fifth Circuit's *Smith* case, in contrast, addressed only a Google geofence. And *Smith* specifically relied on "the intrusiveness and ubiquity of [Google's] Location History data" in finding that that geofence implicated the Fourth Amendment. 110 F.4th at 836. Contrary to Wise's contentions, *Smith*'s ruling is not merely non-binding on this Court; more fundamentally, its logic does not carry over to the less precise and less ubiquitous location data at issue in tower dumps. And, in any event, *Smith* was wrongly decided even as to geofences. Every judge to have considered the constitutionality of the January 6 geofence warrant has sustained it. *See United States v. Easterday*, No. 22-cr-404 (JEB), 2024 WL 195828 (D.D.C. Jan. 18, 2024); *United States v. Rhine*, No. 21-cr-0687 (RC), 652 F. Supp. 3d 38 (D.D.C. 2023); *United States v. Cruz*, No. 22-cr-64 (RBW). And the Fourth Circuit similarly held, in another recent geofence case, that "the government did not conduct a Fourth Amendment search when it obtained two hours' worth of [that defendant's] location information, since he voluntarily exposed this information to Google." The Fourth Circuit recently reached a similar conclusion in *United States v. Chatrie*, 107 F.4th 319, 322 (4th Cir. 2024).

A. The AT&T Cell-Tower Warrant Did Not Infringe Upon Wise's Reasonable Expectation of Privacy

1. Governing Legal Landscape

To assert a Fourth Amendment claim, the defendant must demonstrate "a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). To establish a legitimate privacy expectation, a defendant must demonstrate that his conduct exhibits "an actual (subjective) expectation of privacy," showing that "he seeks to preserve something as private." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (brackets and citation omitted). A defendant must further demonstrate that his expectation is "one that society is prepared to recognize as 'reasonable.'" *Id.* (citation omitted). "[D]efendants always bear the burden of establishing that the government violated a privacy interest that was protected by the Fourth Amendment." *United States v. Sheffield*, 832 F.3d 296, 305 (D.C. Cir. 2016). "Without a reasonable expectation of privacy, a Fourth Amendment search does not occur." *Stewart v. Evans*, 351 F.3d 1239, 1243 (D.C. Cir. 2003) (internal quotation marks and citation omitted).

Applying these principles, the Supreme Court has long recognized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979). This includes business records of banks, *see United States v. Miller*, 425 U.S. 435, 440-443 (1976), and records of telephone numbers that a person contacts or receives communications from, *see Smith*, 442 U.S. at 742-744 (1979). Under this third-party doctrine, a bank or phone customer "assume[s] the risk that the company w[ill] reveal [the information] to the police." *Id.* at 744.

In *Carpenter*, the Supreme Court held that this doctrine did not apply to the government's collection of at least seven days' worth of cell-tower location information from a cellular provider.

585 U.S. at 310 & n.3; *see also id*. at 311 (noting that the government obtained 127 days of data). Although cell-tower records are created and maintained by third-party carriers, *id*. at 313, the Court "decline[d] to extend *Smith* and *Miller* to cover the[] novel circumstances" at issue, *id*. at 309—that is, the electronic tracking of a device for at least seven days over a potentially unlimited geographic area. The Court emphasized "the unique nature of cell phone location records," which provide "a detailed and comprehensive record of the person's [physical] movements" resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Id*. at 309, 312. The Court thus held that the government's collection of cell-tower records documenting a particular phone's location over an extended period and geographic area invades the user's reasonable expectation of privacy. *Id*. at 313.

In doing so, the Court emphasized that the information in *Carpenter* was "not about 'using a phone' or a person's movement at a particular time," but instead implicated "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." 585 U.S. at 315. The Court further stated that its holding was "a narrow one" and did not cover "tower dumps" where the government seeks "a download of information on all the devices that connected to a particular cell site during a particular interval." *Id*. at 316; *see also United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))").

