

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

v.

MELVIN CASTELLANOS,

Defendant.

CRIMINAL ACTION FILE NO.:

1:21-CR-348-TWT-JKL

FINAL REPORT AND RECOMMENDATION

On the morning of February 25, 2021, Atlanta Police Department (“APD”) officers received a 911 call reporting that Defendant Melvin Castellanos had kidnapped his minor daughter, J.C., from a residence in Atlanta. The police did not know where Defendant was heading or the type of car he was driving. But based on reports from family members—specifically, that Defendant had a history of abusing J.C. and that J.C. had very recently texted them saying that she was scared and did not want to be with Defendant—the police were concerned for J.C.’s safety. Within roughly an hour, APD obtained real-time cell-site location information (“CSLI”) for Defendant’s and J.C.’s phones based on an “Exigent Request” under 18 U.S.C. § 2702(c)(4) to T-Mobile, their cell-phone carrier. Over the following 18 hours, APD officers monitored tower pings from Defendant’s

phone, which showed him traveling west, into Texas, toward the Mexican border. At around 5:00 the next morning, a deputy sheriff in Zavala County, Texas, who was on the lookout for Defendant's vehicle, pulled Defendant over. He found J.C. laying on the floorboard under a blanket. The deputy arrested Defendant and seized three cell phones, a bag of clothes, a knife, and a machete. Ultimately, a grand jury seated in this District returned an indictment charging Defendant with enticement of a minor, interstate transport of a minor for unlawful sex, and possession of child pornography. [Doc. 3.]

The case is presently before the Court on Defendant's motion to suppress evidence, motion to suppress search and seizure, and perfected motion to suppress evidence. [Doc. 29, 30, 34.] I held an evidentiary hearing on the motions on September 28, 2022. [See Docs. 47-49, 56.] Three APD officers testified at the hearing: Detective Jim Thorpe, Detective Calvin Thomas, and Investigator Charles Grimsley. [Doc. 56 ("Hr'g Tr.").] Former Zavala County Texas Deputy Sheriff Abraham Perez, who arrested Defendant, also testified at the hearing. [*Id.*] Following the hearing, Defendant filed a "Motion to Suppress Cell Phone Evidence," which limited his theory of suppression to law enforcement's efforts in obtaining real-time CSLI without a warrant. [Doc. 54.] The government has filed

a response in opposition to the motion. [Doc. 55], and Defendant has filed a reply [Doc. 57]. For the reasons that follow, it is **RECOMMENDED** that Defendant's motion to suppress be **DENIED**.¹

I. BACKGROUND

At around 9:00 a.m. on February 25, 2021, APD Officer Jenkins² responded to a 911 call that a minor had been abducted from a residence on Ladawn Lane in Atlanta. (Hr'g Tr. at 17-18.) The caller, M.S.,³ reported that her sister-in-law, J.C., had been abducted by Defendant, J.C.'s father, and that the family had received text messages from J.C. informing them that she was with her father, did not want to be with him, was scared, and feared for her life. (*Id.* at 18-20.)

¹ In his initial motions to suppress, Defendant also challenged law enforcement's use of license plate readers and historical CSLI. [Doc. 30.] It appears, however, that Defendant has abandoned those theories because he did not address them in his post-hearing briefs. [See Docs. 54, 57.] In any event, there is no indication that any such information led to Defendant's arrest or to the seizure of evidence; thus, the constitutionality of those investigative techniques has no bearing on whether evidence seized after Defendant's traffic stop in Texas should be suppressed.

² Officer Jenkins's first name is not reflected in the record.

³ Because this case involves allegations of a child abduction, to protect the privacy of the alleged victim, the Court refers to Defendant and J.C.'s family members by their initials.

At approximately 10:00 a.m., Detective Thorpe arrived at the scene on Ladawn Lane. (Hr’g Tr. at 54.) Officer Jenkins debriefed him on his (Officer Jenkins’s) interviews with family members, and Detective Thorpe directed Officer Jenkins to initiate a statewide AMBER alert and national BOLO in an effort to obtain law enforcement and the public’s assistance in locating and recovering J.C. (*Id.* at 14-15, 20-21, 37-40; Gov’t Ex. 4 [Doc. 49-4] (BOLO); Gov’t Ex. 5 [Doc. 49-5] (BOLO accompanying AMBER alert).) Detective Thorpe also spoke with M.S., who reported that J.C.—who was 15 or 16 years old—had relocated by her family to Georgia from North Carolina because her father had sexually and physically abused her. (Hr’g Tr. at 21-22.) The family believed that Defendant was taking J.C. back to North Carolina. (*Id.* at 22.)

Detective Thorpe obtained the cell phone numbers for Defendant and J.C. and sent them to his supervisor to prepare an exigent circumstances request “to find out what direction they were traveling.” (Hr’g Tr. at 22.) According to Detective Thorpe, he applied for real-time CSLI on an exigent basis because the family advised, first, that J.C. had been abducted by Defendant; second, that Defendant abused her; and third, that no one knew where J.C. was located. (*Id.* at 88.) Detective Thorpe did not call Defendant or J.C.’s phones because he did not want

to alert Defendant that police were involved and risk him throwing away the phones or otherwise making him harder to locate. (*Id.* at 23.)

