UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA v. EDGAR MEDINA; ALIJAH PARSONS; ANDRES GARAY; IRVING MEDINA; and RONALD HALL, Defendants.	)	No. 21-cr-62-JJM-PAS

MEMORANDUM AND ORDER

JOHN J. MCCONNELL, JR., United States District Chief Judge

Edgar Medina, Alijah Parsons, Andres Garay, Irving Medina, and Ronald Hall are accused of kidnapping a United States Postal Service ("USPS") employee as part of an alleged conspiracy to distribute cocaine. ECF No. 81. Before the Court are six Motions to Suppress cell phone data collected as part of the Government's year-long investigation.[1] The Court has been asked to evaluate a tower dump order (ECF No. 137), a warrant authorizing a search of five cell phones recovered during the suspects' initial arrest (ECF No. 134), three warrants authorizing home searches that resulted in the search of five more cell phones (ECF Nos. 135, 131), and multiple warrants for historical cell-site location information ("CSLI") (ECF

[1] The Court has previously ruled on two additional Motions to Suppress and a Motion to Exclude. *See* ECF No. 164 (granted); text order from November 3, 2023 (denied); ECF No. 195 (denied); text order from August 22, 2023 (denied).

Nos. 138, 215).[2] The Court has also been asked to reconsider Edgar Medina's Motion to Suppress the warrants to search his home, car, and person. ECF No. 238.

I. BACKGROUND[3]

On June 1, 2021, a USPS employee was abducted at gunpoint. Two masked individuals—later alleged to be Edward Medina and Ronald Hall—kidnapped the employee and questioned him about a package that had been delivered empty. The employee was later released without incident. ECF Nos. 1, 81. The United States Postal Inspection Service ("USPIS") launched an investigation to track and identify individuals connected to the kidnapping.

A. Initial Investigation

The initial inquiry was a study in "gumshoe" detective work, consisting of package intercepts, address queries, and conventional surveillance techniques. ECF No. 1-1. Based on queries of the initial package, USPIS identified other packages that had been mailed from Puerto Rico with false names and addresses and located the car that had allegedly been used to abduct the postal worker. *Id.* at 3-10. USPIS intercepted three of the packages and obtained warrants to search them. All three tested positive for cocaine. *Id.* at 10-11.

---

[2] This order initially included two geofence warrants and ten warrants for Google Account Information (ECF No. 136), but the Government has since advised the Court that they do not plan to introduce evidence from these warrants at trial and did not use this information as a basis for subsequent warrants. ECF No. 240.

[3] This is an incomplete timeline; the Court only highlights the events necessary to discuss the challenged warrants. These facts are adopted from affidavits and do not reflect official findings of the Court.

Law enforcement set up an undercover operation and arrested Edgar Medina, Ronald Hall, and Andres Garay when they tried to collect these packages. *Id.* at 11-15. A motor vehicle inventory of the cars they were driving revealed two black expandable batons, defense spray, a Taser, three black surgical masks, and a winter hat that matched the description given by the USPS employee.[4] *Id.* at 15. The Government obtained a search warrant for Mr. Medina's home, which revealed a printout of a USPS tracking number for the original parcel with three $100 bills and a handwritten note that stated: "Need full name Physical + vehicle description of carrier(s) on this very date You will be compensated someone will meet you on Friday or Saturday." *Id.* at 16.

Edgar Medina, Andres Garay, and Ronald Hall were indicted for kidnapping, conspiracy, attempt, and possession with intent to distribute cocaine. ECF Nos. 10, 30, and 81.

B. Cell Phone Investigation

Concurrently, investigators pursued a wide-ranging inquiry into the Defendants' cell phones. ECF No. 175 at 4-14. The cell phone investigation began with a Tower Dump Order and a geofence warrant seeking CSLI and Google Location History for all users in the area. ECF No. 177-4 at 22-32 (21-sw-256-LDA); ECF No. 177-1 at 72-103 (21-sw-260-LDA). The Government then conducted a forensic search of five cell phones recovered during the initial arrests. ECF No. 177-1 at 162-178 (21-sw-274-PAS). These searches revealed incriminating text

[4] Five phones were also recovered and searched. ECF No. 177-1 at 168-69.

messages to Alijah Parsons and Irving Medina, who were later indicted as co-conspirators.[5] ECF No. 175 at 7; ECF Nos. 30, 81.

Based on these text messages—as well as phone calls, handwriting samples, and video surveillance that purportedly showed Alijah Parsons mailing fraudulent packages—the Government requested three warrants for Alijah Parsons to search real-time CSLI (seeking location data) for three cell phones believed to be in her possession. ECF No. 177-1 at 218-290 (21-sw-303-LDA and 21-sw-304-LDA); ECF No. 177-2 at 2-37 (21-sw-305-LDA). This evidence was used to justify a search of Ms. Parsons' home and person. ECF No. 177-2 at 39-150 (21-sw-321-PAS and 21-sw-322-PAS). Multiple cell phones were recovered and forensically searched. ECF No. 177-4 at 59-62. The Government then obtained warrants for historical CSLI for four phones linked to Ms. Parsons, also seeking location data. ECF No. 177-1 at 9-69 (21-sw-255-PAS); ECF No. 177-2 at 198-218, 289-305 (21-sw-526-LDA and 22-sw-197-PAS); ECF No. 177-4 at 2-20 (22-sw-210-PAS); ECF No. 175 at 9.

A similar investigation was conducted for Irving Medina, with warrants issued for real-time CSLI (21-sw-377-LDA, 21-sw-378-LDA, and 21-sw-433-LDA) and a cell-site simulator to locate his phones (21-sw-427-LDA). ECF No. 148-1 at 10-12. Information obtained from these searches—as well as incriminating text messages, phone records, and CSLI obtained from the tower dump—was used to support a warrant to search Irving Medina's home and person. ECF No. 148-1 at 6-13 (21-sw-438-PAS). Two more phones were recovered and forensically searched.

---

[5] Irving Medina was also indicted for possession with intent to distribute fentanyl. ECF No. 81 at 5.

Id. at 22-30; ECF No. 148-2 at 2. The Government then obtained warrants for historical CSLI for Irving Medina. ECF No. 150 at 2-53 (21-sw-428-LDA); ECF No. 150-1 at 2-45, ECF No. 150-2 at 1-54 (21-sw-554-PAS).

With ten phones in hand, the Government requested a second geofence warrant five months after the first. ECF No. 177-2 at 232-287 (21-sw-556-PAS). The Government also requested ten warrants for Google Account Information seeking location history and content-based records (phone records, emails, photos, address lists, video, and audio recordings) for the phones that had been seized pursuant to earlier warrants. *See, e.g.*, ECF No. 177-2 at 307-334 (22-sw-199-PAS).

C. Issues Presented

All told, there were fifty-eight warrants issued in the investigation, fourteen of which—plus a Tower Dump Order under 18 U.S.C. § 2703(d)—have been challenged in Motions to Suppress. ECF No. 176 at 5-6 n.1. Taken together, these warrants offer a sobering tour of modern electronic surveillance techniques. Tower dumps, geofences, cell-site simulators, warrants seeking real-time and historical CSLI: these techniques are not only no longer new, but also are now a standard part of an investigative repertoire.[6] ECF No. 137 at 20.

---

[6] As early as 2013, tower dumps were "a relatively routine investigative technique." Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 2 (2013) (citation omitted). Historical CSLI is "routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses." Evan Caminker, *Location Tracking and Digital Data: Can Carpenter Build A Stable Privacy Doctrine?*, 2018 Sup. Ct. Rev. 411, 463 (2018) (citing *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015)).

In light of law enforcement's reliance on these techniques, courts are increasingly asked to evaluate the rights a person has in their cell phone, which contains near-infinite storage capacity and may contain "[t]he sum of an individual's private life," and to consider how these rights may be protected without knee-capping innovative law enforcement technologies out of the gate. *Riley v. California*, 573 U.S. 373, 394 (2014).

Defendants ask the Court to consider these issues: 1) whether the Supreme Court's holding in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) establishes a reasonable expectation of privacy in short-term CSLI; 2) in the alternative, whether Defendants have a property-based interest such that a warrant is required for a tower dump; 3) whether the affidavits supplying probable[7] cause were properly incorporated; and 4) whether the Government's forensic phone searches lacked particularity.[8] ECF Nos. 134 and 137. Separately, the Court evaluates whether the Government had probable cause to search Defendants' homes, persons, and historical CSLI. ECF Nos. 131, 135, 138, 215, and 238.

The Court examines each of these issues in turn.

---

[7] To establish probable cause, the affiant must show why they "believe that (1) a crime has been committed–the 'commission' element, and (2) enumerated evidence of the offense will be found at the place searched–the . . . 'nexus' element." *United States v. Lindsey*, 3 F.4th 32, 39 (1st Cir. 2021) (citation omitted).

[8] Particularity has two prongs: (1) the warrant "must supply enough information to guide and control [the officer's] judgment in selecting where to search and what to seize," and (2) "cannot be too broad in the sense that it includes items that should not be seized." *Lindsey*, 3 F.4th at 40 (citation omitted); *United States v. Corleto*, 56 F.4th 169, 176 (1st Cir. 2022).

II. STANDARD OF REVIEW

The Fourth Amendment protects "persons, houses, papers, and effects" from "unreasonable searches and seizures." A warrant permitting a search or seizure may not issue "but upon probable cause, supported by Oath or affirmation," and must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

III. DISCUSSION

A. Tower Dump Order

Alijah Parsons was charged as a co-conspirator and initially moved to suppress 21-sw-256-LDA (hereinafter the "Tower Dump Order").[9] ECF Nos. 137, 186. She argues that under *Carpenter*, cell phone users have a reasonable expectation of privacy in their location data as revealed through short-term CSLI. ECF No. 137 at 1. The Government argues that Ms. Parsons lacks standing and that the Tower Dump Order was properly issued. ECF No. 175 at 2.

This argument is now moot as to Ms. Parsons, as the Government has said that they do not plan to introduce this information against her. ECF Nos. 240, 241. The Government acknowledged, however, that evidence from the Tower Dump Order was incorporated into later warrants against Edgar Medina, Irving Medina, and Andres Garay, who have since joined and challenge on the same grounds.[10]

---

[9] The Magistrate Judge granted the Tower Dump Order without a warrant under 18 U.S.C. § 2703(d). ECF No. 177-4 at 28.

[10] The Government has stated that they acquired CSLI for Edgar Medina, Irving Medina, and Andres Garay based on their phones. ECF No. 240. Thus, the Court finds that the Defendants have standing to challenge use of their own

ECF Nos. 240, 242, 245, and 247. The sole issue is whether a search occurred, and if so, whether this evidence should be suppressed as fruit of the poisonous tree.

The Court begins by exploring whether cell phone users have a reasonable expectation of privacy in their short-term CSLI.