2. Wise Lacks a Reasonable Expectation of Privacy Under *Carpenter* in AT&T's Limited Cell-Site Location Records at Issue

Under *Carpenter*'s reasoning, the AT&T Cell-Tower Warrant likewise did not infringe upon Wise's reasonable expectation of privacy because it did not seek information that

comprehensively chronicled his movements for an extended period of time or an extended geographic area. Rather, the data revealed the presence of Wise's phone inside one location (the Capitol Building) during a discrete hours-long interval on January 6. Society has long accepted cell tower information—where law enforcement monitors a suspect "for a brief stretch"—as reasonable. *Carpenter*, 585 U.S. at 310; *see also United States v. Chatrie*, 107 F.4th 319, 334 (4th Cir. 2024) ("[A]ccess to a person's short-term movements does not invade his reasonable expectation of privacy."). It was not the sort of "all-encompassing record of the holder's whereabouts" and "intimate window into a person's life" that concerned the Court in *Carpenter*, 585 U.S. at 311. *See United States v. Lauria*, 70 F.4th 106, 129 n.12 (2d Cir. 2023) ("*Carpenter*'s ruling gives no reason to doubt that law enforcement officers lawfully could have obtained more limited cell tower information—for example, information simply telling whether [the defendant's] cell phone was in the vicinity of the Mahopac store at or near the time of the robbery—without need to show probable cause."); *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (explaining that *Carpenter* does not govern "short-term tracking of public movements—akin to what law enforcement could do prior to the digital age") (internal quotation marks and brackets omitted).

Indeed, after *Carpenter*, courts have continued to hold—as the Supreme Court itself suggested in *Carpenter*, *see* 138 S. Ct. at 316—that the government may obtain the temporally limited, geographically limited cell-site information at issue in tower dumps without implicating the Fourth Amendment. *See, e.g.*, *United States v. Walker*, 2020 WL 4065980, at *8, (E.D.N.C. July 20, 2020) (finding "no basis for attaching a Fourth Amendment interest to tower dump" of limited duration and geographic range because such queries only "capture [cell-site location data] 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"); *United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (holding that "*Carpenter* itself . . . did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies)) because the Supreme Court declined to rule that these dumps were searches requiring warrants"); *United States v. Walker*, 2020 WL 4065980, at *8 (W.D.N.C. July 20, 2020); *United States v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021).[6] Consistent with *Walker* and *Adkinson*, *Carpenter* does not apply here because the government obtained location information from AT&T covering only a discrete location at a discrete time.

The tailored nature of the location information in this case—showing the mobile devices present within one location (the Capitol Building) during a discrete six-hour period—underscores that conclusion. First, the Capitol Building—the seat of this country's legislative branch—is secured 24 hours a day. Only authorized people with appropriate identification are allowed access. "[C]onstituent meetings, lobbying sessions, committee hearings, and the like … are typically scheduled and controlled by Senators or Representatives." *United States v. Nassif*, 97 F.4th 968, 976 (D.C. Cir. 2024) (internal quotation marks and citation omitted). "A visitor wishing to tour the historic Capitol Building … must book a tour, enter through the Capitol visitor center between 8:30 a.m. and 4:30 p.m., proceed through security, and subject all carried items to inspection." *Id.* at 977. And surveillance cameras monitor visitors inside the building. Given these security features, no visitor can expect that his or her presence within the Capitol Building and reason for being there will remain a secret. Cell-tower data showing that individual's presence within the

[6] *But see United States v. Medina*, 712 F. Supp. 3d 226 (D. R.I. 2024) (holding that a warrant was required for a tower dump). *Medina* is, nonetheless, instructive, given that here, the government *did* obtain a warrant, and – in any event – the Court applied the good-faith exception to evidence obtained from the original order.

Capitol Building is therefore not likely to capture any private details about his or her activities or associations.

Second, the location information here aligned with the discrete period when a mob encircled and occupied the Capitol Building. The district court explained that a person like Wise—who entered the Capitol through the Senate Wing Door, approximately ten minutes after the first breach of the building—would have understood that his own entry into the building was unauthorized. In other words, Wise could not have reasonably expected to keep his location within the Capitol Building a secret. *See United States v. Gale*, 136 F.3d 192, 195 (D.C. Cir. 1998) ("Without legal authority to be there, Gale lacked the 'legitimate expectation of privacy' in the premises."). Location records showing his presence there were thus not likely to disclose a private fact. This is especially so because, as this Court knows, on January 6, 2021, only authorized persons were allowed into the U.S. Capitol in the first instance. With the Vice President's visit to the Capitol, the ongoing COVID-19 pandemic, and other widespread restrictions on the perimeter of the grounds, any person on Capitol grounds without authorization was already in the process of possibly committing a crime.

Contrast this case with the 127 days of cell-tower location information at issue in *Carpenter*. Such 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." 585 U.S. at 311 (internal quotation marks and citation omitted). It might specifically divulge the person's presence at "private residences, doctor's offices, political headquarters, and other potentially revealing locales" that hold the "'privacies of life.'" *Id.* (internal quotation marks and citation omitted).