At 10:13 a.m., Detective Thomas sent a request on a pre-printed form to T-Mobile asking the wireless carrier to provide the location for the two cell phones at 15-minute intervals for 48 hours. (Hr’g Tr. at 99-100; Gov’t Ex. 6 [Doc. 49-6].) On the form, Detective Thomas indicated that the exigent circumstance involved “Immediate danger of death or serious physical injury to any person.” (Gov’t Ex. 6 at 2.) Eight minutes after Detective Thomas sent the request, T-Mobile provided the first ping data, showing that Defendant and J.C.’s cell phones were in the same place and traveling west. (Hr’g Tr. at 25, 103.) Because the phones were heading west, instead of towards North Carolina, the officers became concerned that Defendant might be heading to Texas to cross the border into Mexico in an effort to get to Honduras.⁴ (*Id.* at 25.)

After receiving the location data, Detective Thorpe prepared an application for an arrest warrant from a state magistrate judge. (Hr’g Tr. at 25.) The

⁴ In the meantime, Detective Thorpe contacted law enforcement in North Carolina; the responding officer interviewed Defendant’s girlfriend, who said Defendant told her he was going to Atlanta in his black Explorer to get J.C. and that “if everything works out, either he will return to Charlotte with his daughter or they will return to Honduras.” (Hr’g Tr. 33-34, 146-47.)

application was based on the location information from T-Mobile, information from the family about Defendant allegedly abusing J.C., and information from Defendant's girlfriend about his plan to return to either Charlotte, N.C. or Honduras with J.C.⁵ (*Id.* at 146-47.) The warrant application was pushed to the front of the magistrate judge's queue, and Detective Thorpe swore the warrant out electronically at 2:17 p.m. (*Id.* at 29, 74-75, 79-80; Gov't Ex. 3.) In all, the application process with the judge took about 15 minutes. (Hr'g Tr. at 80.) Meanwhile, at 2:29 p.m., Detective Thomas asked T-Mobile to provide TrueCall data, which would provide more frequent and precise location data about the phone. (*Id.* at 101-02; Gov't Ex. 7 [Doc. 49-7] at 2, 4.⁶)

Detective Thorpe did not seek a warrant for Defendant's real-time CSLI because he thought a search warrant could not be used to obtain prospective location information. (Hr'g Tr. 15.) He explained that "[a] search warrant would just give us historical data and historical data could be two hours late" and that it

⁵ Detective Thorpe also obtained license plate information for the vehicle Defendant's girlfriend identified and put out a nationwide alert. (Hr'g Tr. at 34.) He later determined, however, that Defendant did not use the black Explorer because the vehicle had been found in North Carolina. (*Id.* at 34-35.)

⁶ Detective Thomas initially requested TrueCall data at 2:03 p.m. in an email to T-Mobile, and T-Mobile responded by asking him to submit a new exigency request form. (Gov't Ex. 7 [Doc. 49-7] at 2, 4.)

can sometimes take several days for a carrier to provide information in response to a warrant. (*Id.* at 15-16.)⁷ It is also undisputed that at no point during the investigation did a member of law enforcement apply for a warrant to ping Defendant's cell phone. (*Id.* at 78.)

Throughout the afternoon and night of February 25, APD received the location of Defendant's phone as he drove from Georgia to Texas. (Gov't. Ex. 9 [Doc. 49-9].) J.C.'s phone had been powered off, and it stopped transmitting location information near Montgomery, Alabama. (Hr'g Tr. at 27; Gov't Ex. 10 [Doc. 49-10].) Officers used the real-time CSLI to contact jurisdictions ahead of where the ping data showed Defendant and J.C. to be. (Hr'g Tr. at 161-64.) By midnight, the pings showed them in or around Louisiana, but because law enforcement did not know what type of vehicle the two were traveling in, officers could not locate the pair despite several tips and traffic stops. (*Id.* at 33, 40-42.)

Later that night, APD Detective Grimsley went back to the Ladawn Lane location and found a Ring camera at a home across the street. (Hr'g Tr. at 43.) Using data from that camera, officers determined that Defendant was driving a gray

⁷ On cross examination Detective Thorpe acknowledged, however, that if a warrant directed a provider to provide real-time cell-site information, the provider would be required to do so. (Hr'g Tr. at 82.)

Nissan Armada. (*Id.* at 43, 170.) Detective Grimsley provided that information to law enforcement in Texas where the real-time CSLI pings indicated Defendant was headed. (*Id.* at 171-72; Gov't Ex. 15 [Doc. 49-13].) Detective Grimsley also worked with Texas law enforcement to coordinate lookouts on the highways to Mexico. (Hr'g Tr. at 173-74.)