1. Background

The Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power'" by "plac[ing] obstacles in the way of a too permeating police surveillance." *United States v. Moore-Bush*, 36 F.4th 320, 320-21 (1st Cir. 2022) (Barron, J., concurring) (internal citations and quotations omitted). To assert a Fourth Amendment right in their persons or effects, a defendant must show that they have a "reasonable expectation of privacy in the area searched and in relation to the items seized." *United States v. Aguirre*, 839 F.2d 854, 856 (1st Cir. 1988). They can do this by showing that they sought "to preserve [something] as private" and "that society is prepared to recognize [this expectation] as [objectively] 'reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citing *Katz v. United States*, 389 U.S. 347, 351-52, 361 (1967)). Or a defendant may establish a Fourth Amendment violation by showing a physical trespass on private property. *See United States v. Jones*, 565 U.S. 400, 404-05 (2012).

The Court assumes that Defendants believed their CSLI to be private. The question is whether the Government "contravened" a reasonable expectation of

---

location data, as obtained from those phones. *See United States v. Ramirez*, 471 F. Supp. 3d 354, 361 (D. Mass. 2020) ("'historical use of' the phone numbers, which produced the CSLI, necessarily satisfies the standing requirement for an individual whose CSLI records have been seized") (citation omitted).

privacy by obtaining this data without a warrant. *Moore-Bush*, 36 F.4th at 328 (Barron, J., concurring). In *Carpenter*, the Supreme Court held that individuals have a reasonable expectation of privacy in "the whole of their physical movements," whether obtained directly through GPS monitoring or indirectly through third-party requests for historical CSLI.[11] 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id.* at 415 (Sotomayor, J., concurring)). Incorporating some of its strongest language on cell phones to date, the Court held that collecting third-party CSLI for seven days constituted a search under the Fourth Amendment. *Id.* at 2217 n.3. The Court held that requests for long-term historical CSLI—like the long-term GPS tracking at issue in *United States v. Jones*—were distinguishable from short-term surveillance that had previously been upheld under the Fourth Amendment.[12] *Id.* at 2215.

The Court took no position on real-time CSLI, tower dumps, conventional surveillance techniques, searches related to national security, or the acquisition of third-party records that might "incidentally" reveal location information, as these issues were not before the Court. *Id.* at 2220. The Court withheld judgment on short-term searches. *Id.* at 2217, n.3 ("[W]e need not decide whether there is a

---

[11] *Carpenter* involved a warrantless search of historical CSLI for a phone number associated with Timothy Carpenter, who was believed to be an accomplice to a series of robberies. 138 S. Ct. at 2212. Police obtained a § 2703(d) order and requested his location data going back seven days and 152 days, respectively.

[12] *See Jones*, 565 U.S. at 430 (Alito, J., concurring) (cited in *Carpenter*, 138 S. Ct. at 2215) (GPS monitoring for twenty-eight days violated the Fourth Amendment because it tracked "every single movement" of the vehicle for close to a month); *contra Knotts*, 460 U.S. at 285 (beeper monitoring did not violate the Fourth Amendment because it was short-term and tracked a vehicle on public roads).

limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny . . . It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."). Finally, the Court limited their holding to location tracking through CSLI, upholding prior cases indicating that an individual has no reasonable expectation of privacy in dialed phone numbers. *Id.* at 2220.

a. Tower Dumps v. Historical CSLI

Carpenter involved a request for long-term "historical CSLI," which is requested when the Government knows the identity of the suspect (or their cell phone number) and asks service providers to disclose "a list of all calls to and from [that] telephone number, along with the locations . . . of the cell towers through which each call originated and terminated." *In re Application of the U.S.A. for an Ord. Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless*, 42 F. Supp. 3d 511, 512 (S.D.N.Y. 2014) (internal citation and quotation omitted). In a tower dump, by contrast, law enforcement identifies the cell towers near the scene of a crime and seeks "[a list of] the telephone numbers that connected to the cell towers during the pertinent time period," along with date, times, and telephone numbers for connecting calls.[13] *Id.*

Tower dumps are used when law enforcement knows the time and place of the crime but not the identity of the suspects. *Cf. United States v. Rhine*, 652 F.

[13] The term "historical CSLI" is a misnomer. Both types of requests involve historical CSLI in that the data is retrospective, but *Carpenter* involved seven days' worth of data for a single person, whereas a tower dump seeks minutes or hours of data for everyone in the area—shorter, but broader in scope.

Supp. 3d 38, 66 (D.D.C. 2023) (describing the same principle in the context of a geofence). By requesting subscriber information for multiple locations, the Government can cross-reference the data to identify who was present at the crime scene.[14] Owsley, *supra* note 6, at 6; Sarah Bramley-Garoutte, Comment, *Priv. After Carpenter v. United States: Can A Tower Dump Warrant Meet the Warrant Requirement?*, 56 Suffolk U. L. Rev. 65, 72 (2023).

Long-term historical CSLI is thus narrowly targeted—it infringes on the privacy of an individual suspect—but is typically quite expansive as to that person, allowing the Government to reconstruct their location for many days or months. *Carpenter*, 138 S. Ct. at 2218 ("With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention [policies] of the wireless carriers."). Tower dumps are narrow as to the individual suspect—they typically seek location data, cell numbers, and subscriber information—but are broad as to third-party data, collecting all phone numbers for users who connected to the relevant cell towers. *Com. v. Perry*, 184 N.E.3d 745, 753-54 (Mass. 2022). Tower dumps routinely scoop up hundreds or thousands of third-party records to pinpoint suspicious accounts. *Matter of Tower Dump Data for Sex Trafficking Investigation*, No. 23 M 87, 2023 WL 1779775, at *2 (N.D. Ill.

---

[14] In a geofence, law enforcement tries to narrow down and identify suspects by canvassing Google Location History for everyone in the area. In a tower dump, they do so by obtaining subscriber information for relevant cell towers. *See generally* Br. of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (Ecf No. 29), *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 3:19-cr-00130-MHL), 2019 WL 8227162.

Feb. 6, 2023) ("Illinois Tower Dump") ("in a dense urban city, it is fair to say that [a tower dump could capture] hundreds, thousands, or hundreds of thousands [of subscribers]"); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) ("[a]ny order authorizing a cell tower dump is likely to affect at least hundreds of individuals' privacy interests"); Owsley, *supra* note 6, at 27-28 (citing a case in which 150,000 telephone numbers were disclosed in order to identify two users).

Here, the Tower Dump Order sought subscriber information for five cell towers near the scene of the alleged surveillance and kidnapping. ECF No. 177-4 at 29-30. The application sought a little over four hours of data across three days. *Id.* For each tower, the Government requested "all records and other information (not including the contents of communications) about all communications, including activations and data transfer information, made using the cell tower during the corresponding timeframes," including:

> a. the telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower ("the locally served wireless device") that registered with the cell tower, including Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), and International Mobile Equipment Identities ("IMEI");
> b. For each communication the "sector(s)" (i.e. the face(s) of the tower(s)) that received a radio signal from the locally served wireless device; and
> c. The date, time, and duration of each communication

Id. at 30-31.

The Government provided AT&T, Sprint/Nextel, Verizon Wireless, and T-Mobile USA with the relevant locations (the five cell towers) and the service providers returned subscriber information for devices that had connected to those towers. This information was used to support warrants for Edgar Medina, Andres Garay, and Irving Medina. ECF No. 240 at 1.

b. *Carpenter* Laid Out a New Framework for Analyzing Cell Phone Location Searches

Prior to *Carpenter*, both short-term and long-term historical CSLI could be obtained without a warrant under 18 U.S.C. § 2703(d), which allows the Government to obtain non-content information from third-party carriers (including names, addresses, phone numbers, and metadata) if they can show "reasonable grounds" that the contents are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(c)-(d).

Courts upheld these orders under the third-party doctrine, which held that individuals have no reasonable expectation of privacy in information that is voluntarily disclosed to a third party. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976) (checks and deposit slips are not the defendant's "private papers" but are business records held by a third party and may thus be properly subpoenaed); *Smith*, 442 U.S. at 742 (individuals have no reasonable expectation of privacy in phone numbers they dial because they voluntarily "convey" those numbers to a telephone switchboard).[15] Because cell phone users "voluntarily disclosed" the

[15] Prior to *Carpenter*, Fourth Amendment challenges were routinely struck down under *Smith* and *Miller*. *See, e.g., In re U.S. for Hist. Cell Site Data*, 724 F.3d

numbers they dialed, all forms of CSLI and other cell phone location data were treated as a third-party business records and were freely searchable under the "reasonable grounds" standard. *See, e.g., United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016) (defendants have no reasonable expectation of privacy in location information voluntarily disclosed to a third party), *rev'd and remanded*, 138 S. Ct. 2206 (2018).

Carpenter upended this paradigm and established that where an individual has a reasonable expectation of privacy—here, in the "whole of their physical movements"—their location data is protected under the Fourth Amendment. In these cases, a § 2703(d) order is not enough, and a warrant supported by probable cause is required, even when the data is held by a third party. 138 S. Ct. at 2221.

The Supreme Court included forceful language on cell phones, noting that "a cell phone—almost a 'feature of human anatomy' [ ]—tracks nearly exactly the movements of its owner [and] faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 2218 (quoting *Riley*, 573 U.S. at 385).

600, 611 (5th Cir. 2013) (historical CSLI is "clearly a business record"); *United States v. Thompson*, 866 F.3d 1149, 1156-58 (10th Cir. 2017), *cert. granted, judgment vacated*, 138 S. Ct. 2706 (2018) (historical CSLI is gathered by "third-party service providers who create records for their own business purposes"); *United States v. Graham*, 824 F.3d 421, 427-28 (4th Cir. 2016) (defendant assumed the risk of disclosure by "expos[ing]" his CSLI to Sprint/Nextel); *United States v. Davis*, 785 F.3d 498, 511-12 (11th Cir. 2015) (court order for the production of MetroPCS's business records did not violate the Fourth Amendment). Many challenges that might have otherwise developed the caselaw on short-term searches v. long-term searches were resolved under the third-party doctrine, thus short-circuiting the underlying questions as to duration.

"In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment." *Id.* at 2223.

The Court suggested that *Smith* and *Miller* were broadly abrogated as to CSLI and other types of cell phone location data:

> [W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements. We decline to extend *Smith* and *Miller* to cover these novel circumstances.

Id. at 2216-17. The Court held that "[g]iven the unique nature of phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 2217. The Court then emphasized that it was a narrow holding and that *Smith* and *Miller* remain in effect for dialed phone numbers and bank records. *Id.* at 2220. The Court left open the question of short-term searches. *Id.* at 2217 n.3.

To determine which cell phone records are protected under the Fourth Amendment, the Court laid out a multifactor test, focusing on the "revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection." *Id.* at 2223. When cell phone tracking encompasses the "whole of [a person's] physical movements" or captures time-

stamped data revealing "familial, political, professional, religious, and sexual associations," it is more likely to be protected. *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). When the acquisition of that data is "easy, cheap, and efficient" compared to traditional investigative tools, it is more likely to be protected. *Id.* at 2217-18. When cell phone tracking achieves "near perfect surveillance" and captures information in both public and private spaces, it is more likely to be protected. *Id.* at 2218. When a search is "retrospective," allowing police to reconstruct a timeline that would otherwise be limited by a "dearth of records" or the "frailties of recollection," it is more likely to be protected. *Id.* When tracking "runs against everyone," allowing police to access user data without knowing in advance who they wish to investigate, it is more likely to be protected. *Id.*

Long-term searches of historical CSLI passed this test with flying colors.