No such disclosure risk was present in the limited location data obtained in this case. Because of their tailored geographic and temporal boundaries, "the [the cell-tower warrant] here did not seek data from [the defendant's] home or any other area in which [the defendant] had a reasonable expectation of privacy." *Davis*, 109 F.4th at 1330. This distinction further explains why the defendant in *Carpenter* had a reasonable expectation of privacy in the location data there and why the defendant does not here.

3. The Fifth Circuit's Privacy Analysis in *Smith* Is Limited to Geofence Warrants and Wrong on Its Own Terms

Instead of grappling with the realities of tower dumps, Wise devotes his supplemental briefing to urging this Court to adopt some (but not all) aspects of the Fifth Circuit's reasoning in *Smith*, 110 F.4th 817, which, as noted, recently held that two defendants had a protected expectation of privacy in their Location History data collected from Google. Wise's claim fails for two reasons: (1) the Google geofence at issue in *Smith* involved different data—Google Location History, not cell-site data—and a readily distinguishable area with markedly different privacy implications; and (2) in any event, *Smith* was wrongly decided.

a. *Smith*'s expectation-of-privacy ruling does not extend to the AT&T Cell-Tower Warrant—which involved only tower dump data, not Google Location History data—much less to an intensely monitored area such as the Capitol.

The geofence warrant in *Smith* specified a 98,000 square-meter area around a rural Mississippi post office where a postal-service driver had been brutally assaulted and robbed. *See* 110 F.4th at 820, 826. Through a three-step process, the warrant sought three hours of location data (including data outside the specified area) and identity information for devices present within the specified area during the hour of the robbery. *Id.* at 827. Law enforcement subsequently

obtained subscriber information for three devices; that information identified two of the assailants. *Id*. at 828.

The Fifth Circuit held that the two assailants had a reasonable expectation of privacy in the location information under *Carpenter* and, therefore, Fourth Amendment standing to contest the warrants. 110 F.4th at 836. The *Smith* court specifically observed that Google's Location History data is "'considerably more precise than other kinds of location data, including cell-site location information because [Location History] is determined based on multiple inputs, including GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, and cell towers.'" *Id.* at 823 (quoting *United States v. Rhine*, 652 F. Supp. 3d 38, 67 (D.D.C. 2023)). Based on this understanding, the court reasoned that "even a snapshot of precise location data … '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.'" *Id*. at 833 (internal quotation marks, brackets, and citation omitted). In addition, the *Smith* court also posited, Google's Location History data "can easily follow an individual into areas normally considered some of the most private and intimate, particularly residences," *id*.—a functionality that *Smith* deemed "invasive for Fourth Amendment purposes" because the tracking occurs "regardless of whether a particular individual is suspicious or moving within an area that is typically granted Fourth Amendment protection." *Id*. at 834. *Smith*, in short, anchored its ruling to the notion that "the intrusiveness and ubiquity *of Location History data*" supported a "'reasonable expectation of privacy'" by the defendants *in that type of data*. *Id.* at 836 (emphasis added). And *Smith* further underscored that limitation when it emphasized that its analysis applied to "the use of geofence warrants … *as described herein*." 110 F.4th at 820 (emphasis added).

The AT&T Cell-Tower Warrant at issue in this case is materially different. For one thing, whereas the *Smith* geofence warrant involved Google Location History data, the AT&T Cell-Tower Warrant is not a geofence and does not involve Google Location History at all. This distinction is significant. As noted, *Smith* expressly observed that Google's Location History data is "'*considerably more precise than other kinds of location data, including cell-site location information*.'" *Id.* at 823 (emphasis added). Nor was *Smith*'s emphasis on the precision of Google Location History a mere throwaway line. To the contrary, the potential precision of Google's location data—real or perceived—played a critical role in the *Smith* court's analysis, underpinning that court's concerns that Google Location History data (1) could "'expose highly sensitive information,'" such as visits to medical facilities, strip clubs, a criminal defense attorney; or (2) could "follow an individual into areas normally considered some of the most private and intimate, particularly residences." *Id*. at 833. In contrast, Wise has not pointed to anything in the record supporting a comparable inference or "intrusiveness" or "ubiquity" for the substantially less precise tower-dump data at issue in this case. Thus, whatever may be said of Google geofences, Wise cannot show that the AT&T Cell-Tower Warrant infringed upon his reasonable expectation of privacy in his device's location at a single location for a relatively brief period on January 6.

For another thing, the target area at issue in *Smith* is readily distinguishable from the area at issue here. As noted, the *Smith* warrant sought hours of location data for all devices present in the public area that happened to circle the robbery scene. The AT&T Cell-Tower Warrant, by contrast, focused on the Capitol Building.