Around 5:00 a.m. the following day, February 26, a Zavala County Sheriff's Deputy pulled Defendant over in the Armada. (Hr'g Tr. at 44.) The deputy stopped the car solely because it matched the description he had been given by a radio dispatcher. (*Id.* at 126, 129, 140.) J.C. was in the backseat of the car, seemed scared, and had visible injuries to her face,⁸ neck, and arms. (*Id.* at 44-45, 129-31.) After running a system check and confirming the Georgia warrant for Defendant, the deputy arrested him. (*Id.* at 131.) The deputy searched Defendant and found two cell phones. (*Id.* at 132.) The deputy also searched the car, where he found a bag of clothes, another cell phone, a machete, and a large knife. (*Id.* at 131-32.) After J.C. was rescued, APD contacted T-Mobile and terminated the exigent ping request. (*Id.* at 45.)

⁸ Including a cut and a black eye. (Hr'g Tr. at 131.)

II. DISCUSSION

A. The Parties' Arguments

Defendant argues that APD's warrantless acquisition of real-time CSLI from T-Mobile violated the Fourth Amendment because he had a reasonable expectation of privacy in his movements as captured through real-time CSLI. [Doc. 54.] He contends that *Carpenter v. United States*, 138 S. Ct. 2206 (2018), in which the Supreme Court recognized a reasonable expectation of privacy in accumulated historical CSLI, applies with equal, if not greater, force to real-time CSLI because cell phones can pinpoint an individual's location almost anywhere and can reveal intimate details about a person's life. [*Id.* at 9-14.]

The government counters, relying on *United States v. Knotts*, 460 U.S. 276 (1983), that it is well-settled that an individual has no reasonable expectation of privacy when traveling on public roads, and because the location information gathered in this case simply showed Defendant's movements on interstate highways, the acquisition of real-time CSLI data did not constitute a search or seizure under the Fourth Amendment. [Doc. 55 at 7-11.] The government further argues that even if Defendant had a reasonable expectation of privacy, the exclusionary rule does not apply because exigent circumstances justified the warrantless acquisition of Defendant's location information. [*Id.* at 11-14.]

On reply, Defendant argues that the privacy interest at play is not whether an individual has an expectation of privacy traveling on a public roadway, but whether an individual has an expectation of privacy in the record of his physical movements as captured through a cell phone. [Doc. 57 at 2.] Defendant contends that acquiring real-time CSLI is more akin to a “technological trespass” than surveilling a vehicle traveling on a highway because it involves the government “commandeering” cell phone transmissions to locate an individual no matter where he is. [*Id.* at 4-5 (quoting *Commonwealth v. Reed*, 647 S.W.3d 237, 247 (Ky. 2022)) (quotation marks omitted).] Defendant also stresses that real-time CSLI “does more than augment visual surveillance” because it allows the government to *locate* an individual without the need for any prior investigation. [*Id.*] Defendant acknowledges (as he must) that *Carpenter* did not explicitly address the collection of real-time CSLI, but he maintains that the “doctrinal impact” of the decision can only mean that an individual has an expectation of privacy in his real-time CSLI for at least the amount of time at issue in this case—that is, 18 hours or more. [*Id.* at 6-7.] Finally, Defendant contends that exigent circumstances do not justify the warrantless search of Defendant’s CSLI precisely because APD had ample time to obtain a warrant for prospective CSLI, as demonstrated by the fact that APD

tracked his movements for 18 hours and obtained an arrest warrant from a state court judge fairly early in that 18-hour period. [*Id.* at 7-11.]

B. Analysis

Defendant's motion raises two issues: whether the collection of real-time CSLI constituted a search under the Fourth Amendment, and, if so, whether the exigent circumstances exception to the warrant requirement applies to the circumstances here. The Court addresses each of those issues in turn.

1. Whether the Collection of Real-Time CSLI Constituted a Search Under the Fourth Amendment

In *Carpenter*, the Supreme Court summarized how wireless carriers use cell site information to locate devices connected to their networks:

Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called “cell sites.” Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller

the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying “roaming” charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

138 S. Ct. at 2211-12. In short, “historical CSLI allows law enforcement to retrace a defendant’s physical movements, while real-time CSLI shows (roughly) where a defendant’s cell phone is currently located.” *United States v. Lewis*, 38 F.4th 527, 536 (7th Cir. 2022).

The Stored Communications Act (“SCA”) generally prohibits providers from disclosing “a record or other information pertaining to a subscriber to or customer of such service” 18 U.S.C. § 2702(a)(3). And while there are various ways in which the government can obtain such information, the method at issue in this case is the so-called exigency request codified at 18 U.S.C. § 2702(c)(4). Under that exception, a provider may divulge “a record or other information” “to a

governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.” 18 U.S.C. § 2702(c)(4). This includes both historical and prospective cell-site information. *United States v. Gilliam*, 842 F.3d 801 (2d Cir. 2016) (holding § 2702(c)(4) authorizes the disclosures of “the location of a customer’s cell phone”).