2. After *Carpenter*, Do Users Have a Reasonable Expectation of Privacy in Short-Term CSLI?

The First Circuit has not ruled on tower dumps but has echoed the Supreme Court's language on CSLI, noting that cell-site data may be effortlessly shared without the user's knowledge or intent:

> [E]very time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger . . . [T]hose pings are recorded every time a cell phone application updates of its own accord, possibly to refresh a news feed or generate new weather data . . . such that even a cell phone sitting untouched in a suspect's pocket is continually chronicling that user's movements throughout the day.

United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (a user makes an "affirmative decision" to share their IP address by accessing a website, whereas disclosure of

CSLI is involuntary) (citing *Carpenter*, 138 S. Ct. at 2220). The First Circuit has not yet weighed in on reasonable expectation of privacy for short-term CSLI.[16]

Many other jurisdictions have held that there is no reasonable expectation of privacy in short-term CSLI. *See United States v. Adkinson*, 916 F.3d 605, 610-11 (7th Cir. 2019) (distinguishing the tower dump on other grounds, but noting that the Supreme Court declined to rule on the issue); *United States v. Patterson*, No. 4:19CR3011, 2020 WL 6334399, at *3 (D. Neb. Aug. 5, 2020) (applying the good-faith exception), *report and recommendation adopted*, No. 4:19-CR-3011, 2020 WL 6334406 (D. Neb. Oct. 28, 2020); *United States v. Walker*, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *8 (E.D.N.C. July 20, 2020) (no Fourth Amendment interest and good faith applies); *United States v. Rhodes*, No. 1:19-CR-0073-AT-LTW, 2020 WL 9461131, at *2-4 (N.D. Ga. June 18, 2020) (no Fourth Amendment interest), *report and recommendation adopted*, No. 1:19-CR-73-AT-LTW, 2021 WL 1541050 (N.D. Ga. Apr. 20, 2021). Post-*Carpenter*, some courts have also continued to apply the third-party doctrine. Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 Harv. L. Rev. 1790, 1836-38 (2022).

---

[16] The First Circuit has addressed *Carpenter* in the context of IP addresses (*Hood*, 920 F.3d at 92; *United States v. Morel*, 922 F.3d 1, 9 (1st Cir. 2019)), non-location phone records (*Johnson v. Duxbury, Massachusetts*, 931 F.3d 102, 107 (1st Cir. 2019)), pharmaceutical records (*United States Dep't of Just. v. Ricco Jonas*, 24 F.4th 718, 737-40 (1st Cir. 2022)), and pole camera surveillance (*United States v. Moore-Bush*, 963 F.3d 29 (1st Cir. 2020), *reh'g en banc granted, opinion vacated*, 982 F.3d 50 (1st Cir. 2020), *and on reh'g en banc*, 36 F.4th 320 (1st Cir. 2022)). None of these cases involved tower dumps or cell phone location data, and in these cases, the court has often been at pains to distinguish CSLI from other types of records.

The Court does not believe that *Carpenter* inevitably points to this conclusion. First, the Supreme Court treats disclosure and duration as separate issues, considering on one hand whether Mr. Carpenter's CSLI was voluntarily disclosed (answering in the negative), and asking on the other hand, whether the Government's acquisition of Mr. Carpenter's long-term CSLI was invasive enough to constitute a search (answering in the affirmative). *Carpenter*, 138 S. Ct. at 2217 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."). The Court distinguished between two different lines of cases—cases about "what a person . . . shares with others" (citing *Smith* and *Miller*) and cases involving "physical location and movements" (citing *Knotts* and *Jones*). *Id.* at 2214-17. The facts in *Carpenter*, they held, fell squarely in the latter camp. *Id.* at 2217.

The Supreme Court notes that *Smith* and *Miller* are ill-equipped to deal with the unique issues posed by CSLI. Cell phone location data is a "qualitatively different" type of record because unlike a dialed number, a cell phone "goes wherever its owner goes, conveying . . . a detailed and comprehensive record of the person's movements." *Id.* at 2216-17. "At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers." *Id.* at 2222 (citing *Riley*,

573 U.S. at 386 ("A search of . . . a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents].")).

The Court takes these statements at face value. *See United States v. Diggs*, 385 F. Supp. 3d 648, 657 (N.D. Ill. 2019) ("This court must take the Supreme Court at its word as to the third-party doctrine's pre-*Carpenter* reach") (citing *Mathis v. United States*, 579 U.S. 500, 514 (2016) ("[A] good rule of thumb for reading [Supreme Court] decisions is that what they say and what they mean are one and the same.")). In *Carpenter*, the Supreme Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." 138 S. Ct. at 2217. Far from closing the book on tower dumps, *Carpenter* instructs that *Smith* and *Miller* no longer bar the question. *Id.* The Supreme Court did not expressly *exclude* tower dumps; they simply declined to weigh in on issues not before them. *Id.* at 2220.

The issue is before this Court now, and *Carpenter* gives the Court a straightforward framework to apply it. Under *Carpenter*, the Fourth Amendment question is evaluated based on the "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness" of the search, not whether the cell phone company happens to hold that data. *Id.* at 2234 (Kennedy, J., dissenting). The Court applies the factor-based test in *Carpenter* and finds that USPIS conducted a search when they obtained Defendants' CSLI.

Tower dumps are not long-term searches, and thus do not implicate "the whole of [Defendants'] physical movements," but they do obtain "near perfect

surveillance" of a population at a moment in time. *Id.* at 2217-18. Here, UPSIS acquired data from five towers for over four hours across a densely packed residential neighborhood in Pawtucket, capturing the subscriber information and location history for everyone in the vicinity. ECF No. 177-4 at 29-30. Law enforcement effectively took five snapshots of the entire area, collecting telephone call numbers and unique identifiers "for each wireless device in the vicinity of the cell tower . . . that registered with the cell tower." *Id.* at 31. The order does not distinguish between devices that affirmatively placed a call and devices that passively pinged the towers. *Id.* Nor is it limited to dialed numbers; rather, USPIS sought "all records and other information (not including the contents of communications) about all communications, including activations and data transfer information," for all devices in the area during the relevant period. *Id.* at 30.

This was a comprehensive search, and the data they acquired was intimate and personal. The Tower Dump Order indicates that law enforcement may access information for both sides of the conversation ("For each communication sent or received via the wireless provider's network, these records may include . . . the telephone call number and unique identifiers for the wireless device that connected to the provider's cellular tower and sent or received the communication"). *Id.* at 26. This allowed police to access time-stamped data revealing "familial, political, professional, religious, and sexual associations" for all persons in the area—including Edgar Medina, Irving Medina, and Andres Garay. *Carpenter*, 138 S. Ct. at 2217. The point was not only to capture who was present, but also to reconstruct

a timeline of who the Defendants called, when they called, and how often. *See, e.g.*, ECF No. 148-1 at 12-13 (relying on tower dump data to show not only that Irving Medina was physically present, but also that he made multiple calls to Edgar Medina).

The search was not limited to calls between Defendants; it would have captured this information for all users in the area. And because the cell towers were located in a residential neighborhood, the order would certainly have tracked conversations being held in private homes, by people not under investigation. *See United States v. Karo*, 468 U.S. 705, 714 (1984) (monitoring in a residence is subject to the Fourth Amendment); *United States v. Powell*, 943 F. Supp. 2d 759, 775 (E.D. Mich. 2013) ("If at any point a tracked cell phone signaled that it was inside a private residence . . . the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant."), *aff'd*, 847 F.3d 760 (6th Cir. 2017).

A tower dump is "easy, cheap, and efficient" compared to traditional investigative techniques. *Carpenter*, 138 S. Ct. at 2218. To replicate these searches with traditional surveillance, police would have had to cross-reference lists by hand and knock on hundreds of doors to obtain the identities of all persons near the kidnapping. To obtain call logs and duration information, they would have had to search every phone individually. This type of search would be logistically impossible without a § 2703(d) order. Moreover, it was a "retrospective" search, allowing the Government to "travel back in time" to reconstruct Defendants'

locations and identities. ECF No. 177-4 at 26; *Carpenter*, 138 S. Ct. at 2218. There was no need for the Government to identify ahead of time who they wished to search, because they could simply pull the records and use them identify the suspects after the fact.

Finally, the tracking "runs against everyone," allowing police to access a high volume of user data in a way that would be impossible to do with traditional surveillance. *Carpenter*, 138 S. Ct. at 2218. CSLI is "continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation." *Id.* The Government acknowledged at oral argument that USPIS did not just acquire subscriber information for Edgar Medina, Irving Medina, and Andres Garay. They acquired it for everyone in the area for a period of over four hours. "There is no historic analogue for the ability effortlessly to compile . . . the locations, identities, and associations of tens of thousands of individuals, just in case one might be implicated in a criminal act." *Perry*, 184 N.E.3d at 762 (holding that warrant is required for a multi-day tower dump, even when it produces only three hours of CSLI).

Courts that have been asked to evaluate geofence warrants—which are similar to tower dumps, and likewise implicate CSLI—have largely declined to apply *Smith* and *Miller* and have further indicated that *Carpenter* should apply to short-term searches. In *United States v. Chatrie*, the court noted that two hours of Google Location History was akin to the historical CSLI at issue in *Carpenter* because it was "detailed, encyclopedic, and effortlessly compiled." 590 F. Supp. 3d

901, 935-36 (E.D. Va. 2022) (citing *Carpenter*, 138 S. Ct. at 2216). Even when a user affirmatively enables Google Location History, he "simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up Google Assistant." *Id.* In *Chatrie*, the court distinguished *Smith* and *Miller* and noted that a geofence request might well require a warrant under the test outlined in *Carpenter*.[17] *Id.* Likewise, in *Matter of Search of Info. Stored at Premises Controlled by Google*, the court observed that "there is much to suggest that *Carpenter*'s holding . . . should be extended to the use of geofences involving intrusions of much shorter duration." 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020).

In *United States v. Moalin*, the Ninth Circuit (analyzing the NSA's bulk data collection program) stated that *Smith* and *Miller* likely do not extend to metadata such as originating or terminating phone numbers, IMSI and IMEI numbers (i.e., unique identifiers associated with particular users or devices), or location data. The court noted that "[i]f you have enough metadata you don't really need content," and that "in recent years the distinction between content and metadata 'has become increasingly untenable.'" 973 F.3d 977, 989-92 (9th Cir. 2020) (internal citations and quotations omitted). For instance:

> A woman calls her sister at 2:00 a.m. and talks for an hour. The record of that call reveals some of the woman's personal information, but

---

[17] These cases deal in hypotheticals because Google requires a warrant before disclosing subscriber information for a geofence request, so reasonable expectation of privacy is typically not at issue. *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 359-60 (N.D. Ill. 2020) (citation omitted).

