[J-2-2021]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT

BAER, C.J., SAYLOR, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

COMMONWEALTH OF PENNSYLVANIA,	:	No. 42 MAP 2020
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court at No. 151 EDA 2018
	:	dated January 24, 2020 Affirming
v.	:	the Judgment of Sentence of the
	:	Montgomery County Court of
	:	Common Pleas, Criminal Division, at
DAVID PACHECO,	:	No. CP-46-CR-0002243-2016 dated
	:	November 29, 2017
Appellant	:	
	:	ARGUED: March 9, 2021

OPINION

CHIEF JUSTICE BAER **DECIDED: November 17, 2021**

We granted allowance of appeal to determine whether trial court orders that authorized the disclosure of Appellant David Pacheco's real-time cell site location information ("CSLI") were the functional equivalent of search warrants and satisfied the requisites of the Fourth Amendment pursuant to the United States Supreme Court's decision in *United States v. Carpenter*, 138 S.Ct. 2206 (2018). For the reasons set forth herein, we hold that the challenged orders were the functional equivalent of search warrants and complied with the Fourth Amendment. Accordingly, we affirm the judgment of the Superior Court, which affirmed Appellant's judgment of sentence.

I. Background Summary

The record establishes that in 2015, the Narcotics Enforcement Team of the Montgomery County District Attorney's Office ("Commonwealth"), working with the

Federal Drug Enforcement Agency ("DEA"), learned that a large Mexican drug-trafficking organization was smuggling heroin into the United States for distribution, and that Appellant, a resident of Norristown, Pennsylvania, played a significant role in the operation by retrieving the heroin in Atlanta, Georgia, and transporting it to wholesale buyers in New York City.

At various times throughout the nearly year-long investigation, the Commonwealth applied for and obtained several orders pursuant to the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("Wiretap Act"), 18 Pa.C.S. §§ 5701-82. The orders at issue in this appeal are those entered pursuant to Subchapter E of the Wiretap Act ("Pen Registers, Trap and Trace Devices, and Telecommunication Identification Interception Devices"), 18 Pa.C.S. §§ 5771-75.[1] A brief discussion of the statute is helpful to facilitate an understanding of the case.

Relevant here, Section 5772 sets forth the requirements for an application requesting an order authorizing the disclosure of mobile communications tracking information.[2] This section permits the Attorney General or a district attorney to make an application for mobile communications tracking information to either a court of common pleas having jurisdiction over the offense under investigation or to a Superior Court judge

[1] This appeal involves a request for production and disclosure of mobile communications tracking information and does not involve a pen register, trap and trace device, or a telecommunication identification interception device. While not referenced in the title of Subchapter E, this subchapter also governs requests for mobile communications tracking information.

[2] "Mobile communications tracking information" is defined as "[i]nformation generated by a communication common carrier or a communication service which indicates the location of an electronic device supported by the communication common carrier or communication service." 18 Pa.C.S. § 5702. Law enforcement will frequently refer to mobile communications tracking information as a "ping."

when an application for an order has already been made for the targeted phone in that court. 18 Pa.C.S. § 5772(a).

Notably, Section 5772 requires that the application include: (1) the identity of both the attorney making the application and the investigative agency conducting the investigation; (2) the applicant's certification that "the information likely to be obtained is relevant to an ongoing criminal investigation conducted by that agency;" and (3) an affidavit by an investigative or law enforcement officer "which establishes probable cause for the issuance of an order under section 5773." *Id.* at § 5772(b).

Section 5773 addresses the issuance of an order thereunder and provides, in relevant part, that upon application under Section 5772, the court shall enter an *ex parte* order authorizing the disclosure of mobile communications tracking information "if the court finds that there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained by such installation and use on the targeted telephone." 18 Pa.C.S. § 5773(a).

The statute further directs that an order issued under that section shall specify:

> (i) That there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted telephone.
>
> (ii) The identity, if known, of the person to whom is leased or in whose name is listed the targeted telephone, or, in the case of the use of a telecommunication identification interception device, the identity, if known, of the person or persons using the targeted telephone.
>
> (iii) The identity, if known, of the person who is the subject of the criminal investigation.
>
> (iv) In the use of pen registers and trap and trace devices only, the physical location of the targeted telephone.