Fourth Amendment jurisprudence involving requests for CSLI under the SCA is an evolving—and complicated—area of the law. The Fourth Amendment protects “[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. “Generally speaking, whether ‘government-initiated electronic surveillance’ constitutes a ‘search’ triggering Fourth Amendment protection depends on whether a person has a reasonable expectation of privacy in the area searched.” *United States v. Howard*, 858 F. App’x 331, 332 (11th Cir. 2021) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Courts use “a two-part test to determine whether an individual has a legitimate expectation of privacy in the object of a search: (1) the individual must manifest a subjective expectation of privacy in the object of the challenged search, and (2) society must be willing to recognize that

expectation as legitimate.” *United States v. Smith*, 39 F.3d 1143, 1144 (11th Cir. 1994) (citing *California v. Ciraolo*, 476 U.S. 207, 211 (1986)); *see also United States v. Robinson*, 62 F.3d 1325, 1328 (11th Cir. 1995). “Ordinarily, a person lacks a reasonable expectation of privacy in information he has voluntarily disclosed to a third party.” *United States v. Trader*, 981 F.3d 961, 967 (11th Cir. 2020).

In *Carpenter*, the Supreme Court held that the third-party doctrine does not apply to retrospective collection of cell-site location information for periods of at least seven days because “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” 138 S. Ct. at 2217. There, the government obtained an order under the SCA to obtain historical CSLI for Carpenter’s cell phone for a 127-day period from one service provider and seven days from a second. *Id.* at 2212. Central to the Court’s reasoning was that people carry cell phones at all times, which means that cell-site information can provide an “all-encompassing record of the holder’s whereabouts.” *Id.* at 2217. As the Court explained, “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Id.* at 2218. Historical CSLI

also “gives police access to a category of information otherwise unknowable”—potentially allowing the government to reconstruct an individual’s movements for years. *Id.* In short, by accessing such accumulated historical CSLI, the government “invaded Carpenter’s reasonable expectation of privacy *in the whole of his physical movements.*” *Id.* at 2219 (emphasis added).

Due to the relative novelty of using CSLI to track an individual’s movements, the Court explicitly characterized its decision as “a narrow one.” *Carpenter*, 138 S. Ct. at 2220. The Court’s decision “left open the possibility that the government could obtain less than seven days’ worth of cell-site location information without a warrant,” and even “left open the possibility that the government could collect cell-site location information in real time” *Trader*, 981 F.3d at 968 (citing *Carpenter*, 138 S. Ct. at 2217 n.3, 2220). The Court also indicated that certain case-specific exceptions may support a warrantless acquisition of CSLI, including when the “exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment”—including when there is a “need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent

destruction of evidence.” *Carpenter*, 138 S. Ct. at 2222-23 (alteration in original) (citation omitted). The Court explained:

if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency.

Id. at 2223.

The case at bar implicates much of what *Carpenter* left explicitly unresolved. The total sum of data collected here was approximately 18 hours, far shorter than the seven days at issue in *Carpenter*. The type of data collected was limited, real-time CSLI, not accumulated historical CSLI. And the location data was obtained in order to locate the Defendant and the victim following a child abduction because the police feared for the ongoing safety of J.C., as opposed to *Carpenter*, where the data was obtained to investigate criminal activity occurring months earlier.

The parties fundamentally disagree on how far *Carpenter* should be extended to protect real-time CSLI from warrantless searches. At its core, the government’s position depends on what information the police *actually obtained* in collecting CSLI. In the government’s view, if the data captured reveals only

information that an individual would have no reasonable expectation of privacy in—here, Defendant’s movements on a public highway—the Fourth Amendment is not implicated. Defendant, by contrast, contends the capabilities of the data source—here, Defendant’s phone—is determinative, because what matters is what information the police *might obtain* in collecting CSLI. Defendant argues that because collecting CSLI could potentially reveal intimate details about an individual’s personal life, any acquisition of that data qualifies as a search under the Fourth Amendment. In Defendant’s view, then, the issue is not whether there was a search, but rather whether the search was reasonable. And while both sides have done an exemplary job briefing the issue, the Court finds the government’s position to be more in line with the law in this Circuit.

The Court starts with the Seventh Circuit’s decision in *United States v. Hammond*, 996 F.3d 374 (7th Cir. 2021), which, at this time, is the sole post-*Carpenter* Circuit decision that addresses whether the collection of real-time CSLI to locate a suspect constitutes a search under the Fourth Amendment. In that case, the police identified Hammond as the lead suspect in a string of armed robberies. Then, upon learning his cell phone number, an officer obtained real-time CSLI for Hammond’s phone through an exigent request under § 2702(c)(4). *Id.* at 380-81.