> more is revealed by access to the sister's call records, which show that the sister called the woman's husband immediately afterward. Or, a police officer calls his college roommate for the first time in years. Afterward, the roommate calls a suicide hotline. These are simple examples; in fact, metadata can be combined and analyzed to reveal far more sophisticated information than one or two individuals' phone records convey.

Id. The ability to cross-reference a large body of data makes it "relatively simple to superimpose our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups and quickly paint a picture that can be startlingly detailed . . . identify[ing] the strength of relationships and the structure of organizations." *Id.* (citing Br. of Amici Curiae Brennan Center for Justice et al. at 21, *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020) (No. 13-50572), 2015 WL 6966514 ("Brennan Center Amicus Brief")). A savvy investigator does not need seven days of data to do this type of analysis: they could do it with phone numbers collected over an hour or two—and notably, could conduct this type of inquiry for anyone in the target location.

Even before *Carpenter*, some judges opted not to follow *Smith* and *Miller* and required a warrant for a tower dump, citing the need to protect third-party information. *See, e.g., In re U.S. ex rel. Ord. Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 700-02 (S.D. Tex. 2012) (denying a § 2703(d) request that failed to safeguard third-party data); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d at 770-71 (granting a warrant for the same). After *Carpenter*, many law enforcement agents have erred on the side of caution and simply gotten a warrant. *See, e.g., Matter of Search of Info. Associated with Cellular Tel. Towers Providing*

Serv. To [Redacted] Stored at Premises Controlled by Verizon Wireless, 616 F. Supp. 3d 1, 8-9 (D.D.C. 2022) ("DC Tower Dump") (following *Carpenter*'s "murky" ruling, the government chose to pursue a warrant "out of an abundance of caution") (internal quotation omitted); *United States v. Foster,* No. 3:21-CR-00114-SLG, 2023 WL 155442, at *1 (D. Alaska Jan. 11, 2023) (evaluating a tower dump warrant); *Illinois Tower Dump*, 2023 WL 1779775, at *1 (granting a tower dump warrant that included protocols for managing third-party information).

Smith and *Miller* do not apply here because this case involves CSLI, which is not "voluntarily exposed" in the same way that a dialed number or a bank record is shared with a third party. The Government seeks more than just a dialed number when requesting a tower dump order: the goal is to associate that number with subscriber information, identify a suspect, track their location, and reconstruct their conversations. Owsley, *supra* note 6, at 17; *see also* Brennan Center Amicus Brief at 7 ("Today, communications metadata easily reveals lawful, First Amendment-protected activities in a way that was unimaginable when the Court decided *Smith* in 1979."). The disclosure of a single phone number may not implicate the Fourth Amendment under *Smith*, but the aggregation of many numbers—paired with the geolocation data linked to specific towers and the request for subscriber information—surely does. Brennan Center Amicus Brief at 22.

Nor can the Court draw an easy comparison with the short-term search at issue in *Knotts*, which was previously upheld by the Supreme Court. In *United States v. Knotts*, police used a beeper to track a vehicle. 460 U.S. 276, 278 (1983).

The Supreme Court held that this was not a search because it was essentially "augment[ed]" visual surveillance: police followed a car for a short distance, on public roads, where the vehicle's path was "voluntarily conveyed to anyone who wanted to look." *Id.* at 281-82 (cited in *Carpenter*, 138 S. Ct. at 2215). Tower dumps, by contrast, identify a suspect by cross-referencing hundreds or thousands of records collected from all users (whether physically located in public or private spaces) in the target area. Bramley-Garoutte, *supra*, at 72. This is qualitatively different from the type of search at issue in *Knotts.* Furthermore, whereas *Knotts* involved tracking in public, here police had good reason to believe that the towers in question served residential areas, for the simple reason that the crime took place near the USPS employee's home. *See Karo*, 468 U.S. at 714 (holding that the Fourth Amendment is violated when a beeper is tracked into a private home).

Finally, the Tower Dump Order is not comparable to traditional methods of surveillance, such as short-term video surveillance. It is true that, as with traditional surveillance, a geofence or tower dump captures a person's "movement at a particular time." *Carpenter*, 138 S. Ct. at 2220. But if a tower dump were reimagined as a visual search, it would be one in which police could look at a few minutes of video surveillance—a brief aerial snapshot of a city block, for instance—and instantly derive the name, address, connecting phone records, length of service, telephone number, and payment information for every person in the vicinity, as well as their physical location. *See* 18 U.S.C. § 2703(c)(2) (describing what can be retrieved in a § 2703(d) order). *Carpenter*'s narrow application was meant to

preserve traditional surveillance methods, not authorize sweeping mass surveillance techniques for all users in the area. *See, e.g., Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341-42 (4th Cir. 2021) (*Carpenter* "squarely applies" to an aerial surveillance program that "tracks every movement" of every person outside in Baltimore City for forty-five days). A tower dump is not the same as simply looking at a few minutes of surveillance tape, because the ability to quickly associate vast amounts of data allows law enforcement to see far more than what simple visual surveillance would reveal and extends effortlessly into both public and private spaces. *See Karo*, 468 U.S. at 714; *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that the Fourth Amendment is violated where the government uses sense-enhancing technology not available to the public to search a home).

The "basic purpose of [the Fourth] Amendment" is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Carpenter*, 138 S. Ct. at 2213 (citation omitted). People quite reasonably assume that the Government should not be able to use your cell phone to spy on you. Here, the Government engaged in mass surveillance of an entire population for over four hours. This was a violation of the Fourth Amendment.

The Court finds that Defendants have a reasonable expectation of privacy in their short-term CSLI, and thus a warrant was required for the Tower Dump Order.

3. After *Carpenter*, Do Users Have a Property-Based Right in their Short-Term CSLI?

Defendants—through Ms. Parsons—also argue that their CSLI constitutes "papers and effects," and they thus have a property-based interest under the Fourth Amendment based on 47 U.S.C. § 222, which prohibits telecommunications carriers from disclosing user information without consent.[18] ECF No. 137 at 13-15 (noting that § 222 classifies CSLI as "customer proprietary information").

The Court need not reach this argument, having determined that the Defendants have a reasonable expectation of privacy in their CSLI. They also have not provided enough information to determine whether the CSLI is "[theirs] under law." *Carpenter*, 138 S. Ct. at 2267-68, 2272 (Gorsuch, J., dissenting). They have not articulated which provisions in their provider's privacy policy would support the argument that CSLI is protected, or which provisions of the law—beyond a bare reading of § 222(f)—support a property-based interest. Without more information, a property-based claim to these records is speculative.

4. Good-Faith Exception

The Government argues that even if Defendants have a reasonable expectation of privacy, the Court should uphold the Tower Dump Order under the good-faith exception. ECF No. 175 at 29-31; ECF No. 246 at 2-3.

---

[18] This argument has been developed elsewhere by the Brennan Center for Justice, the American Library Association, the Electronic Privacy Information Center, and others. *See* Brennan Center Amicus Brief at 22-25 ("Communications metadata . . . demands Fourth Amendment protection, no less than pamphlets or hard copy letters."). It was also raised by Justice Gorsuch in *Carpenter*, who argued that users may retain property rights in metadata even when this information is stored and held by a third party. 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

Under *United States v. Leon*, a warrant that violates the Fourth Amendment may still be upheld unless (1) the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; (2) the warrant is "so facially deficient—i.e., 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"; (3) the Magistrate Judge "wholly abandoned his judicial role"; or (4) the judge was "misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." 468 U.S. 897, 923 (1984) (citations omitted).

When police rely on binding appellate precedent that explicitly authorizes a given practice but is later held to be unconstitutional, the good-faith exception applies. *Davis v. United States*, 564 U.S. 229, 249-50 (2011); *see also Illinois v. Krull*, 480 U.S. 340, 349-50 (1987) (good-faith exception applies to a warrantless search where law enforcement relied in good faith on a statute that was later held to be unconstitutional). Less clear is how it applies to areas where the law is simply unsettled. As Justice Sotomayor has noted, "when police decide to conduct a search or seizure in the absence of case law . . . specifically sanctioning such action, exclusion of the evidence obtained may deter Fourth Amendment violations." *Davis*, 564 U.S. at 251 (Sotomayor, J., concurring). The First Circuit has emphasized that "where judicial precedent does not clearly authorize a particular practice, suppression has deterrent value because it creates an 'incentive to err on

the side of constitutional behavior.'" *United States v. Sparks*, 711 F.3d 58, 64 (1st Cir. 2013) (citation omitted).

Here, no warrant was acquired, and any discussion of whether it would have been sufficient on these facts is entirely speculative. The issue is whether USPIS believed in good faith that they could obtain short-term CSLI through a § 2703(d) order rather than a warrant. Given that the Supreme Court expressly declined to rule on tower dumps, was it reasonable to assume that a § 2703(d) order was sufficient? Or did the holding in *Carpenter* effectively put USPIS on notice that other forms of electronic surveillance—tower dumps, cell-site simulators, and real-time CSLI—might also require a warrant going forward? There is no First Circuit case on point, and the Supreme Court's guidance is less than clear.

So, the Court will fall back on the touchstone of "reasonableness" in its analysis. *Riley*, 573 U.S. at 381-82 (citation omitted). The Court finds that on these facts, it was reasonable for USPIS to rely on the judge's order. The plain language of *Carpenter* does not obviously put law enforcement on notice that tower dumps are constitutionally suspect. 138 S. Ct. at 2220. And the plain language of 18 U.S.C. § 2703(c) permits the Government to obtain CSLI using either a warrant or an order. 18 U.S.C. § 2703(c) (a service provider must disclose a record "when the governmental entity—(A) obtains a warrant . . . [or] (B) obtains a court order for such disclosure under subsection (d)"). The fact that some officers have sought a warrant out of an "abundance of caution" does not suggest that everyone is required to do the same. *DC Tower Dump*, 616 F. Supp. 3d at 8-9.

Importantly, USPIS didn't hide the ball: they flagged the issue for the Magistrate Judge, who approved the order. ECF No. 177-4 at 22-23, n.1. In his § 2703(d) application, USPIS Inspector Richard Atwood acknowledged that tower dumps were something of an open question but distinguished the tower dump order from the long-term search at issue in *Carpenter*. *Id.* The Court does not agree that tower dumps are wholly novel or that the good-faith exception should automatically apply when a case involves unsettled law. ECF No. 246 at 3 (citing *United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017)). But here, USPIS acknowledged the ambiguity upfront and put the issue to the judge to decide.[19]

Finally, in the wake of *Carpenter*, USPIS would have been hard-pressed to find clear guidance in lower court rulings. Post-*Carpenter*, tower dump warrants are increasingly common and are routinely evaluated by district courts. *See, e.g.*, *DC Tower Dump*, 616 F. Supp. 3d at 8-9; *Foster*, 2023 WL 155442, at *1; *Illinois Tower Dump*, 2023 WL 1779775, at *1. But these cases have largely involved warrants that were voluntarily sought. Few courts have required a warrant, and the Government cites ample precedent that goes the other way. *See, e.g.*, *Adkinson*, 916 F.3d at 611; *Rhodes*, 2020 WL 9461131, at *2. Here, the good-faith exception should apply.