As noted, the AT&T Cell-Tower Warrant focused on two antennas that serviced the Capitol Building, where Wise clearly lacked any reasonable expectation of privacy. As explained above, the Capitol Building is a protected government facility that houses the country's legislative branch.

It is secured 24 hours a day, entry is regulated, and surveillance cameras monitor visitors inside. *See* p.12, *supra*. The same observation applies to adjacent areas on January 6; the building's exterior plaza and nearby streets were also closed to the public. *See Rhine*, 652 F. Supp. 3d at 87. Finally, "the nearest [commercial business or residence] is no less than about a quarter of a mile away." *Id.* This geographic separation between the Capitol Building and the various private locations cited by the Fifth Circuit in *Smith* undermines any speculation that AT&T's tower dump data here could have disclosed any private or sensitive location information. *See* pp.12-13, *supra*. For that reason as well, even if the two defendants in *Smith* had a reasonable expectation of privacy in their location information within the rural Mississippi area, Wise lacked a similar expectation in his cell-site location information within the Capitol Building.

b. In any event, *Smith*'s finding was wrong on its own terms, for multiple reasons. First, contrary to the *Smith* court's statements, the geofence warrant in that case did not provide "a detailed and comprehensive record of the person's [physical] movements" resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Carpenter*, 585 U.S. at 309. The warrant instead obtained information about the individuals "'using a phone' … at a particular time" in a particular rural Mississippi location. *Id*. at 315. The Supreme Court in *Carpenter* made clear that its "narrow" holding did not encompass that circumstance. *Id*. at 316.

Second, the Fifth Circuit wrongly dismissed the third-party doctrine's application. The court acknowledged that Google users must opt in to the Location History function, but questioned whether that opt-in was knowing and voluntary. The fact that two-thirds of Google users *decline* the function, *see Chatrie*, 107 F.4th at 331, undercuts the concern that the opt-in is illusory. And while some users may hurriedly select the opt-in when creating a Google account, *see Smith*, 110

F.4th at 836, the same situation assuredly arises when some bank customers quickly sign bank-enrollment forms explaining how the bank will collect and share their information. Yet it is black-letter law that those customers lack privacy expectations over their account information by virtue of "voluntarily convey[ing it to the bank[]."[7] *Miller*, 425 U.S. at 442.

Finally, the Supreme Court's refusal to apply the third-party doctrine in *Carpenter* was tethered to a specific conclusion: that "carrying [a cell phone] is indispensable to participation in modern society" and "there is no way to avoid leaving behind a trail of location data." 585 U.S. at 315. The same cannot be said of Google's Location History function. It is not essential to participation in modern society; "[location history's] activation is unnecessary to use a phone or even to use apps like Google Maps." *Chatrie*, 107 F.3d at 331. In fact, Google account holders can also turn the function off and delete their location histories whenever they want.

Not surprisingly, since *Carpenter*, courts have held that the government may obtain limited Google Location History of the type at issue in the January 6 geofence warrants without implicating the Fourth Amendment. The Fourth and Eleventh Circuits have held that the government did not conduct a Fourth Amendment search when it obtained limited geofence-location data from Google. Both circuits distinguished *Carpenter* on the ground that a defendant lacks a reasonable expectation of privacy in a discrete period of location-history data collected by Google.[8] *See United States v. Davis*, 109 F.4th 1320, 1330 (11th Cir. 2024) (no reasonable expectation of privacy in location data at six locations for 40-50 minutes); *Chatrie*, 107 F.4th at

[7] That customers may not anticipate the bank's later decision to share the information is of no moment. "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Miller*, 425 U.S. at 443.

[8] The government discusses the Fifth Circuit's recent contrary decision below at pp.24-30.

330-331 (no reasonable expectation in two hours of location data). The Seventh Circuit has similarly found no reasonable expectation of privacy in location records "where the officers only collected real-time [cell-site location information] for a matter of hours while the suspect travelled on public roadways." *United States v. Hammond*, 996 F.3d 374, 392 (7th Cir. 2021). Other circuits have reached similar conclusions in related contexts. *See, e.g.*, *Sanchez v. Los Angeles Dep't of Transp.*, 39 F.4th 548, 559-561 (9th Cir. 2022) (e-scooter location data). And every district court to have considered the constitutionality of the January 6 geofence has sustained it. *See Easterday*, 2024 WL 195828; *Rhine*, 652 F. Supp. 3d 38; *Cruz*, No. 22-cr-64.