> (v) A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device or the telecommunication identification interception device relates.

18 Pa.C.S. § 5773(b)(1).

Additionally, Section 5773 sets forth a maximum 60-day limit on orders entered under that provision, with extensions permissible upon satisfaction of the criteria for obtaining an initial order. *Id.* at § 5773(c). Finally, Section 5773 provides that orders entered under that provision shall be sealed unless otherwise ordered by the court. *Id.* at § 5773(d).

Consistent with these statutory provisions, on or about August 28, 2015,[3] the Commonwealth filed in the Montgomery County Court of Common Pleas ("trial court") an application and affidavit along with a proposed order pursuant to Section 5772, seeking, *inter alia*, the disclosure of mobile communications tracking information relating to a specific telephone number. The application averred that members of the Pennsylvania State Police, the Commonwealth, and the DEA were investigating heroin trafficking in Montgomery County and they believed that Appellant was an integral part of the heroin distribution organization. Application of Montgomery County Assistant District Attorney Kelly Lloyd, DA-166-2015, at 0-1.[4] The Commonwealth asserted that Appellant utilized the mobile cellular telephone bearing the number enumerated in the application, and that it had become necessary to track or otherwise maintain the physical location of the cell phone. *Id.* at 1.

[3] While the application is not dated, the accompanying affidavit of probable cause is dated August 28, 2015.

[4] For unexplained reasons, the first page of the application is numbered as "0," and the second page is numbered as "1."

The application further stated that Montgomery County Detective Michael J. Reynolds had prepared an attached affidavit setting forth specific and articulable facts that established probable cause to believe that information relevant to an ongoing criminal investigation would be obtained from the enumerated cell phone or on any replacement telephone number billed to the same subscriber for the upcoming 60-day period. *Id.* at 1, ¶ 3. The application also averred that the information which would likely be obtained would relate to violations of the Crimes Code including, but not limited to, the manufacture, delivery, and/or possession with the intent to deliver a controlled substance, 35 P.S. § 780-113, criminal conspiracy, 18 Pa.C.S. § 903; and criminal use of communication facility, 18 Pa.C.S. § 7512. *Id.* at 2, ¶ 4. Additionally, the application requested the court to direct the telecommunication service providers to initiate a signal to determine the location of the subject's mobile device on the provider's network and disclose those signals as mobile communications tracking information at such intervals and times as directed by the law enforcement agent serving the order. *Id.* at 6. The application also requested that the order be without geographical limitations, so long as the results of the disclosure of mobile communications tracking information is monitored within the jurisdiction of the court. *Id.* at 7. Finally, the application requested that the order be sealed. *Id.*

Attached to the application was a 29-page affidavit of probable cause completed by Detective Reynolds.[5] Identifying Appellant as the target of the criminal investigation, the affidavit set forth Detective Reynold's experience and education in investigating drug trafficking and his beliefs regarding the use of cell phones in drug trafficking and the distribution of drugs from source countries, including Mexico. Affidavit of Probable Cause

[5] While the affidavit itself is not paginated, for ease of reference we refer to the pages in chronological order. Our count of 29 pages includes only the affidavit itself and not the attachments thereto.

of Montgomery County Detective Michael J. Reynolds, dated August 28, 2015, at 1-6. Significantly, the affidavit states that the facts alleged establish probable cause to believe that Appellant, and others known and as of yet unknown, are committing and will continue to commit offenses including, but not limited to, manufacture, delivery, and/or possession with the intent to deliver a controlled substance, 35 P.S. § 780-113, criminal conspiracy, 18 Pa.C.S. 903, dealing in proceeds of unlawful activities, 18 Pa.C.S. § 5111, and criminal use of communication facility, 18 Pa.C.S. § 7512. *Id.* at 4.