The Court does not reach this conclusion lightly. Applying the good-faith exception means upholding a search that was conducted without probable cause. 18 U.S.C. § 2703(d) (an order merely requires "specific and articulable facts showing

[19] Nothing suggests that the Government sought a Tower Dump Order to circumvent the requirements for particularity and probable cause.

that there are reasonable grounds to believe [that the records] are relevant and material to an ongoing criminal investigation."). It also relieves the Government of the obligation to show particularity. U.S. Const. amend. IV. But in this case, the Government was operating in a context where the Supreme Court expressly declined to rule, the statute does not require a warrant, precedent points in both directions, and a judge approved the order. It was thus reasonable for USPIS to assume that they could rely on the § 2703(d) order. The *Leon* good-faith exception applies.

For these reasons, the Court DENIES Defendants' Motion to Suppress evidence from the Tower Dump Order. ECF Nos. 137, 242, 245, and 247.

B. "Five Phones Warrant"

The Court turns to Ronald Hall's challenge—joined by Edgar Medina and Andres Garay—seeking to suppress evidence obtained from five phones recovered during the initial arrests (21-sw-274-PAS, hereinafter "Five Phones Warrant").[20] ECF No. 134. Mr. Hall argues that the affidavits accompanying the search warrant were not attached when the application was presented to the Magistrate Judge, and so the application failed to establish probable cause. *Id.* at 1. He also argues that the warrant is overbroad.[21] *Id.* The Government acknowledges that the affidavits

---

[20] This warrant uncovered voluminous evidence against these three Defendants—including call logs, contacts, internet searches, photographs, videos, and user attribution data—as well as incriminating text messages that implicated Irving Medina and Alijah Parsons as co-conspirators. ECF No. 176 at 9.

[21] Mr. Hall also initially sought a *Franks* hearing, which was denied because there was no showing of any false or reckless statement in the warrant application.

were not attached but argues that the warrant should be upheld under the good-faith exception. ECF No. 176 at 12. They also challenge standing.[22] *Id.* at 11.

The Court turns to the first issue, incorporation.

1. Incorporation of Affidavits

The Five Phones Warrant relied on two affidavits to show probable cause, Exhibits A and B, that were not attached to the warrant application.[23] The section on probable cause begins, "As set forth in Exhibits A and B, I believe MEDINA, GARAY, HALL and others are responsible for arranging the shipments of large amounts of controlled substances." ECF No. 177-1 at 168. But as the Government acknowledges, "[n]either the U.S. Attorney's Office, nor the Court, has any record of Exhibits A and B having been submitted to the Court with the 21-SW-274 application packet."[24] *Id.* at 3-4.

Mr. Hall correctly notes that because 21-sw-274-PAS relied on the unattached affidavits to show probable cause ("As set forth in Exhibits A and B"), the warrant is invalid as lacking in demonstrable probable cause. ECF No. 134 at 3. The law in this Circuit is that an attached affidavit may supply probable

---

[22] Regarding standing, the Defendants acknowledge that they own the phones. ECF No. 183 at 8. To the extent that they seek to challenge their own text messages, the Defendants thus have standing to challenge a search of these phones. *See Aguirre*, 839 F.2d at 856-57 (a defendant has standing if they can show ownership, possession, control, historical use, or the ability to regulate access).

[23] Exhibit A described facts related to the kidnapping, including the fact that one of the suspects was observed using a phone in the victim's driveway. ECF No. 134-1 at 40-51. Exhibit B refers to the complaint affidavit, which notes that Edgar Medina was seen using a phone on the day of his arrest. *Id.* at 58-75.

[24] The record suggests that there are at least four other instances where affidavits were referenced but not attached, and up to fifteen where the affidavit was attached but not incorporated. ECF No. 183-1 at 2; ECF No. 177-1 at 2-4.

cause "if the affidavit accompanies the warrant, and the warrant uses suitable words of reference which incorporate the affidavit." *United States v. Sheehan*, 70 F.4th 36, 50 (1st Cir. 2023).

Sheehan involved a child pornography investigation in which an officer—having failed to show probable cause in the primary affidavit—sought to search a cache of devices based on an underlying affidavit that was neither expressly incorporated nor attached. *Id.* at 48-50. The Government tried to argue that the affidavit was "implicitly incorporated" because it was issued consecutively and referred to by docket number, so the authorizing clerk would presumably have been aware of the facts. *Id.* at 49. The First Circuit rebuffed these arguments, noting that "[u]nder . . . established circuit precedent, incorporation [requires] both suitable words to that effect and the attachment of the affidavit." *Id.* at 50 (citing *United States v. Moss*, 936 F.3d 52, 59 n.9 (1st Cir. 2019); *United States v. Klein*, 565 F.2d 183, 186 n.3 (1st Cir. 1977)). "Submitting a warrant application so deficient in probable cause such that no officer could reasonably rely upon it is exactly the kind of police conduct the exclusionary rule was meant to deter." *Id.* at 54. Therefore, when the primary affidavit lacks probable cause, an unattached affidavit cannot be relied on to supply it. *Id.* at 50-51.

a. Good Faith

The Government pleads good faith, arguing that this was merely a "filing error," that there was no misconduct, and that the error should be attributed to the Assistant United States Attorney who filed the application rather than the affiant.

ECF No. 176 at 12-13. They argue that under *Herring v. United States*, only "*purposeful* conduct" may trigger the exclusionary rule. *Id.* at 14. They note that the warrant packet was prepared separately and in haste, and that it was reasonable—in the heat of the moment—for Inspector Atwood to file it without checking, and to assume that the Magistrate Judge knew the facts. *Id.* at 16-17.

This argument contradicts the plain language of *Sheehan*, which emphasizes that failing to attach the affidavit showing probable cause goes to the "core competency of a police officer." 70 F.4th at 54. It also contradicts *Leon*, which holds that suppression is appropriate where an officer "could not have harbored an objectively reasonable belief in the existence of probable cause." 468 U.S. at 926. The operative question is not whether Inspector Atwood was reckless, but whether an officer objectively acts in good faith when relying on a warrant that is wholly lacking in probable cause. *Sheehan*, 70 F.4th at 54-55. The First Circuit explained that "[t]he expansion of the good-faith exception in *Herring v. United States*, [555 U.S. 135 (2009)] to cases involving police negligence does not alter our analysis . . . Nothing in *Herring* suggests an expansion of the good-faith exception to circumstances that *Leon* previously held to be beyond the pale—such as the issuance of a warrant based on an affidavit 'so lacking in indicia of probable cause' as to render any reliance on it 'entirely unreasonable.'" *Sheehan*, 70 F.4th at 54 (citing *Leon*, 468 U.S. at 923).

The Government emphasizes that the Court should look at "all of the circumstances" when assessing good faith. ECF No. 176 at 15. But here, as in

Sheehan, the error lies with the Government. It matters little whether the error was committed by the affiant, the Assistant United States Attorney, or the paralegal tasked with uploading the file. ECF No. 177-1 at 2-4. The issue of "who prepared the warrant application" was explored exhaustively at oral argument, but under *Leon*, good faith is required of all of the officers, whether they executed the warrant, applied for it, or provided material information. 468 U.S. at 923 n.24.

Nor was Inspector Atwood entirely blameless. The record indicates that "[n]either the U.S. Attorney's Office, nor the Court, has any record of Exhibits A and B having been submitted to the Court with the 21-SW-274 application packet." ECF No. 177-1 at 4. Nevertheless, he swore out the application and attested to their existence. *Id.* at 3. It was thus objectively unreasonable for him to rely on the Magistrate Judge's issuance of that warrant.[25] *Sheehan*, 70 F.4th at 51 ("[B]ecause petitioner himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate's assurance that the warrant [was valid].") (citing *Groh v. Ramírez*, 540 U.S. 551, 563-65 (2004)). The affiant is responsible for the materials he submits and a judge's failure to catch the error does not mitigate an officer's unreasonable conduct in failing to establish probable cause. *Id.*

The Court has every reason to believe this was an unintentional mistake. As the Government points out, "no officer has an incentive to deliberately make [this

---

[25] It is irrelevant that the Magistrate Judge may have been apprised of the facts because a judge may not consider unattached, external materials to a warrant. *Sheehan*, 70 F.4th at 50. Here, moreover, the Magistrate Judge could not have simply looked back through the file to identify "Exhibit A," because there were nine previous affidavits it could potentially have referenced. ECF No. 176 at 8.

type of] error." ECF No. 176 at 18. But where the error results in a warrant wholly lacking in probable cause, there is no need to conduct "an additional or individualized assessment of the deliberateness and culpability of police conduct."[26] *Sheehan*, 70 F.4th at 54. "Submitting a warrant application so deficient in probable cause such that no officer could reasonably rely upon it is exactly the kind of police conduct the exclusionary rule is meant to deter . . . If the good-faith exception is to have any limits, it cannot encompass the police conduct that occurred here." *Id.* at 54-55. The good-faith exception does not save the Government's error.

b. Probable Cause

The Government argues, in the alternative, that the primary affidavit (even absent the Exhibits) contained sufficient facts to show probable cause. ECF No. 176 at 20. They argue that the affidavit "reminded the Judge that she had found probable cause to arrest the defendants the day before" and that the bare facts—including the fact that an investigation was ongoing and that five phones had been recovered from Defendants' cars—are enough to show probable cause. *Id.* at 23-24.

When evaluating a warrant, the Court looks to the "four corners of the affidavit." *United States v. Lindsey*, 3 F.4th 32, 39 (1st Cir. 2021) (citation omitted).

---

[26] The Court notes that the same conclusion would be reached under *Herring*, since here there is evidence of "systemic error." 555 U.S. at 147-48; *see* ECF No. 183-1 at 2; ECF No. 177-1 at 2-4. The Court is particularly concerned that, in canvassing the fifty-eight warrants in this case, the Government failed to identify and disclose at least one additional warrant that lacked probable cause due to an incorporation error. ECF No. 215; *see infra* Part D. Such errors go to the "core competency of a police officer, disrupt the public's faith in the justice system, and compromise the reliability of the Government's investigation. *Sheehan*, 70 F.4th at 54. Under either standard, it would be appropriate to suppress the evidence.

Here, Inspector Atwood begins with express words of incorporation ("I hereby incorporate all background facts from [Exhibits A and B]") and purports to establish probable cause by reference:

> As set forth in Exhibits A and B, I believe MEDINA, GARAY, HALL and others are responsible for arranging the shipments of large amounts of controlled substances, to wit, cocaine, from individuals in Puerto Rico. The controlled substances were sent to the Providence area for distribution of those drugs in the Providence area. An investigation is ongoing into a June 1, 2021 armed abduction of a United States Postal employee who, in the course of the abduction, was asked about the contents of one such shipment. Information gleaned in the course of the investigation reveals that the suspects utilized cell phones to both conduct surveillance on the Postal employee before abducting him, and to communicate on the dates of suspect parcel deliveries.