In sum, the geofence warrant at issue in *Smith* is readily distinguishable from the limited, less precise tower dump data the FBI obtained from AT&T in connection with its Capitol riot investigation. And *Smith* was wrongly decided in the first place. There is no sound reason for this Court to follow—and expand upon—*Smith*'s errors in this case.

B. Wise's Fourth Amendment Challenge Also Fails on Its Merits Because the AT&T Cell-Tower Warrant Articulated Probable Cause and Was Sufficiently Particular

Even assuming the information disclosed by AT&T implicated Wise's privacy interests, the government obtained a search warrant that complied with the Fourth Amendment. The warrant was supported by probable cause and identified the records to be seized with sufficient particularity.

1. The AT&T Cell-Tower Warrant Affidavit Established Probable Cause

The probable-cause standard "is not a high bar," *District of Columbia v. Wesby*, 583 U.S. 48, 57 (2018) (citation omitted), and "is less than a preponderance of the evidence," *United States v. Burnett*, 827 F.3d 1108, 1114 (D.C. Cir. 2016). When approving a search warrant, the magistrate judge need only determine whether "reasonable inferences" from the evidence described in the

warrant application establish 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, 240 (1983). Because the probable-cause standard deals not "with hard certainties, but with probabilities," *id*. at 231 (citation omitted), the facts presented to the magistrate judge need only "'warrant a person of reasonable caution in the belief' that contraband or evidence of a crime is present," *Florida v. Harris*, 568 U.S. 237, 243 (2013) (brackets and citation omitted).

The AT&T Cell-Tower Warrant affidavit in this case easily passes muster. First, it noted that the Capitol Building was secured on January 6 with access limited to authorized people carrying appropriate identification. ECF No. 102-3 at 16. Second, it documented how the mob forced entry into the building: breaking windows, assaulting police officers, and forcing the suspension of the joint session of Congress. *Id.* at 17-19. Third, it observed that many individuals in the mob carried cell phones. *Id.* at 20. Fourth, it explained that AT&T stored location data for mobile devices connected to its networks, and that AT&T likely had records documenting the devices that had connected from within the Capitol Building on January 6. *Id.* at 22-23.

These facts amply demonstrate a fair probability that records in AT&T's possession would identify individuals who entered the Capitol Building on January 6 as part of the mob. That, in turn, would allow law enforcement to identify individuals who either committed or witnessed various federal crimes occurring within the building that day. *Id.* at 8 (listing crimes under investigation). To the extent Wise contends that the AT&T Cell-Tower Warrant failed to establish probable cause, that claim lacks merit.

2. The AT&T Warrant Was Sufficiently Particular

"[T]he Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'" *Maryland*

v. Garrison, 480 U.S. 79, 84 (1987). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Id*.

The AT&T warrant amply satisfies this requirement by specifying the particular property to be searched and records to be seized. The AT&T warrant delineated the records to be searched: records associated with two cellular towers providing service to the Capitol Building during three periods on January 6: 12:00-12:15 p.m., 1:00-6:30 p.m., and 9:00-9:15 p.m. ECF No. 102-3 at 4-5. The warrant also contained a particularized description of the records that AT&T was to provide the government: telephone numbers and the date, time, and duration of any communications associated with the cell towers. *Id.* at 6. The warrant specified that the government would review this list and identify the devices for which it would seek subscriber information.[9] *Id.*

These features make clear that the AT&T warrant did not authorize a "wide-ranging exploratory search[]" of AT&T records. *Garrison*, 480 U.S. at 84. The warrant was instead "constrained—both geographically and temporally—to the [crimes] under investigation" at the Capitol Building on January 6. *United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (internal quotation marks omitted). Indeed, the warrant sought information for devices that connected a single cell antenna system, with two locations, providing service within Capitol building. And "the period[s] w[ere] narrow and precise … with exact times listed." *Id.* "Given these specific

[9] The warrant affidavit stated that the government would request subscriber information for these devices using subpoenas under the Stored Communications Act, 18 U.S.C. § 2703(c)(2). ECF No. 102-3 at 26.

limitations, the warrants were 'sufficiently definite' to eliminate any confusion about what the investigators could search." *Id*.