The affidavit bases its assertion of probable cause on various sources, including information provided by other investigators and law enforcement agencies, as well as three separate confidential informants who had participated in previous drug-trafficking investigations that led to the arrest of two individuals. *Id.* at 6-25. These confidential informants had personal knowledge that Appellant played a pivotal role in the Mexican drug cartel's activities under investigation.

The trial court issued orders on August 28, 2015, authorizing the requested forms of electronic surveillance pursuant to Section 5773 of the Wiretap Act.[6] Based upon the aforementioned application and affidavit, the court, in issuing the orders, found probable cause to believe that information relevant to an ongoing criminal investigation would be recovered by authorizing investigators to obtain data relating to the physical location of a cell phone, identified by an enumerated phone number, or any replacement telephone

[6] The orders issued on August 28, 2015, were docketed at DA-165-2015, DA-165(A)-2015, DA-166-2015, and DA-227-2015, which subsequently were introduced into evidence at the Suppression Hearing as Commonwealth Exhibits 1 through 4, respectively. *See* N.T., Suppression Hearing, 4/10/2017, at 73-76. Each order reflected a different phone number sought to be surveilled, with the exception of DA-165(A)-2015, which was merely an extension of DA-165-2015. Thus, the three phone numbers to be surveilled each had a separate application, affidavit of probable cause, and order. The language of the orders were the same, save for the target telephone phone number specified.

number billed to the same subscriber, believed to be Appellant. Trial Court Order, DA-165-1015, 8/28/2015, at ¶ 1.[7]

The orders identified Appellant by name as the subject of the investigation and the source of the heroin, and stated that the information likely to be obtained by the electronic surveillance would relate to the particular criminal offenses enumerated in the application. *Id.* at ¶ 3-4. The orders specifically authorized Appellant's telecommunications service providers to send signals, otherwise known as "pings," to Appellant's cell phone at intervals and times as directed by law enforcement, which signals generate real-time CSLI, and then disclose to investigators Appellant's whereabouts.[8] Trial Court Order, 8/28/2015, at ¶ 9. The orders further clarified that their directives shall be without geographical limitations as long as the results of the disclosures are monitored within the jurisdiction of the court. *Id.* at 12.

On October 15, 2015, the trial court issued a nearly identical order permitting usage of the various electronic surveillance and tracking methods of the same telephone number believed to be utilized by Appellant for an additional 60 days, for a total tracking

---

[7] No information was disclosed to detectives regarding any replacement telephone number billed to the same subscriber or determined to be used by the same suspect; the only information disclosed pertained to the target telephone numbers specified on the orders. Trial Court Suppression Order, 5/4/2017, at ¶¶ 17, 18.

[8] The Superior Court has explained that a "ping" determines "the real time location of [a] cell phone by looking at the cell signal between the phone and the closest cell tower and finding the last known address where the cell phone transmitted a signal requesting service." *Commonwealth v. Rushing*, 71 A.3d 939, 946 (Pa. Super. 2013), *rev'd on other grounds*, 99 A.3d 416 (Pa. 2014). To elaborate, real-time CSLI is actively obtained via the wireless service provider sending a command signal to the targeted cell phone, which activates the phone's location subsystem to determine the location of the phone. The cell phone then transmits its location back to the wireless provider who, in turn, discloses the information to law enforcement. The location information generated is generally accurate within less than 30 meters. This case does not involve historical CSLI, discussed *infra*.

period of 120 days to investigate the same enumerated violations of the Crimes Code set forth in the Commonwealth's application and affidavit of probable cause.

While not challenged in this appeal, on December 11, 2015, and January 6, 2016, the Commonwealth sought and obtained orders from the Superior Court pursuant to Subchapter B of the Wiretap Act ("Wire, Electronic, or Oral Communication"), authorizing the interception of oral, electronic, and wire communications for the cell phone registered to Appellant, as well as three other cell phones believed to be used by him. Upon examination of the information received as a result of the various orders entered, the Commonwealth was able to identify nine occasions between September of 2015 and January of 2016, when Appellant travelled from Norristown to Atlanta and New York as a member of the Mexican drug trafficking organization. During each excursion, Appellant obtained a retrofitted car battery containing three kilograms of heroin in Atlanta, returned to Norristown, and then transported the drugs to New York, using his cell phone to facilitate the transactions.