The police used ping data for approximately six hours until Hammond was located and arrested. *Id.* at 381. During his prosecution, Hammond moved to suppress evidence seized after his arrest, arguing that under *Carpenter*, the warrantless collection of real-time CSLI violated the Fourth Amendment because he had a reasonable expectation of privacy in his movements. *Id.* at 382-83. The Seventh Circuit disagreed, finding that the case was more analogous to *Knotts* because Hammond’s location was monitored for only around six hours, which was “very different from the 127 days of monitoring at issue in *Carpenter* and more similar to the monitoring of the discreet car trip at issue in *Knotts*.” *Id.* at 389. In addition, the court noted that the “real-time CSLI request only collected location data that [the defendant] had already exposed to public view while he travelled on public, interstate highways and into parking lots within the public’s view.” *Id.* The court explained:

Crucially, unlike in *Carpenter*, the record of Hammond’s (and *Knotts*’) movements for a matter of hours on public roads does not provide “a window into [the] person’s life, revealing . . . his familial, political, professional, religious, and sexual associations” to the same, intrusive degree as the collection of historical CSLI. Law enforcement used the real-time CSLI to find Hammond’s location in public, not to peer into the intricacies of his private life. The records here and in *Knotts* do not suggest that law enforcement used either real-time CSLI or the beeper to examine the defendants’ movements inside of a home or other highly protected area. And, Hammond does

not argue that he was in private areas during this time period. In *Carpenter*, law enforcement's surveillance became a "search" because the surveillance followed Carpenter long enough to follow him into, and record, his private life. But here, and in *Knotts*, law enforcement only followed Hammond on public roads, for the duration of one car trip.

Id. at 389 (citation omitted; alteration in original). "Real-time CSLI collected over the course of several hours," the court wrote, "simply does not involve the same level of intrusion as the collection of historical CSLI." *Id.* The court further reasoned that "[t]he collection of historical CSLI in *Carpenter* was different because it would be too costly and difficult to follow a suspect for over four months," and society expects that law enforcement could not secretly monitor every movement for a very long period of time. *Id.* at 390. But when a suspect is traveling on public roads, the court explained, "society is fully aware that officers may follow and track a suspect's movements for several hours." *Id.* In the court's view, it is "critical" to keep in mind that the officers were pursuing a suspect who had "already committed several, violent felonies and was likely to do so again" and "had reason to believe that he was armed . . . and likely to attempt another armed robbery" *Id.*

The Eleventh Circuit, meanwhile, has not directly confronted whether the warrantless acquisition of real-time CSLI constitutes a search or seizure under the

Fourth Amendment. *See United States v. Green*, 981 F.3d 945, 958 (11th Cir. 2020) (“The question of whether acquiring [real-time tracking data] constitutes a search . . . remains unanswered today.”). But in an unpublished case, *United States v. Howard*, 858 F. App’x 331 (11th Cir. 2021), the Circuit held that the warrantless acquisition of GPS location information from a vehicle the defendant was driving did not implicate the Fourth Amendment. In *Howard*, a confidential informant consented to the installation of a GPS tracking device on her truck that would allow the police to remotely monitor the truck’s real-time location while it was moving. *Howard*, 858 F. App’x at 331. Shortly after the device was installed, Howard took possession of the truck from the informant, and the police began tracking it using GPS location data.⁹ *Id.* at 331-32. Officers tracked the truck for around 22 hours, arresting Howard as he parked at a fast food restaurant.¹⁰ *Id.* at 332. In a motion to suppress evidence, Howard argued that the warrantless GPS monitoring of his location violated the Fourth Amendment. *Id.* at 332-34. The Eleventh Circuit

⁹ At first, law enforcement confirmed through visual surveillance that the GPS was accurately reporting the truck’s location, but then stopped visual surveillance and relied exclusively on GPS reporting to track its movement. *Howard*, 858 F. App’x at 331.

¹⁰ Specifically, the GPS tracker was installed around 2:30 p.m.; Howard took possession of the truck around two hours later; and he was arrested at 2:00 p.m. the following day. *Howard*, 858 F. App’x at 331-32.

disagreed, finding *Knotts* directly on point. *Id.* at 333. It reasoned that “the GPS tracking device at issue in this case ‘augmented [the officers’] sensory faculties’ by allowing the officers to gather remotely information about the truck’s location and movement on public roads: information that could have been obtained by police through visual surveillance.” *Id.* The court further explained, “we can discern no material difference between the duration of the beeper monitoring involved in *Knotts* (which seems to have taken place over the course of one day) and the 22-hour GPS monitoring involved in this case.” *Id.* The court also found that the fact the GPS device showed the stops the defendant made along his travel route did not transform it into a search because those stops could have been observed via visual surveillance and, thus, the defendant had no reasonable expectation of privacy in “whatever stops he made.” *Id.* (quoting *Knotts*, 460 U.S. at 282). And perhaps most significant for present purposes, the Court distinguished *Carpenter*, finding that the “real-time GPS monitoring of a vehicle traveling on public roads” was “easily distinguishable from the historical CSLI data at issue in *Carpenter*.” *Id.* The court pointed out that that, unlike monitoring a vehicle or a package, “people ‘compulsively’ carry cell phones on their person at all times” so that “tracking of a cell phone . . . ‘achieves near perfect surveillance’ of the phone’s owner as the ‘cell

phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.” *Id.* (quoting *Carpenter*, 138 S. Ct. at 2218). The court further noted that *Carpenter* dealt with historical CSLI, “which allowed police to reconstruct a person's past movements without the police having decided in advance to investigate that person.” *Id.*