ECF No. 177-1 at 167-68. Taken as a whole, this paragraph states that 1) someone sent drugs to Providence; 2) a kidnapping is being investigated; 3) "[i]nformation gleaned in the course of the investigation" suggests that the Defendants used cell phones to commit these crimes. The affidavit thus establishes that crimes were committed (drug trafficking and armed abduction) but fails to connect the Defendants to either crime or show a nexus to the phones in question.

The application then states that the five phones were recovered from the Defendants' cars after they "attempted to retrieve suspect parcels." *Id.* at 168-69. No facts are included as to what parcels they attempted to retrieve or why they were suspect. It goes on to state general facts about drug trafficking based on Inspector Atwood's "training and experience," including the observation that drug traffickers often maintain records and communicate by cell phone, and that "it is common for drug traffickers to own multiple phones of varying sophistication and

cost."[27] *Id.* at 169-70. The relevant facts connecting the Defendants or their phones to the crimes in question are "set forth in Exhibits A and B," which are not attached. *Id.* at 168.

This is far less than the probable cause showing in *Sheehan*, which was roundly struck down by the First Circuit.[28] 70 F.4th at 47. Here, there are no facts that an officer could reasonably rely on to show probable cause, and no nexus between the alleged crime (kidnapping and drug trafficking) and the place to be searched (the phones in question). The warrant application is entirely conclusory, and an affidavit that is conclusory as to nexus "is not sufficient to establish the necessary probable cause." *Illinois v. Gates*, 462 U.S. 213, 239 (1983).

Without Exhibits A and B, there is no "substantial basis" from which the Magistrate Judge could infer that relevant evidence would be found on the phones. *Id.* Inspector Atwood's beliefs as to Defendants' involvement are relevant but are not sufficient to show probable cause. *Id.* (a magistrate cannot solely rely on the affiant's sworn statement that he "has cause to suspect and does believe" that Defendants committed a crime) (internal quotation omitted). The fact that he

---

[27] The recovery of multiple phones, paired with the officer's "training and experience," can be enough if there is "substantial evidence [of drug trafficking] in the warrant application." *See Lindsey*, 3 F.4th at 39-40. But here the warrant application lacks such facts and relies on conclusory observations as to the Defendants' involvement in these crimes.

[28] In *Sheehan*, the warrant included a "cursory" description of the allegedly pornographic images, a statement that Sheehan had previously been arrested for indecent assault and battery of a minor, and an explanation of how police had obtained the devices. 70 F.4th at 47. The First Circuit held that this provided "almost no basis, never mind a substantial basis, from which the magistrate could infer that Sheehan's phone contained child pornography." *Id.*

intended to rely on Exhibits A and B to supply probable cause makes the omission all the more glaring.

For these reasons, the Government's argument that the primary affidavit (even absent the Exhibits) contained sufficient facts to show probable cause fails.

2. Overbreadth

Having already determined that the warrant is invalid for lack of probable cause, the Court declines to evaluate particularity and overbreadth. ECF No. 134.

That said, the Court is skeptical of the Government's position that a "computer-assisted [scan] of the entire medium" was justified at this early stage in the investigation, when at best, there was probable cause to believe that Defendants used their cell phones to make phone calls. ECF No. 177-1 at 175. The Court is concerned, likewise, that the Five Phones Warrant did not include the search protocols adopted in earlier and later searches to ensure that the inquiry was appropriately limited to items for which the Government had probable cause.[29] *See, e.g.*, ECF No. 177-2 at 49-51 ("Search Procedure for Digital Device(s)").

But in the First Circuit, "[t]he remedy in the case of a seizure that casts its net too broadly is . . . not blanket suppression but partial suppression." *United States v. Aboshady*, 951 F.3d 1, 9 (1st Cir. 2020) (citation omitted). Even if the scope of the warrant was too broad, "[Defendants] would only be entitled to suppression of those [materials] . . . that reasonably fell outside the scope of the

[29] At oral argument, the Government argued that these protocols were not required and did not limit these searches in any way. *See, e.g.*, ECF No. 252 at 3-5. Suffice it to say, this position does not alleviate the Court's concerns.

warrant." *Id.* To date, Mr. Hall has not specified what evidence, if any, was outside the scope of the warrant, and the Court has not been presented with any evidence showing the Government's intended use of evidence that is unsupported by probable cause. As such, the Court declines to consider the warrant on these grounds. If Defendants point to any specific evidence that the Government seeks to use that was not supported by probable cause, the Court will entertain that motion.

The Five Phones Warrant is invalid because it failed to incorporate Exhibits A and B and was otherwise lacking in probable cause. As such, it was objectively unreasonable for Inspector Atwood to rely on it. *Leon*, 468 U.S. at 923. There is no need for the Court to consider overbreadth.

For these reasons, the Court GRANTS the Motion to Suppress the Five Phones Warrant. ECF No. 134.

C. Search of Home and Person

The Five Phones Warrant revealed incriminating text messages between multiple Defendants. These messages were used with other evidence to justify the seizure of five more phones, which were taken pursuant to home searches for Alijah Parsons and Irving Medina and forensically searched according to a detailed search protocol. *See, e.g.*, ECF No. 177-2 at 53-96.

Irving Medina and Alijah Parsons write separately to challenge the searches of their homes and persons, including the searches of five cell phones recovered. ECF Nos. 131, 148, 135. Edgar Medina further asks the Court to reconsider the

search of his home, person, and vehicle. ECF Nos. 129 (denied), 238 (renewed). The Government objects. ECF Nos. 170, 172, 243.

1. Standard for a Home Search

A warrant to search a home—like any other warrant—must be supported by probable cause, determined based on the totality of the circumstances, considering the "type of crime [and] the nature of the items sought." *Gates*, 462 U.S. at 230-31; *United States v. Charest*, 602 F.2d 1015, 1017 (1st Cir. 1979). The affidavit must show that "(1) a crime has been committed–the 'commission' element, and (2) enumerated evidence of the offense will be found at the place searched–the . . . 'nexus' element." *Lindsey*, 3 F.4th at 39 (citation omitted). To establish nexus, the Government needs to show why they believed there was a "fair probability" that phones (or other evidence of drug crimes) would be recovered at the Defendants' residences. *Gates*, 462 U.S. at 238.

A judge may base this determination on circumstantial evidence. *United States v. Gonzalez-Arias*, 946 F.3d 17, 24 (1st Cir. 2019) (probable cause may exist to search for drugs in a home even if "agents or their informants never spotted the illicit objects at the scene"). But mere knowledge that a defendant is a drug dealer is not enough, and the First Circuit has "expressed skepticism that probable cause can be established by the combination of the fact that a defendant sells drugs and general information from police officers that drug dealers tend to store evidence in their homes." *United States v. Roman*, 942 F.3d 43, 51-52 (1st Cir. 2019) (citation omitted). For this reason, "generalized observations" must be "combined with

specific observations" that link drug activity to the home. *Id.* at 52 (citation omitted). Where these facts exist, probable cause may be shown. *See, e.g., United States v. Ribeiro*, 397 F.3d 43, 50-52 (1st Cir. 2005).

2. Irving Medina

Irving Medina argues that the warrant to search his home was not supported by probable cause. ECF Nos. 131, 148 (challenging 21-sw-438-PAS). The warrant application alleged that Irving Medina participated in the kidnapping by conducting surveillance of the USPS employee prior to his abduction, that he used two cell phones to arrange surveillance, and that the phones in question, Phone-5346 and Phone-5288, would be found in his home. ECF No. 148-1 at 6-15, 22. Mr. Medina argues that there is no evidence of knowledge to support an accomplice theory and no "nexus" to the home because the Government has not shown that drug activities took place there. ECF No. 148 at 16; ECF No. 251.

When the Court is reviewing a warrant, "great deference" should be paid to the magistrate's determination of probable cause, and the warrant will be upheld if the Court determines that the magistrate had a "substantial basis" for believing that the search would reveal evidence of a crime. *Gates*, 462 U.S. at 236 (citation omitted). To support the claim that Irving Medina agreed to conduct surveillance (and thus was involved in the commission of a crime), the warrant points to a text exchange involving Phone-5288 dated May 28, four days before the kidnapping:

> GARAY: "Are you comfy taking the Taurus to the bucket?[30]" – 1:34:59 pm
> I. MEDINA's phone no.: 5288: "I don't' see why not" – 1:35:12 pm

[30] A derogatory nickname given to the City of Pawtucket.

GARAY: "Cool" – 1:36:17 pm
GARAY: "When can you head there?" – 1:36:37 pm
I. MEDINA's phone no.: 5288: "Right now if you want" – 1:38:18 pm
GARAY: *sends a photo of an aerial satellite photo of the Pawtucket Post Office, located at 40 Montgomery Street.* – 1:38:26 pm
GARAY: "OK cool" – 1:38:26 pm
I. MEDINA's phone no.: 5288: "WTH is that" – 1:38:46 pm
GARAY: "Read the streets" – 1:38:57 pm
I. MEDINA's phone no.: 5288: "Go there" – 1:39:04 pm
GARAY: "Try to park in there" – 1:39:08 pm
I. MEDINA's phone no.: 5288: "I did" – 1:39:09 pm[31]

ECF No. 148-1 at 9. This exchange was discovered during a search of Andres Garay's phone shortly after his arrest.[32] It suggests that Irving Medina was aware that he was being asked to conduct surveillance, and that he agreed to do it.

Another exchange involving Phone-5346, dated June 8 (the date of the package deliveries), further supports this inference:

GARAY: "Lmk when you're shot to head there" – 10:11:37 am
I. MEDINA's phone no.: 5346: "I'll be there in minute" – 10:12:51 am
GARAY: "Remember to post up with good distance" – 10:13:14 am

Id. at 6.

The affidavit goes on to list other incriminating facts: Phone-5346 was registered to "Semaj Prince," who does not exist, but was later linked to Irving Medina. *Id.* at 7. CSLI from the Tower Dump Order placed Irving Medina near the alleged victim's home on May 28 and May 29 when the Defendants were alleged to have been conducting surveillance and showed multiple calls with Edgar Medina

---

[31] 21-sw-438 gives two dates for this exchange, May 28 and June 28, 2021. No one has challenged his discrepancy, and the Court assumes it is a typo.

[32] The suppression of the Five Phones Warrant does not preclude the Government's use of these messages against Irving Medina, because he does not have a reasonable expectation of privacy in Andres Garay's phone. *United States v. McDowell*, 918 F.2d 1004, 1007 (1st Cir. 1990).

during this period. *Id.* at 12-13. The warrant also pointed to numerous calls between Edgar Medina, Andres Garay, and Irving Medina before and after the kidnapping. *Id.* at 7. The affidavit notes that Irving Medina has a criminal history and was being held on an outstanding warrant. *Id.* at 7-8. While in jail, he allegedly asked his girlfriend to keep his two cell phones "safe." *Id.* at 8.