By surveilling intercepted phone conversations, detectives learned that Appellant planned to return to Norristown from Georgia on January 10, 2016, driving with the retrofitted car battery containing the drugs. Police apprehended Appellant at that time and seized from the car battery three kilograms of heroin, which was the equivalent of approximately 100,000 singe-dose bags. Appellant was arrested and charged with nine counts each of possession with intent to deliver and criminal use of a communications facility, two counts of dealing in unlawful proceeds, and one count each of conspiracy to commit possession with intent to deliver and corrupt organizations.

On May 27, 2016, Appellant filed a motion to suppress raising several issues, including a challenge to the real-time CSLI collected by investigators. Relevant here, in a supplement to the motion to suppress filed on November 18, 2016, Appellant contended

that the Commonwealth failed to "seek a search warrant from the [c]ourt to legally utilize 'Mobile Tracking Technology' . . . or similar technology . . . as . . . is required and necessary under Article I, Section 8 of the Pennsylvania Constitution and the Fourth Amendment of the United States Constitution." Supplement to Motion to Suppress, 11/18/2016, at ¶ 5. Appellant maintained that the use of mobile tracking technology constitutes a "search" for constitutional purposes that is unreasonable, as general searches are constitutionally prohibited absent a warrant based upon probable cause. *Id.* at ¶ 6. Concluding that the orders authorizing the real-time CSLI failed to satisfy the probable cause standard, Appellant posited that the evidence obtained pursuant to those orders must be suppressed. In his supporting Memorandum of Law, Appellant alleged that the detectives tracked his real time CSLI for at least 60 days, into private residences without limitation. Memorandum of Law in Support of Supplemental Motion to Suppress Evidence, 3/16/2017, at 14.

Following a hearing on April 10, 2017, the trial court denied Appellant's motion to suppress. In its opinion in support thereof, the trial court held, *inter alia*, that under a totality of the circumstances test and based on the four corners of the affidavit of probable cause, the court orders for mobile communication tracking information are supported by probable cause. Trial Court Suppression Opinion, 5/4/2017, at ¶ 12. The court explained that probable cause existed from the combined information of the three confidential informants, the cellular analysis of electronic devices that corroborated at least one of the confidential informant's information, and the call detail records revealing that Appellant was in contact with known drug dealers in Mexico and other persons previously apprehended in a narcotics case. *Id.* at ¶ 15.

The trial court further rejected Appellant's claim that the challenged orders were unlawful general warrants because they failed to include limitations on the time and

manner of real-time location tracking. The trial court reasoned that Subchapter E of the Wiretap Act does not require limitations on the time or manner of phone location tracking. *Id.* at ¶ 11. Recognizing that the state and federal constitutions require that a warrant describe the items to be seized as specifically as reasonably possible, the court opined that this requirement was satisfied as each order in this case was particularized to a single phone number's activity and, thus, did not constitute a general warrant. *Id.* at ¶ 11.

During the jury trial, the parties stipulated that between September 13, 2015 and December 5, 2015, Appellant made seven trips from Norristown, Pennsylvania, to Atlanta, Georgia, to acquire from Marcelo Enciso approximately three kilograms of heroin concealed in a car battery. The parties further stipulated that Appellant would then deliver the car battery concealing the drugs to the Hernandez family in Bronx, New York, and return later to collect the proceeds from the drug sale. The Commonwealth presented evidence consistent with the stipulation, including multiple phone calls between Appellant and the other participants discussing coordination of the trips and the price of the drugs. The Commonwealth further presented photos taken in Atlanta depicting Enciso and Appellant exchanging car batteries outside of a gas station. Appellant testified on his own behalf, admitting that he engaged in the alleged drug transactions, but contending that he did so under duress, claiming that the Mexican drug cartels coerced him to act as a drug courier by threatening to kill members of his family if he did not cooperate.