The upshot of *Hammond* and *Howard* is that *Carpenter* should not be extended categorically to all real-time CSLI. Those decisions take the view that whether a Fourth Amendment violation has occurred instead depends on how much data was captured and for how long,¹¹ and more importantly, what the data reveals about an individual's location and movements. *Accord United States v. Dewilfond*, 54 F.4th 578, 580-81 (8th Cir. 2022) (finding no Fourth Amendment violation where law enforcement monitored the defendant's movements on public roadways for two days using a GPS tracker that a cooperating source had consented to being installed); *People v. Edwards*, 63 Misc. 3d 827, 831 (N.Y. Sup. Ct. 2019) (holding that two days' worth of CSLI did not constitute a search under the Fourth

¹¹ Obviously, the longer the period of time CSLI is captured, the more data will likely be captured.

Amendment because the state was not “using CSLI data in an effort to trace *all* of defendant’s movements over an *extended* period of time as part of a *long-term* investigation into defendant’s whereabouts and conduct”); *cf. United States v. Baker*, 563 F. Supp. 3d 361, 381 (E.D. Pa. 2021) (distinguishing *Hammond* and finding that government’s request for real-time CSLI of defendant’s phone constituted a search where it located the defendant within a private house).

Here, APD officers collected information for less than 24 hours, while Defendant traveled on public roadways, solely for the purpose of finding Defendant and the minor child whom they believed to be in grave danger based upon the family’s reports that he had abused and abducted her. Importantly, there is no indication whatsoever that the real-time CSLI collected actually revealed *any* potentially private information that *Carpenter* expressed concern about, such as where Defendant lived, with whom he associated, where he worshipped, whom he supported politically, and so on. What’s more, it is highly unlikely that this snapshot of real-time CSLI would have exposed details about Defendant’s life to the government. Law enforcement was confronted with an active child abduction, and there was no practicable danger that Defendant’s movements—as he was fleeing across the country, and potentially out of the country, with the child—would

betray the intimacies of his daily life to the government. So even though real-time CSLI could *potentially* reveal details about someone's movements, that did not happen here, and the likelihood of it happening at all was relatively scant in comparison to circumstances at work in *Carpenter*.

The Court appreciates Defendant's argument that *Carpenter*, taken to its furthest end, could be read to protect the acquisition of any CSLI, regardless of whether it is historical or prospective, and regardless of the duration of its collection. After all, for as concerned as *Carpenter* was that historical CSLI could reveal intimate details about someone's life, the Supreme Court's discussion only addressed the possibility that sensitive, private information could have been gleaned from the CSLI collected in that case, and did not cite a single example of actual private information about Carpenter that was divulged to the government. Indeed, there was no indication in the Court's opinion that the records revealed anything more than the fact that Carpenter's phone was near areas where robberies had taken place. But, it is also not inconsistent with *Carpenter* to conclude that an individual does not have a reasonable expectation of privacy in short-duration, real-time CSLI in an emergency situation, such as a child abduction investigation; and the *Hammond* decision, as well as Eleventh Circuit authority cited above, present

compelling reasoning for why the two should be treated differently. So while *Carpenter* was concerned that if too much CSLI was gathered, it could show the whole of someone's private movements, those concerns are far less implicated by what was essentially real-time pursuit of a kidnapper and his victim across the Southeast.

United States v. Melton, Cr. No. 21-1721 KG, 2022 WL 1404718 (D.N.M. May 4, 2022), a recent unpublished district court case on which Defendant relies, is not persuasive. In *Melton*, the police learned that Terrell, a homicide suspect, was traveling with an unknown companion (who turned out to be Melton, the defendant) to the city of Truth or Consequences, New Mexico. *Id.* at *1. Believing both men to be armed and dangerous, the police obtained real-time CSLI from Melton's cell phone provider via an exigency request and used that information to locate and arrest them. *Id.* at *2. Melton filed a motion to suppress arguing that the warrantless tracking of his CSLI was a search under the Fourth Amendment, and the court agreed. *Id.* at *4. The court reasoned that *Carpenter* "tacitly recognized a cognizable privacy interest in [real-time CSLI] when it acknowledged that 'case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances,'" and noted that "if law enforcement

is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI.” *Id.* (quoting *Carpenter*, 138 S. Ct. at 2222, 2223). The *Melton* court further explained that the acquisition of real-time CSLI qualified as a search because “the Government . . . did not employ traditional surveillance techniques that would allow identification of Defendant (or Terrell’s) location without recourse to Defendant’s CSLI.” *Id.* In other words, the source of the data—Melton’s cell phone—was the determinative factor in deciding whether Melton had a reasonable expectation of privacy.