Under *Roman*, a warrant to search a home must provide "specific observations" linking criminal activity to the residence and must allege some connection beyond the fact that the Defendant is a known drug dealer. 942 F.3d at 51-52. Here, the text messages, paired with other evidence, suggest that Irving Medina was an accomplice and that he used these phones to arrange surveillance prior to the kidnapping of the USPS employee and during the package deliveries. Even without deference to the magistrate, the warrant provides a substantial basis to believe that he knowingly participated in these crimes. *Gates*, 462 U.S. at 236.

As far as nexus to the home, real-time CSLI placed both phones at 75 Moore Street, which was identified as Irving Medina's address. ECF No. 148-1 at 10-12. It was thus highly likely that the phones would be recovered from the house. *See United States v. Corleto*, No. 19-cr-76-1-PB, 2020 WL 406357, at *8 (D.N.H. Jan. 23, 2020) (finding that probable cause to search a home existed where a "chain" connected a user account to an IP address, and the IP address to a residence), *aff'd*, 56 F.4th 169 (1st Cir. 2022). There was no need for the Government to further show that drug dealing was taking place in the home.

For this reason, the Court DENIES Irving Medina's Motion to Suppress evidence from the search of his home and person. ECF No. 131.

3. Alijah Parsons

Alijah Parsons makes a similar argument, challenging 21-sw-321-PAS and 21-sw-322-PAS. ECF No. 135 (search of home and person). Here, the warrants alleged that Alijah Parsons used a cell phone to book a plane ticket to Puerto Rico, where she mailed packages containing cocaine to the United States and texted with Edgar Medina to arrange their pickup in Rhode Island. *See, e.g.*, ECF No. 155 at 4-7. The Government points to text messages with Edgar Medina's phone and real-time-CSLI that placed the relevant phones at her home. *Id.* at 7-8. The warrant authorized a forensic search of three cell phones in her possession, as well as the seizure of handwriting samples, weapons, drugs, currency, financial records, travel documents, and other evidence. *Id.* at 19-26.

Ms. Parsons' argument proceeds on slightly different grounds. She argues that there is no "nexus" to her home or to the phones in question. ECF No. 135 at 6 ("the Government conducted no surveillance . . . no statement of any activity at her home . . . [n]o hallmarks of a stash house"). She raises an incorporation challenge, arguing that the complaint affidavit was missing and that the affidavit showing probable cause was not attached to the warrant. *Id.* at 14-18; ECF No. 182 at 3-4. Finally, she argues that these warrants were overbroad and not particularized under the Fourth Amendment. ECF No. 135 at 18-20.

a. Probable Cause

As above, the affidavit must show probable cause to believe that (1) a crime has been committed, and (2) enumerated evidence of the offense will be found at the place searched. *Lindsey*, 3 F.4th at 39 (citation omitted). Both requirements are met here.

The underlying affidavit establishes probable cause of the commission of a crime by reciting basic facts about the kidnapping (thus obviating the need to attach these in a separate affidavit). ECF No. 155 at 4-5. As far as nexus goes, the affidavit notes that Ms. Parsons contacted USPS on three phones—Phone-5364, Phone-4884, and Phone-5289—to ask about Edgar Medina's wallet after he was arrested. *Id.* at 5. Phone-5289 was linked to a trip that Ms. Parsons had taken to Puerto Rico.[33] *Id.* at 5-6. USPIS subsequently obtained video surveillance from this trip showing Ms. Parsons mailing packages with fraudulent return addresses that were later found to contain cocaine. *Id.* at 6. The affidavit pointed to text messages between Alijah Parsons and Edgar Medina involving package deliveries and USPS receipts. *Id.* at 5-7. Real-time CSLI showed that all three phones—including the phone that Ms. Parsons used to arrange her trip to Puerto Rico—were located at her home. *Id.* at 7-8.

This clears the standard set by *United States v. Roman*. 942 F.3d at 51-52 (where the court required "specific observations" linking purported drug activity to

---

[33] The warrant application incorrectly listed this as Phone-5364. *See* ECF No. 155 at 6; ECF No. 177-4 at 65-69. The Government acknowledged the error, and it does not change the Court's analysis. ECF No. 175 at 7-8 n.13.

a home to justify a search of the residence). In addition to the text messages, the affidavit shows that (1) Ms. Parsons used a phone to arrange her trip to Puerto Rico; (2) where she was observed mailing packages later found to contain cocaine; and (3) the phone was later identified as being at her home. ECF No. 155 at 5-8.

Probable cause does not "demand proof beyond a reasonable doubt," but only enough to "support a fair probability" that a crime was committed, and that evidence is likely to be found in the place to be searched. *United States v. Coombs*, 857 F.3d 439, 446 (1st Cir. 2017) (citations omitted). These warrants meet the probable cause standard.

b. Incorporation

Nor is incorporation fatal to these warrants. *Sheehan* holds that a warrant is invalid where an affidavit fails to show probable cause and relies on an underlying affidavit that is neither incorporated nor attached. 70 F.4th at 50-51. *Sheehan* borrows the standard for incorporation from an earlier line of cases that deal with particularity in the execution of a warrant. *See, e.g.*, *Groh*, 540 U.S. at 557-58; *Klein*, 565 F.2d at 186 n.3. In *Groh*, the Supreme Court emphasized that the Fourth Amendment requires particularity in the executed warrant. 540 U.S. at 563 (striking down a warrant that was presented to the defendant without particularly describing the items to be seized). "The fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Id.* at 557. In *Sheehan*, by contrast, the

First Circuit considered whether a Magistrate Judge can find probable cause based on an unattached, unincorporated affidavit. 70 F.4th at 50-51.

Here, the affidavit was supported by probable cause and properly reviewed by the Magistrate Judge.[34] ECF No. 155 at 4-8; ECF No. 155-1 at 4-8. Ms. Parsons was able to access the warrant application in discovery, thus allowing her to challenge these determinations. *Id.* There is also no issue with particularity because the record shows that the executed warrants—as delivered to Ms. Parsons—included a detailed list of the places to be searched and the items to be seized.[35] ECF No. 155 at 95-108; ECF No. 151-1 at 91-99. *See* Attachments A and B. Therefore, the Court finds unpersuasive Ms. Parsons' incorporation arguments.

c. Overbreadth and Particularity

Finally, the Court turns to overbreadth and particularity. 21-sw-321-PAS and 21-sw-322-PAS authorize comprehensive searches. In addition to the three cell phones, the warrants sought handwriting samples, weapons, controlled substances, drug paraphernalia, currency, financial records, "[i]tems showing unexplained wealth," documents and records indicating customers and co-conspirators (including

---

[34] As for the complaint affidavit, this was attached and was properly incorporated. *See* ECF No. 155 at 5, 29-46. The Government does not use the words "I hereby incorporate," but does expressly direct the reader's attention to the affidavit. *Sheehan*, 70 F.4th at 50. And even if there was an incorporation error, the primary affidavit shows probable cause as to Ms. Parsons' involvement.

[35] The Court notes that as to 21-sw-322-PAS, Attachments A and B are not included with the Government's exhibit list (*see* ECF No. 177-2 at 98-99) but a full review of the record shows that it was presented to her on execution. *See* 21-sw-322, ECF No. 5.

emails, text messages, photos, and videos stored on digital devices), travel documents, call log information, and more. *See, e.g.*, ECF No. 155 at 19-23.

The Court acknowledges that these are broad searches. But in the First Circuit, "[t]he remedy in the case of a seizure that casts its net too broadly is . . . not blanket suppression but partial suppression." *Aboshady*, 951 F.3d at 9 (citation omitted). Because Ms. Parsons has not identified any specific evidence she wishes to suppress, there is no need to review the issue at this time. *Id.* If she wishes to bring such a motion in future, the Court will consider it at that time.

For these reasons, the Court DENIES Ms. Parsons' Motion to Suppress evidence found during the search of her home and person. ECF No. 135.

4. Edgar Medina

Edgar Medina asks us to reconsider his Motion to Suppress evidence obtained in the search of his home, person, and automobile. ECF No. 129 (challenging 21-sw-263-PAS, 21-sw-264-PAS, and 21-sw-265-PAS). The Court denied this motion, noting that the affidavit established "a fair probability (perhaps even overwhelming likelihood)" that evidence of drug dealing or kidnapping would be found in these places. *See* text order from August 22, 2023. Mr. Medina asks us to reconsider. ECF No. 238. The Government objects. ECF No. 243.

Mr. Medina argues that the affidavit fails to establish probable cause. ECF No. 238 at 2 ("[a]ffiant does not make a substantial showing . . . that Mr. Medina was selling drugs; possessing drugs; mailing drugs or receiving drugs" such that searches of his home, person, and vehicle were justified). He argues that the

evidence is speculative, that the affidavit is "strictly based on assumptions," and that knowledge of drug dealing, paired with the officer's training and experience, is not enough to justify a search of a home. *Id.* at 2-3. "The evidence needed to establish probable cause is more than a mere suspicion [or] rumor." *Id.* (citing *United States v. Han*, 74 F.3d 537, 541 (4th Cir. 1996)).

Mr. Medina correctly notes that courts have "rejected a per se rule automatically permitting the search of a defendant's home when he has engaged in drug activity." *Roman*, 942 F.3d at 51. But this is not a case in which Mr. Medina is alleged to be involved in drug trafficking, generally. Nor is it a case in which the warrant relies solely on the officer's "training and experience." *Ribeiro*, 397 F.3d at 52. The affidavit states that a parcel addressed to "Mr. Medina 262 George Waterman Rd Johnston, RI 02919" tested positive for cocaine, and that other parcels were mailed to the same address. ECF No. 151 at 10, 12-14. It states that Mr. Medina's car—which matched the description of the vehicle used for the kidnapping—was parked at this address, and it provides evidence to show that he lived at this address. *Id.* at 10. The affidavit states that "[d]rug traffickers often keep drugs in places where they have ready access and control, such as at their residence," but this was hardly the only piece of evidence (and certainly not the most persuasive). *Id.* at 15.

Probable cause is not a high bar, and the Government has easily cleared it. *United States v. Adams*, 971 F.3d 22, 32 (1st Cir. 2020). For this reason, the Court

DENIES Edgar Medina's renewed Motion to Suppress evidence from the search of his home, car, and person. ECF No. 238.

D. Historical CSLI

Following the home searches for Alijah Parsons and Irving Medina, the Government issued a series of warrants for historical CSLI, seeking to reconstruct Defendants' location data for various periods of time from May to June 2021. Irving Medina, Alijah Parsons, and Andres Garay have raised individual challenges to the acquisition of their historical CSLI. ECF Nos. 138, 149, 136, 137, and 215. All these searches lasted for more than seven days, and the Government obtained warrants for all of them, as required under *Carpenter*. 138 S. Ct. at 2217. The sole issue is whether these warrants are valid.

The Court addresses each of these challenges in turn.

1. Irving Medina

Irving Medina challenges two warrants for historical CSLI for Phone-5346, which sought retrospective location data for fifteen days and thirty-eight days, respectively. ECF Nos. 138, 149. The warrants in question—21-sw-554-PAS and 21-sw-428-LDA—were properly issued under *Carpenter*. Irving Medina argues that these warrants were not supported by probable cause and that the evidence linking him to criminal activity is speculative at best. ECF No. 149 at 4-5.