Finally, the AT&T warrant incorporated "directions as to how the government must handle the … data." *In re: Information Stored at Premises Controlled by Verizon Wireless*, 616 F. Supp. 3d 1, 11 (D.D.C. 2022). As explained above, the warrant directed AT&T to identify devices that were present in the Capitol Building before and after the mob. The government would exclude those devices because they would not likely constitute evidence of a crime; it would then seek subscriber information for the remaining devices. ECF No. 102-3 at 25-26. These constraints further "tailored the warrants to the greatest degree possible to obtain … data from the Service Providers to assist in identifying" individuals who entered the Capitol Building. *Verizon Wireless*, 616 F. Supp. 3d at 12. "[T]he particularity requirement seeks to assure that the[] searches … should be as limited as possible" with "nothing … left to the discretion of the officer executing the warrant." *United States v. Heldt*, 668 F.3d 1238, 1256 (D.C. Cir. 1981) (citation omitted). The magistrate judge reasonably found that the limitations catalogued above accomplished that purpose for this warrant.

The Eighth Circuit's decision in *James* confirms this conclusion. *James* held that a series of cell-tower warrants used to solve a spree of robberies complied with the Fourth Amendment's particularity requirement. In so holding, the court stressed that the warrants "covered only the cellular towers near each robbery" for a "narrow and precise" period. 3 F.4th at 1106. Those limitations "eliminate[d] any confusion about what the investigators could search." *Id.* The same is true here. The AT&T cell-tower warrant sought location information for the area and time associated with the mob's breach of the Capitol Building on January 6. That, in turn, limited the executing officers' discretion over the scope of the search.

Wise's contrary contentions, which just rehash the Fifth Circuit's particularity discussion in *Smith*, lack merit. Wise twice cites (ECF No. 101 at 8, 12) *Smith*'s statement that the geofence warrant in that case "force[d] [Google] to search through its *entire* database" because the investigators did not know the identity of the suspect. 110 F.4th at 837. But that logic fails here for at least two basic reasons. First, whatever may be said of that logic in the context of actual *geofence* warrants, Wise provides no reason—and none exists—to extend it to the *tower dump* warrant at issue here. The tower dump warrant directed AT&T to search the records pertaining to two—and only two—cell towers, both of which were located inside the Capitol Building complex. Nor is there any basis, in fact or logic, to speculate that, to accomplish that simple task, AT&T was somehow required to search a broader dataset of all its customers—as opposed to the records of the two towers at issue. For that reason alone, Wise's reliance on *Smith*'s particularity analysis crashes before it even gets off the ground.

Second, *Smith*'s reasoning is flawed even as applied to actual geofence warrants. Geofence warrants do not command Google to search its entire database of accounts. They instead direct Google to identify the records in its possession corresponding to mobile devices detected to be within a designated geographic area at a particular time. This distinction is significant because, as Judge Contreras explained in *Rhine*, "the relevant [Fourth Amendment] question is not how Google runs searches on its data, but what the warrant authorizes the Government to search and seize." 652 F. Supp. 3d at 82. So long as the warrant defines those metrics with specificity, it authorizes a "search for the items described … anywhere in the [target location] where those items might be located." *United States v. Weaver*, 808 F.3d 26, 38 (D.C. Cir. 2015). Yet, under *Smith*'s contrary approach, "many search warrants and most third-party subpoenas for protected records would be unconstitutionally overbroad because they necessarily would require the third party to

search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server." *Rhine*, 652 F. Supp. 3d at 82; *see also Chatrie*, 107 F.4th at 330 n.16 ("[A] search only occurs once the government accesses the requested information"); *Davis*, 109 F.4th at 1331 ("[E]ven if Google did have to search every single account when it sought to determine which devices were subject to the warrant, that search would not implicate [the defendant's] Fourth Amendment rights. The Constitution is not concerned with a private party's search of its own records.").[10]

C. Subsequent AT&T Warrant Affidavits Included AT&T Cell-Tower Warrant Information and Accurately Described When the Government's Investigation into Wise Specifically Began

While the defendant does not remotely attempt to explain why the alleged inaccuracies or omissions are, in fact, material to probable cause, the defendant's argument is constructed on a factual house of cards. For example, the defendant alleges that "[l]aw enforcement knew of the geofence warrants and their findings, yet omitted that information from their subsequent search warrants." Supp. App. At 9. That is wrong. The defendant also alleges that "law enforcement asserted their entire investigation and identification into Mr. Wise began after a January 26, 2022, tip, not in October 2021, . . . nor in January or February of 2021 when the geofence warrant was executed and identified Mr. Wise." *Id.* at 16. This too is incorrect. When each fact is accessed holistically and independently, the defendant's narrative is shockingly inaccurate.

First, contrary to the repeated false claims in the defendant's argument, information regarding the AT&T Cell-Tower Warrant was not omitted from the affidavits in support of the

[10] The government identifies and discusses additional flaws in *Smith*'s particularity analysis in its Answering Brief in *United States v. Cruz*, No. 23-3064, at 24-30 (D.C. Cir. filed Oct. 9, 2024) (oral argument not yet scheduled).