The jury convicted Appellant of all charges, with the exception of corrupt organizations. On November 29, 2017, the trial court sentenced Appellant to an aggregate term of incarceration of 40 to 80 years, followed by 10 years of probation. Appellant timely filed a notice of appeal, raising several issues. Germane to this appeal, Appellant challenged the trial court's denial of his motion to suppress. Specifically, in his Pa.R.A.P. 1925(b) statement, he framed his issue as follows:

> Whether the trial court erred by failing to suppress all evidence derived from the warrantless real-time tracking of [his] cell phone where such evidence was obtained in violation of the Pennsylvania Wiretap Act, Article I, Section 8 of the Pennsylvania Constitution, and the Fourth and Fourteenth Amendment to the United States Constitution?

Concise Statement, 1/31/2018, at 1.

II. Trial Court Opinion

In its opinion pursuant to Pa.R.A.P. 1925(a), the trial court held that Appellant waived his challenge to the denial of suppression of CSLI information by setting forth a vague statement of matters complained of on appeal that did not disclose what evidence was obtained without a court order or warrant. Trial Court Opinion, 3/8/2018, at 7. Examining the grounds upon which Appellant sought to suppress the CSLI evidence at the suppression hearing, the court found that none of those claims encompassed the issue of whether the Commonwealth obtained and used information without obtaining a warrant. *Id.* at 8-9. Acknowledging that Appellant may be claiming that the court orders authorizing the electronic surveillance of CSLI were insufficient because warrants were required, the court concluded that Appellant could not be making such claim, as the Wiretap Act specifically requires court orders, not warrants. *Id.* at 8. The court additionally found that Appellant's remaining claims, unrelated to this appeal, lacked merit.

III. The Carpenter Decision

Approximately three months after the trial court issued its opinion and before the Superior Court adjudicated Appellant's direct appeal, the United States Supreme Court decided C*arpenter v. United States*, 138 S.Ct. 2206 (2018), which addressed "whether the Government conducts a search under the Fourth Amendment when it accesses

historical cell phone records that provide a comprehensive chronicle of the user's past movements."[9] *Id.* at 2211.

Based on suspicions that Carpenter was involved in a string of robberies, federal prosecutors sought and obtained two court orders pursuant to the Federal Stored Communications Act ("SCA"). That statute permits the government to compel the disclosure of certain telecommunications records upon a demonstration of "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The two orders, issued by federal magistrate judges pursuant to Section 2703(d) of the SCA ("D orders"), directed Carpenter's wireless service providers to disclose to prosecutors historical CSLI records for a four-month interval (127 days) coinciding with when the robberies occurred. The records revealed the location of Carpenter's cell phone whenever it made or received calls during the requested timeframe. The information received from these records placed the phone near four of the robberies. Carpenter subsequently was arrested and charged with six counts each of robbery and carrying a firearm during a federal crime of violence.

Prior to trial, Carpenter moved to suppress the historical CSLI records provided by his wireless carriers, contending that the government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The district court denied the suppression motion, and Carpenter subsequently was convicted of six counts of robbery, and five firearm offenses. On

[9] Unlike real-time CSLI, which, as noted, is obtained when the wireless service provider sends a command signal to the targeted cell phone to activate the phone's location subsystem and then provides the current location of the phone to law enforcement, historical CSLI is automatically generated and routinely collected by wireless service providers each time a cell phone connects to a cell tower.

appeal, the United States Court of Appeals for the Sixth Circuit affirmed Carpenter's judgment of sentence, finding that he lacked a reasonable expectation of privacy in the location information collected by the FBI because he had voluntarily shared that information with his wireless carriers.

The United States Supreme Court reversed. Recognizing the ever-evolving nature of digital technology, the High Court observed that historical CSLI records maintained by wireless network providers did not fit neatly under existing jurisprudence. *Id.* at 2214. The Court reasoned that requests to obtain cell phone location records implicate two lines of cases involving privacy interests. Relating to the first line of cases, which pertain to an individual's expectation of privacy in his physical location and movements, the Court contrasted its decision in *United States v. Knotts*, 460 U.S. 276 (1983), which held that law enforcement's use of a beeper to aid in tracking Knotts' car was not a search for purposes of the Fourth Amendment because a person travelling in an automobile on public streets has no expectation of privacy in his movements from one place to another, with *United States v. Jones,* 565 U.S. 400 (2012), which found that the federal agents' installation of a GPS tracking device on Jones' car to monitor continually the vehicle's movement for 28 days constituted a search under the Fourth Amendment. *Id.* at 2215. Examining the privacy interests involved, the Court concluded that collection of historical CSLI records present greater privacy concerns than the GPS monitoring of a vehicle in *Jones* because a cell phone "tracks nearly exactly the movements of its owner." *Id.* at 2218.