The undersigned chooses not to follow *Melton* because it conflicts with the reasoning of *Hammond*, which provides a sound basis to harmonize *Knotts* and *Carpenter* by focusing on what information is actually captured during the collection of CSLI.¹² Nor does the undersigned agree that, because the Supreme

¹² The Court recognizes that *Hammond* is not the final word on this issue and that other courts, most notably the Supreme Court of Kentucky, have adopted a categorical rule that any acquisition of CSLI constitutes a search under the Fourth Amendment. *See Commonwealth v. Reed*, 647 S.W.3d 237, 246-49 (Ky. 2022) (likening the capture of real-time CSLI to a “dragnet” and explaining that it is akin to a trespass because it requires the cell service provider to ping an individual’s phone, which enables the provider (and the government) to locate the phone). But given the Eleventh Circuit’s willingness in *Howard* to look at what data is actually obtained, the undersigned believes that the approach taken by the *Hammond* is more consistent with the law in the Circuit.

Court noted that exigent circumstances may be relevant, the Court “tacitly recognized” that an individual has a privacy interest in real-time CSLI. Again, the Court was clear that it was taking no position as to whether the short-term acquisition of real-time CSLI implicated the Fourth Amendment. Finally, the undersigned is not persuaded that it matters whether traditional surveillance techniques were attempted or even successful. What matters is the expectation of privacy, and for the reasons discussed above, the undersigned does not believe that society recognizes that an individual in the midst of an alleged child abduction has a reasonable expectation of privacy in real-time CSLI for a period of 18 hours as he travels on public highways.

Defendant also draws a distinction between locating someone and tracking them, analogizing the monitoring of real-time CSLI to using a cell-site simulator to locate a device. [Doc. 57 at 4 (citing *Jones v. United States*, 168 A.3d 703, 712 (D.C. 2017).] But under the facts of this case, that is a distinction without a difference. True, the police were attempting to locate Defendant, but that was also true in *Knotts*, *Howard*, and *Hammond*.

In the end, the undersigned recognizes that this is a close issue and reasonable minds can disagree as to how far *Carpenter* extends. But under the

circumstances of this case and given the guidance from *Hammond* and *Howard*, the Court finds that the collection of real-time CSLI here—which, to reiterate, was limited to Defendant’s movements on public highways for around 18 hours in the midst of an alleged child abduction—did not constitute a search under the Fourth Amendment.

2. Whether the Exigent Circumstances Exception Applies

Even if the acquisition of real-time CSLI were a search under the Fourth Amendment, the undersigned still finds that the government has carried its burden to show that exigent circumstances justified the warrantless acquisition of that information. As noted above, *Carpenter* explained that “even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual’s cell-site records,” including when exigent circumstances exist that “make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.” 138 S. Ct. at 2222 (citation omitted; alteration adopted). “Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence.” *Id.* at 2223. “The most urgent emergency situation excusing police compliance with the warrant requirement is, of course, the need to protect or preserve life.”

United States v. Holloway, 290 F.3d 1331, 1335 (11th Cir. 2002). Indeed, “[i]t is difficult to imagine a scenario in which immediate police action is more justified than when a human life hangs in the balance.” *Id.* at 1337.

For exigency to excuse the warrant requirement, the government bears the burden to “demonstrate both exigency and probable cause.” *Holloway*, 290 F.3d at 1337. “In emergencies . . . law enforcement officers are not motivated by an expectation of seizing evidence of a crime. Rather, the officers are compelled to search by a desire to locate victims and the need to ensure their own safety and that of the public.” *Id.* “Thus, in an emergency, the probable cause element may be satisfied where officers reasonably believe a person is in danger.” *Id.* at 1338. “Separately, the government must also demonstrate that the resulting search was strictly circumscribed by the nature of the exigency that authorized it and limited to the areas where a person reasonably could be found.” *United States v. Cooks*, 920 F.3d 735, 742 (11th Cir. 2019) (cleaned up).

Here, the government has carried its burden to demonstrate both exigency and probable cause. The APD officers reasonably believed that J.C. had been abducted, that she was in serious danger, and that locating her and Defendant was essential to ensuring her safety. J.C.’s sister-in-law told APD that Defendant had

a history of abusing J.C. sexually and physically; that he traveled from North Carolina to Georgia and took J.C.; and that J.C. had texted the family telling them that she was with Defendant, did not want to be with him, and was scared and in fear of her life. (Hr’g Tr. at 17-20.) The APD officers took these reports seriously and believed that J.C. was in danger. (*Id.* at 96.) Officers also used other investigative methods in parallel to try to locate Defendant and J.C., including issuing an AMBER alert, disseminating a BOLO, interviewing Defendant’s girlfriend in North Carolina, and distributing an image obtained from a neighbor’s camera of the vehicle that Defendant used to abduct J.C.

Further, officers “limited their requests to real-time pings of cell phone numbers associated with Defendant . . . thus demonstrating that their requests ‘were strictly circumscribed by the nature of the exigency that authorized’” the pings. *United States v. Jones*, No. 2:19-CR-44-RWS-JCF, 2021 WL 7541382, at *8 (N.D. Ga. Oct. 7, 2021) (citing *Cooks*, 920 F.3d at 742), *report and recommendation adopted*, 2022 WL 575907 (N.D. Ga. Feb. 25, 2022). In fact, the T-Mobile form stated that “all interception and location information assistance will terminate if the appropriate legal demand or customer consent is not received within 48 hours,”

further demonstrating that the purpose of the request process was narrowly tailored to provide information in an emergency. (*See* Gov’t Ex. 6 at 2.)