Subsequent AT&T Warrants. As quoted above, *see* pp. 6-7, *supra*, the results of the AT&T Cell-Tower warrant as to the defendant's phone number were plainly and expressly described in the affidavits. Specifically, both affidavits stated that the government had obtained "records from AT&T for cell towers providing service to the United States Capitol" from "an authorized search warrant." Government's Exhibit A to ECF No. 56 at ¶ 40; Government's Exhibit B to ECF No. 56 at ¶ 41.

Similarly, the defendant's claim that the affidavits supporting the Subsequent AT&T Warrants improperly "omitted [the] tip from October of 2021 and instead referred to [the tipster's] later statement made in January 2022" is unfounded. The defendant alleges that the government's investigation began when the tipster first reached out to the FBI, which the defendant speculates was in October 2021. However, the matter was opened with the FBI in January 2022. The date of the tip is also not material. Even if the tipster sent an "introductory e-mail" or otherwise contacted the FBI in October 2021, the FBI's investigative steps began in January 2022 after the tipster was interviewed by the FBI. Thus, the affidavits supporting the Subsequent AT&T Warrants did not omit *material* information that would affect the probable cause analysis.

D. The Good-Faith Exception Independently Forecloses Relief

After setting forth inapplicable, non-binding case law and making factual assertions not tied to the evidence, Wise then attempts to weave them together into a baseless accusation that the government did not act in good faith to support his argument that the Subsequent AT&T Warrants should be suppressed. Specifically, the defendant alleges that "[a]gents knew their conduct was wrongful and thus tried to hide it under the cover of a tip followed by a search warrant." ECF No. 101 at 15. The Supp. Arg. continues: "But they had already identified Mr. Wise's device through unconstitutional means and needed to state a 'clean' way they began their investigation." *Id.* As

described in detail above, there is no legitimate basis for the defendant's claims that the Subsequent AT&T Warrants omitted information or contained errors, much less the necessary showing to warrant exclusion.

The exclusionary rule is a "'judicially created remedy"' that is "designed to deter police misconduct." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (citation omitted). The Supreme Court has explained that to justify suppression, a case must involve police conduct that is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system" in suppressing evidence. *Herring v. United States*, 555 U.S. 135, 144 (2009); *see Davis v. United States*, 564 U.S. 229, 236-239 (2011).

Leon recognized a good-faith exception to the exclusionary rule in the context of search warrants: evidence should not be suppressed if officers acted in an "objectively reasonable" manner in relying on a search warrant, even if the warrant was later deemed deficient. 468 U.S. at 922. *Leon* noted, for instance, that an officer's reliance would not be objectively reasonable when a warrant was "so lacking in indicia of probable cause" or "so facially deficient … in failing to particularize the place to be searched or the things to be seized … that the executing officers cannot reasonably presume it to be valid." *Id*. at 923 (internal quotation marks and citations omitted). "[T]he threshold for establishing" such a deficiency "is a high one, and it should be." *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012). "In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient." *Leon*, 468 U.S. at 921.

The circumstances here do not come close to overcoming *Leon*'s good-faith exception. As in *Messerschmidt*, it would "not have been unreasonable—based on the facts set out in [the AT&T warrant] affidavit[s]—for an officer to believe" that the requested information constituted evidence

relevant to crimes occurring inside the Capitol Building on January 6. 565 U.S. at 551. The affidavits articulated a fair probability that the individuals who stormed the building carried cell phones with them and that the providers had location records identifying those individuals. The warrants also provided clear geographic and temporal limitations specifying the records to be searched and seized. Given these features, the executing officers could reasonably rely on the magistrate judge's conclusion that the warrants complied with the Fourth Amendment's probable-cause and particularity requirements.

At least three district judges in the District of Columbia—in *Cruz*, *Rhine*, and *Easterday*—have rejected Fourth Amendment probable-cause and particularity claims attacking a Google geofence warrant. The Eighth Circuit has also rejected a particularity challenge to a cell-tower warrant resembling the AT&T warrant here. *See James*, 3 F.4th at 1106.