The second line of cases implicated by the collection of historical CSLI, the Court found, involved the long-standing principle that a person does not have a reasonable privacy interest in information he voluntarily turns over to third parties, *i.e.*, the third-party

doctrine.[10] *Id.* at 2216. Observing that CSLI conveys a "detailed and comprehensive record of the person's movements," the Court declined to extend the third-party doctrine to historical CSLI, concluding that a third party's possession of CSLI does not overcome the phone user's claim to Fourth Amendment protection. *Id.* at 2217. The Court based its conclusion on the fact that historical CSLI, while commercially generated, is not voluntarily "shared" as one understands the term, considering that cell phones are "indispensable to participation in modern society," and that "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering it up." *Id.* at 2220.

Accordingly, the High Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," and that the "location information obtained by law enforcement from Carpenter's wireless carriers was the product of a search." *Id.* at 2217. The Court emphasized that historical CSLI's "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., Concurring)). The Court characterized the location records as holding the "privacies of life," observing that individuals compulsively carry their cell phones at all the times beyond public thoroughfares and into private residences and potentially revealing venues. *Id.* at 2217-18 (citation omitted). The Court observed that the "retrospective quality of the data here gives police access to a category of information otherwise unknowable." *Id.* at 2218. Thus, the Court concluded, when the government

[10] The third-party doctrine originated in *United States v. Miller*, 425 U.S. 435, 443 (1976), where the Court held that one who revealed his affairs to another had taken the risk that the information would be conveyed by that person to the government.

obtained Carpenter's CSLI from the wireless carriers, it invaded his reasonable expectation of privacy in the whole of his physical movements. *Id.* at 2219.

Based on the foregoing, the Court held that the government must generally obtain a warrant supported by probable cause before acquiring historical CSLI records.[11] *Id.* at 2221. Addressing the D orders issued to obtain Carpenter's historical CSLI, the Court determined that those orders did not satisfy the Fourth Amendment because the federal statute only required the government to show "reasonable grounds" for believing that the "records were relevant and material to an ongoing investigation." *Id.* (citing 18 U.S.C. § 2703(d)). The Court found that this burden fell "well short of the probable cause required for a warrant," emphasizing the lack of some quantum of individualized suspicion. *Id.* Thus, the Court declared that before compelling a wireless carrier to turn over a subscriber's CSLI, the government must obtain a warrant. *Id.*

Finally, while the High Court determined that Carpenter was entitled to relief, the Court emphasized that its decision should be construed as a narrow one, stating explicitly that the decision did not extend to matters not before it, including the collection of real-time CSLI, which is at issue here. *Id.* at 2220.

IV. Appeal in Superior Court

On appeal to the Superior Court, Appellant argued, *inter alia*, that the trial court erred by holding that he waived his challenge to the denial of suppression of real-time CSLI evidence by failing to set forth the claim clearly in his Pa.R.A.P. 1925(b) statement of matters complained of on appeal. Appellant further contended that the trial court erred in denying his motion to suppress CSLI evidence where the Commonwealth illegally

[11] The Court recognized that an exception to this general rule would exist where the exigencies of the circumstances render the needs of law enforcement so compelling that a warrantless search is objectively reasonable. *Id.* at 2222.

tracked his cell phone in violation of the Pennsylvania Constitution, the Fourth Amendment, and the High Court's then-recent decision in *Carpenter*.