The affidavit for 21-sw-428-LDA states that a USPS employee was abducted at gunpoint, and that Edgar Medina, Andres Garay, and Ronald Hall were subsequently arrested in connection with the kidnapping. ECF No. 150 at 34. It

notes that Andres Garay had been corresponding with Phone-5346 by text since 2020, and that these texts were "mostly just general conversations," except for the following exchange on June 8, 2021 (the date of the package deliveries):

> GARAY: "Lmk when you're shot to head there" – 10:11:37 am
> SUBJECT PHONE: "I'll be there in a minute" – 10:12:51 am
> GARAY: "Remember to post up with good distance" – 10:13:14 am

Id. at 34-35. The affidavit states that Garay was present at 102 Congress Ave at approximately 10 a.m. but includes no information as to whether the user was present. *Id.* The affidavit goes on to note that Phone-5346 was registered to "Semaj Prince" (a false name) and later identified as belonging to Irving Medina, who had a criminal history and had called Andres Garay and Edgar Medina numerous times during the relevant period. *Id.* at 35-36. It states that Irving Medina was being held on a different charge, and that he had asked his girlfriend to keep his phones "safe."[36] *Id.* at 36.

Reasonable minds can differ as to whether receiving and acknowledging this text message suggests that Irving Medina agreed to conduct surveillance. But where reasonable minds can differ, the Court is required to give deference to the magistrate. *United States v. Barnard*, 299 F.3d 90, 93 (1st Cir. 2002) ("In a doubtful or marginal case, the court defers to the issuing magistrate's determination of probable cause"). As to "commission," there was probable cause to believe that a crime was committed because the application laid out the bare facts

[36] 21-sw-428-LDA sought location data for fifteen days. 21-sw-554-PAS properly incorporated the affidavit from 21-sw-428-LDA as to probable cause but expanded the time frame to thirty-eight days. ECF No. 150-1 at 6-7.

of the kidnapping and linked these facts to the phone in question. *Lindsey*, 3 F.4th at 39. As to "nexus," a search of historical CSLI was likely to reveal the identity of the user, and his location. *Id.*

Probable cause does not require "proof beyond a reasonable doubt [or even] preponderance of the evidence." *Gates*, 462 U.S. at 235. "[O]nly the probability, and not a prima facie showing, of criminal activity is the standard of probable cause." *Id.* (citation omitted). The Government has established that here.

As such, the Court DENIES Irving Medina's Motion to Suppress CSLI from Phone-5346. ECF No. 138.

2. Alijah Parsons

Ms. Parsons challenges the Government's efforts to acquire her location data in two instances—first, in her Motion to Suppress evidence from the geofence warrants (ECF No. 136), and second, in her Motion to Suppress evidence from the Tower Dump Order (ECF No. 137).[37] She also challenges the Government's search of historical CSLI in her reply brief for the Tower Dump Order. ECF No. 186 at 7.

These motions are broadly written and incorporate "any unspecified warrant as to Google" and "any other process, order, or warrant accomplishing essentially a tower dump not specified herein." ECF No. 136 at 2, n.1; ECF No. 137 at 1, n.11. The Government obtained four warrants for historical CSLI for relevant phone

[37] Ms. Parsons acknowledged that these challenges are now moot but reserved her right to challenge historical CSLI. ECF No. 241 at 3 ("Defendant Parsons reserves any part of the foregoing motions addressing the separate search and seizure of her individual cellphone accounts historical CSLI data which she continues to challenge.").

numbers associated with Alijah Parsons. ECF No. 175 at 9 (citing 21-sw-526-LDA, 21-sw-255-PAS, 22-sw-197-PAS, and 22-sw-210-PAS). As noted above, a Tower Dump Order is distinct from a search for historical CSLI; they seek different types of information, and thus cannot be attacked on the same grounds. *Supra* Part A. Likewise, the overbreadth arguments for historical CSLI are not analogous to those involving forensic phone searches and cannot be raised here. *Supra* Part C.

Even if the Court assumed that the Motions to Suppress geofence and tower dump records encompassed historical CSLI for a specific user, Ms. Parsons would still need to show that the warrants lacked probable cause. She would have a hard time doing so based on the affidavits in question. The warrant applications for 21-sw-526-LDA and 21-sw-255-PAS state that Ms. Parsons used one of these phones to book a trip to Puerto Rico with Spirit Airlines where she was later seen mailing fraudulently addressed packages found to contain cocaine. *See* ECF No. 177-1 at 9-69 (21-sw-255-PAS); ECF No. 177-2 at 198-218 (21-sw-526-LDA). These affidavits include a host of new, highly incriminating details, such as deleted photos recovered from her phone showing USPS employees at work and receipts for the target packages. *Id.*

Affidavits supporting 22-sw-197-PAS and 22-sw-210-PAS are more ambiguous, pointing to incriminating text messages and phone calls made to alleged co-conspirators. ECF No. 177-2 at 289-305 (22-sw-197-PAS); ECF No. 177-4 at 2-20 (22-sw-210-PAS). But these warrants are not before the Court, and Ms. Parsons has not independently briefed these in her Motions to Suppress.

For these reasons, the Court takes no position on Ms. Parsons' challenge to historical CSLI at this time.

3. Andres Garay

Andres Garay challenges the search of historical CSLI for Phone-9050 on the grounds that the supporting affidavits were not properly incorporated. ECF No. 215. His argument is similar to the objection to the Five Phones Warrant: the affidavits were not attached, so the warrant lacks probable cause. ECF No. 134.

Mr. Garay notes that the instant search warrant (22-sw-177-LDA) relied on the affidavit from an underlying warrant (21-sw-552-PAS), which in turn relied on an affidavit from an underlying warrant (21-sw-498-LDA), which supplied probable cause for all three. Each affidavit was expressly incorporated, but the affidavit for 21-sw-498-LDA was not attached to the final warrant.[38] ECF No. 215-1 at 2-3. 22-sw-177-LDA recites the foregoing travel and states: "I thus submit this affidavit with updated IMSI and further ESN information and hereby incorporate by reference the entire affidavit I previously submitted in support of that search warrant to establish probable cause. *See* Exhibit 1." ECF No. 215-2 at 42 (attaching and incorporating the intermediary affidavit, but not the original).

The Government argues that this error should be disregarded because unlike the Five Phones Warrant, the previous warrants—21-sw-498-LDA and 21-sw-552-PAS—were valid. ECF No. 231 at 1. They argue that the second warrant was

[38] 21-sw-498-LDA includes an account of text messages recovered from Andres Garay's cell phone following the initial arrest. It was reissued multiple times to correct errors and because AT&T failed to produce the requested data.

reissued to correct a typographical error, and thus good faith should apply. *Id.* at 5-7. Alternatively, the Government argues that all three should be treated as a single warrant. *Id.* at 6 ("[I]t is a mistake to view Warrants 498, 552 and 177 as three separate warrants . . . Warrants 552 and 177 are more appropriately viewed as under-oath corrections to Warrant 498."). Finally, they argue that there is no evidence of a systemic problem and good faith should rule the day. *Id.* at 8-11.

It is generally true, as the Government argues, that minor clerical errors do not invalidate a warrant. *See, e.g., United States v. McMillian*, 786 F.3d 630. 640 (7th Cir. 2015) (incorrect street number did not invalidate a warrant where there was no chance another location could be searched by mistake). But Mr. Garay is not arguing that the affidavit included a factual error: he is pointing out that it was not included at all. Without the affidavit, 22-sw-177-LDA reflects the travel of the case but does not include probable cause to support a search of his phone.[39] ECF No. 215-2 at 42. The warrant application for 22-sw-177-LDA may have been reissued to correct a typographical error—but as presented to the Magistrate Judge, it was devoid of probable cause.

This matter is resolved by *Sheehan*, which instructs that where an underlying affidavit is the sole source of probable cause, it must be expressly incorporated *and* attached. 70 F.4th at 50. The Court acknowledges that here, unlike the Five Phones Warrant, there may have been a valid underlying warrant further back in the chain. But 22-sw-177-LDA was the warrant that was approved,

[39] The intermediary affidavit notes that Mr. Garay was indicted but includes no other information and relies on the original affidavit to supply these facts.

executed, and ultimately used to obtain Mr. Garay's historical CSLI, and it did not include the relevant affidavit. *Id.* at 47 ("[a]n affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause.") (citing *Gates*, 462 U.S. at 239). The good-faith exception does not apply where a warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* at 51 (citing *Leon*, 468 U.S. at 923).

As noted above, the Government acknowledged that there were four other warrant applications that cited an exhibit that was not attached, suggesting that the omission was not a "one-off." ECF No. 183-1 at 2; *Herring*, 555 U.S. at 147-48 (distinguishing simple negligence from "systemic error or reckless disregard of constitutional requirements."). This warrant was not on the list and was only later found to be missing an affidavit. ECF No. 183-1 at 2. The fact that the Government made the same error multiple times—and then was unable to quickly locate all instances of the error—gives the Court pause in blessing a warrant that was devoid of probable cause.

Sheehan tells us that it is "objectively unreasonable" to submit a single warrant application that is wholly lacking in probable cause, let alone two or more. 70 F.4th at 54-55. It does not matter that the magistrate failed to catch the error: it was unreasonable for law enforcement to rely on it, and it was their responsibility to ensure that it was properly filed. *Id.* at 51 ("[A]n officer's reliance on a magistrate's approval of a facially deficient warrant is especially unreasonable

when those 'deficiencies arise from the failure of the [officer] conducting the search to provide the required supporting information.'") (citation omitted).

As Mr. Garay notes, proper data management is an essential law enforcement function, as "[t]here are few criminal cases in the modern age that do not involve some form of electronic information either as actual evidence or in the documentation of the investigation." ECF No. 215-1 at 7. The Court agrees, and thus finds that the benefits of suppression outweigh the costs. *Herring*, 555 U.S. at 147 ("[T]he deterrent effect of suppression must be substantial and outweigh any harm to the justice system."). By excluding the evidence, the Court hopes to encourage better practices that meet the constitutional standard going forward.

For these reasons, the Court GRANTS Mr. Garay's Motion to Suppress CSLI from Phone-9050. ECF No. 215.

IV. CONCLUSION

For the reasons above, the Court GRANTS Defendants' Motion to Suppress evidence from the Five Phones Warrant. ECF No. 134. The Court GRANTS Andres Garay's Motion to Suppress historical CSLI from Phone-9050. ECF No. 215.

The Court DENIES Defendants' Motions to Suppress the Tower Dump Order under the good-faith exception (ECF Nos. 137, 242, 245, and 247). The Court finds that all remaining challenged warrants are supported by probable cause and thus DENIES Alijah Parsons' Motion to Suppress a search of her home and person (ECF No. 135), Irving Medina's Motions to Suppress the search of his home, person, and

historical CSLI (ECF Nos. 131 and 138), and Edgar Medina's Motion for Reconsideration (ECF No. 238).

IT IS SO ORDERED.

John J. McConnell, Jr.
United States District Chief Judge

January 23, 2024