Defendant states in passing that “police wanted the location data because detectives suspected that [Defendant] had abducted her—although there were no witnesses and no evidence to corroborate that suspicion.” [Doc. 54 at 2.] To the extent that Defendant means to argue that M.S.’s 911 call or the family members’ statements to the police were insufficient to establish probable cause, the Court disagrees. “Once presented with an emergency situation, the police must act quickly, based on hurried and incomplete information.” *Holloway*, 290 F.3d at 1339. The information conveyed to law enforcement was arguably even more reliable than in *Holloway*, where the Eleventh Circuit found that an anonymous 911 call that reported a serious threat to human life was sufficient to establish probable cause to search the defendant’s home under exigent circumstances. *Id.* Evaluating the officers’ actions “by reference to the circumstances then confronting [them], including the need for a prompt assessment of sometimes ambiguous information concerning potentially serious consequences,” *id.* (quoting 3 Wayne LaFare, Search & Seizure § 6.6(a) (3d ed. 1996)), the Court finds that the officers

reasonably believed that an emergency situation justified obtaining real-time CSLI on an exigent basis.

Defendant also argues that, regardless of whether exigency might have initially existed, it dissipated because APD officers applied for and obtained an arrest warrant at around 2:17 p.m.—approximately four hours after receiving the first ping, yet took no steps to obtain a search warrant for Defendant’s CSLI. [Doc. 57 at 8-9.] According to Defendant, once the police could have applied for a warrant for prospective CSLI, there was no longer an exigency. The Court disagrees.

In *United States v. Jones*, another judge in this District addressed—and rejected—an argument very similar to the one that Defendant makes here. In that case, the police used an exigency request to obtain real-time CSLI and GPS information to determine a defendant’s location. *Jones*, 2021 WL 7541382, at *3-4. Before receiving any of the location data, the police obtained an arrest warrant, but did not ask the judge for a search warrant for CSLI or GPS information. *Id.* at *4. The defendant argued that the application for the arrest warrant terminated the exigency because, by then, there was no inevitable delay in getting a search warrant. *Id.* at *8. The court disagreed, based on the officer’s testimony that he did not

believe that he had time to prepare a search warrant application or that he needed one anyhow. *Id.* Critically for our purposes, in *Jones*, by the time that law enforcement applied for an arrest warrant, no location data had yet been received. In other words, the warrantless seizure of information could likely have been avoided had the police simply applied for search warrants at the same time they secured an arrest warrant.

Here, T-Mobile had been providing information for several hours pursuant to an exigent request at the time of the arrest warrant application, and Detective Thorpe did not apply for a search warrant because he believed it was unnecessary. He testified that in active kidnapping situations, APD used exigent requests for real-time location information, regardless of whether the target device belongs to the suspect or the victim. (Hr’g Tr. at 15.) And it is important to recall that, during the 18-hour period that the police were searching for J.C. and Defendant, and the police were still actively investigating the case, as they still did not know what car the two were in or Defendant’s precise location. In fact, it was not until the early morning hours of February 26 that APD finally determined the type of car that Defendant was driving. This case is hardly the sort of “mine-run criminal investigation” where law enforcement seek accumulated CSLI to investigate earlier

crimes. *See Carpenter*, 138 S. Ct. at 2223. Instead, it was an active child abduction—one of the specific emergencies that the Supreme Court explained would “likely justify the warrantless collection of CSLI.” *Id.* And the limited nature of the investigation—collecting only real-time location information about Defendant’s movements on public roads—mitigates concerns about the kind of “dragnet-type law enforcement practices” that involve “twenty-four hour surveillance of any citizen” that the Fourth Amendment protects against. *See Knotts*, 460 U.S. at 283-84. Also, there was no settled authority at the time (just as there remains still no settled authority today) establishing that a warrant was necessary to obtain real-time CSLI, especially where the CSLI had been requested based on exigent circumstances. Thus, the Court hesitates to find that the mere passage of time should have caused APD officers to realize that they needed to apply for a warrant to obtain the information that they were already receiving. *See Baker*, 563 F. Supp. 3d at 384 (finding that the fact police applied for a search warrant for the defendant’s house did not extinguish exigency for obtaining CSLI, “a tactic which had not yet been squarely addressed by the courts”). Accordingly, even if the collection of real-time CSLI were a search, suppression is not warranted under the exigency exception to the warrant requirement.

III. CONCLUSION

For the foregoing reasons, it is **RECOMMENDED** that Defendant's motions to suppress [Docs. 29, 30, 34, 54] be **DENIED**.

I have now addressed all referred pretrial matters relating to Defendant and have not been advised of any impediments to the scheduling of a trial. Accordingly, this case is **CERTIFIED READY FOR TRIAL**.

IT IS SO RECOMMENDED this 17th day of February, 2023.



JOHN K. LARKINS III
United States Magistrate Judge