Finally, even under the Fifth Circuit's flawed framework, the good-faith exception would *still* apply in this case. After concluding that the disputed Google geofence warrant in *Smith* violated the Fourth Amendment's particularity requirement, it held that suppression was unwarranted because law enforcement's actions were "'reasonable and appropriate'" "considering the novelty of the technique and the dearth of court precedent to follow." 110 F.4th at 840 (citation omitted). That holding provides strong confirmation that the officers who executed AT&T warrants here—three years prior to the *Smith* decision—reasonably relied on the magistrate judge's probable cause and particularity determinations. *See United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) (stating that, if eight federal judges were mistaken in upholding a particular warrant, investigators "could reasonably have made the same mistake"). Here, how would law enforcement have any reason to believe that the act they took in 2021 would somehow be unconstitutional three years later? Ignoring the fact that geofence warrants are *not* tower dump

process and ignoring the above assessment challenging the *Smith* decision as to geofence warrants, it is patently unreasonable to suggest – let alone accuse – law enforcement of believing that their actions were improper at the time the warrants were signed and executed. Suppression is thus unwarranted.

E. Defendant Has Not Met Burden for *Franks* Hearing

There is no absolute right for a defendant to demand an evidentiary hearing to challenge a search conducted pursuant to a validly issued search warrant. Instead, under the framework announced by the Supreme Court in *Franks v. Delaware*, 438 U.S. 154 (1978), the defendant must first carry a threshold burden of making a "substantial preliminary showing," *Franks*, 438 U.S. at 155, that "(1) the affidavit contained false statements; (2) the statements were material to the issue of probable cause; and (3) the false statements were made knowingly and intentionally, or with reckless disregard for the truth,'" *United States v. Becton*, 601 F.3d 588, 594 (D.C. Cir. 2010) (quoting *United States v. Richardson*, 861 F.2d 291, 293 (D.C. Cir. 1988)). The Supreme Court emphasized that the right to a *Franks* hearing was of "limited scope," and explained that the requirement of a threshold showing by the defendant was necessary "to prevent the misuse of a veracity hearing for purposes of discovery or obstruction." *Id.* at 167, 170; *see also United States v. Thorne*, No. 18-cr-389 (BAH), 548 F.Supp.3d 70, 103 (D.D.C. June 30, 2021) ("To mandate an evidentiary hearing, the movant's attack on the affidavit supporting the warrant must be more than conclusory") (citations omitted).

The defendant here has not carried his threshold burden of a substantial showing under *Franks* to justify reopening the probable cause determinations regarding the warrants at issue. *See also* ECF No. 56. As an initial matter, as discussed above, the defendant has not identified any false statements in the affidavits. Moreover, none of the defendant's factual allegations were

material to the issue of probable cause. The defendant's claim appears to be that if the Subsequent AT&T Warrants identified October 2021 or January 2021, "the timing of the investigation would be questioned and probable cause would be defeated as geofence warrants are harshly criticized." Supp. App. at 17. But changing the date of the tip by a few months at best[11] and/or inserting the word "geofence" in the affidavits would not change the probable cause analysis in any way.

The remaining prong requires that defendant establish "reckless disregard for the truth," which the D.C. Circuit has construed as requiring that the affiant "in fact entertained serious doubts as to the truth" of their statements. *United States v. Davis*, 617 F.2d 677, 694 (D.C. Cir. 1979) (internal quotations omitted). "This subjective test may be met not only by showing actual deliberation but also by demonstrating that there existed obvious reasons to doubt the veracity of the informant or the accuracy of his reports." *Id.* (internal quotations omitted). The defendant has not shown anything to support his baseless allegation, nor could he.

In *Franks*, the Supreme Court cautioned that its ruling was intended to have "a limited scope," in order to prevent it from being "misused by defendants as a convenient source of discovery" and burdening district courts. 438 U.S. 167. The defendant's request would do just that. His request for a *Franks* hearing should be denied.

III. Conclusion

Therefore, for the foregoing reasons, and those described in the Government's Opposition to Motion to Suppress Evidence, ECF No. 56, the defendant's motion to suppress should be denied

[11] This argument appears to be an effort for the defendant to attempt to resurrect to its earlier staleness arguments. For all the reasons described in the government's prior response, ECF 56 at 14-16, 32-34, this argument should be rejected.

without an evidentiary hearing.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

By: */s/ Sarah Rocha*
Sarah Rocha
Trial Attorney / Detailee
D.C. Bar No. 977497
601 D Street, NW
Washington, DC 20579
Tel. No.: 202-330-1735
Email: sarah.wilsonrocha@usdoj.gov

/s/ Taylor Fontan
Taylor Fontan
Assistant United States Attorney
Indiana Bar No. 35690-53
601 D St. N.W, Washington, D.C. 20530
Tel. No.: (202) 815-8597
Email: taylor.fontan@usdoj.gov