The Superior Court affirmed Appellant's judgment of sentence. *Commonwealth v. Pacheco*, 227 A.3d 358 (Pa. Super. 2020). Initially, the court agreed with Appellant that he preserved his challenge to the warrantless collection of CSLI evidence by presenting the issue in his motion to suppress and setting forth the issue with sufficient clarity in his Pa.R.A.P. 1925(b) statement of matters complained of on appeal. *Pacheco*, 227 A.3d at 365-66.

Regarding the merits of Appellant's suppression claim, the Superior Court observed *Carpenter's* holding that the acquisition of historical CSLI evidence constituted a search for constitutional purposes, and that the government must generally obtain a warrant supported by probable cause before acquiring such records. *Id.* at 368. The court further observed *Carpenter's* holding that the "D orders" were insufficient because the governing statute only required prosecutors to demonstrate reasonable grounds for believing that the records were relevant and material to an ongoing investigation, which fell short of the probable cause standard required for a warrant. *Id.* at 368-69.

Finding "no meaningful distinction between the privacy issues related to historical and real-time CSLI," the Superior Court extended *Carpenter's* rationale to real-time CSLI tracking, and held that Appellant has a legitimate expectation of privacy in the real-time record of his physical movements. *Id.* The court concluded that when prosecutors sought and obtained real-time information about Appellant's location, they conducted a "search" under the state and federal charters. *Id.*

The Superior Court next examined whether the orders authorizing disclosure of the CSLI satisfied the warrant requirements of the Fourth Amendment.[12] The court relied upon *Dalia v. United States*, 441 U.S. 238 (1979), for the proposition that orders issued under the federal Wiretap Act constituted warrants under the Fourth Amendment if three requisites were satisfied: (1) the orders must be issued by neutral, disinterested magistrates; (2) those seeking the orders must demonstrate probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction" for a particular offense; and (3) the orders must particularly describe the items to be seized and the place to be searched. *Pacheco*, 227 A.3d at 371 (citing *Dalia*, 441 U.S. at 255).

The Superior Court concluded that the orders issued here pursuant to Subchapter E of Pennsylvania's Wiretap Act satisfied the requisites set forth by the High Court in *Dalia* because: (1) the orders were issued by a neutral, disinterested common pleas court judge who was authorized to issue the orders under Sections 5772(a) and 5773 of the Wiretap Act; (2) the orders specifically stated that there was probable cause that the information sought would aid in the apprehension of Appellant for the particular offenses including, but not limited to, the manufacture, delivery and/or possession with intent to deliver a controlled substance, criminal conspiracy, and criminal use of a communication facility; and (3) the orders described the place to be searched (Appellant's cell phone) and the items to be seized (the real-time CSLI for that phone). *Id.* at 372. Accordingly, the court ruled that the orders were the equivalent of a warrant obtained pursuant to the Fourth Amendment, and thus, the search in this case was legal. *Id.*

---

[12] The Superior Court found that Appellant did not set forth a separate analysis pursuant to *Commonwealth v. Edmunds*, 586 A.2d 887, 895 (Pa. 1991), regarding whether the Pennsylvania Constitution provided him with greater protection than the federal constitution; thus, it presumed that Appellant is entitled to the same protection under both the federal and state charters, and examined his claim solely pursuant to Fourth Amendment jurisprudence. *Pacheco*, 227 A.3d at 366 n.8.

The Superior Court emphasized that the orders were obtained pursuant to lengthy affidavits of probable cause, extensively detailing the criminal investigation into Appellant's role in the Mexican cartel's illegal activities at issue, which were attested to by the personal observation of the affiant, information provided by other law enforcement agencies, several confidential informants, and information from other electronic and physical surveillance. *Id.* When read in their entirety, the Superior Court held, the orders "indicate that the [trial] court found *probable cause* that the information obtained would lead to evidence that [Appellant] was violating specific provisions of the [C]rimes [C]ode and would enable law enforcement to track and locate him through his cell phone." *Id.* at 372-373.

The Superior Court reasoned that the orders were substantially different from the "D orders" issued in *Carpenter*, which were based merely on "*reasonable grounds*" to believe that the records sought were relevant and material to an ongoing criminal investigation. *Id.* at 373 (citing 18 U.S.C. § 2703(d)). The court emphasized that "[u]nlike the Pennsylvania Wiretap Act, the federal statute did not require, and the government did not provide, an affidavit of probable cause individualized to Carpenter and his suspected crimes for the issuance of the 'D orders.'" *Id.* at 373.

V. Allowance of Appeal in this Court

This Court subsequently granted Appellant's petition for allowance of appeal to address the following issues:

> (1) Whether the Superior Court Panel erred in finding that an Order by a Court of Common Pleas permitting the Commonwealth to search 108 days of real time cell site location information was the equivalent of a search warrant, as required by *United States v. Carpenter*, 138 S.Ct. 2206, 201 L. Ed. 2d 507 (2018)? Furthermore, did the Order of the Court of Common Pleas permit the Commonwealth to track Petitioner's cell phone(s) in violation of the Pennsylvania Constitution, the Fourth Amendment, the Pennsylvania Wiretap Act and the recent decision in *Carpenter*?

> (2) Whether the Superior Court properly held that the decision of the United States Supreme Court in *Carpenter v. United States*, 138 S.Ct. 2206, 201 L. Ed. 2d 507 (2018), extends to the collection of real time cell site location information.

Commonwealth v. Pacheco, 237 A.3d 396 (Pa. 2020).[13]

As these issues ultimately challenge the decision of the suppression court, our standard of review is whether the suppression record supports the trial court's factual findings; we maintain *de novo* review over the suppression court's legal conclusions, as they are questions of law. *Commonwealth v. Mason*, 247 A.3d 1070, 1080 (Pa. 2021). Our scope of review is limited to considering only the evidence of the prevailing party at the suppression hearing and so much of the evidence of the non-prevailing party as remains uncontradicted when read in the context of the suppression record. *In re L.J.,* 79 A.3d 1073, 1080 (Pa. 2013).

VI. Issue I

A. Parties' Arguments

The parties first address the threshold issue of whether the High Court's ruling in *Carpenter* (that the government's acquisition of historical CSLI constituted a search that requires a warrant supported by probable cause) applies with equal force to the collection of the real-time CSLI evidence at issue here.

Appellant asserts that the Superior Court properly held that the acquisition of 108 days of his real-time CSLI implicates, at a minimum, the same privacy concerns that arose from the government's collection of extensive historical CSLI in *Carpenter,* and therefore

---

[13] Issue (1) was granted as framed by Appellant. The Court directed the parties to address the threshold legal inquiry presented in Issue (2) because the *Carpenter* Court stated expressly that its narrow ruling applied exclusively to the collection of historical CSLI in that case, and did not encompass other forms of electronic surveillance, such as the acquisition of real-time CSLI at issue herein. *Carpenter*, 138 S.Ct. at 2220 (stating, "[o]ur decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps.'"); *id.* at n.4 (emphasizing that the Court decides "no more than the case before us").

constitutes a search for purposes of a constitutional analysis under the state and federal constitutions. He argues that like historical CSLI, acquisition of real-time CSLI allowed law enforcement to achieve near perfect surveillance of his location, beyond public thoroughfares to private residences in which he sought refuge. Further, he posits, both types of CSLI collection allow the government "to conduct continuous surveillance of a citizen's every move for an extended period of time in a way which was not previously possible due to the practical limitations associated with traditional surveillance methods." Brief for Appellant at 21.

Indeed, in Appellant's view, collection of his real-time CSLI results in a greater privacy intrusion than that involved with historical CSLI, as real-time tracking raises distinct privacy concerns relating to the manner by which it is acquired. He emphasizes that historical CSLI is automatically generated as the cell phone periodically communicates with cell-phone towers in its normal course of operation, while real-time CSLI tracking requires the wireless service providers to signal or "ping" the cell phone at the request of law enforcement and then provide the location information to investigators.

Thus, Appellant asserts, unlike historical CSLI, there can be no argument that he voluntarily abandoned his expectation of privacy by disclosing his real-time CSLI to a third party, as the CSLI was generated and transmitted at the sole discretion of police officers for the explicit purpose of a criminal investigation. He further contends that real-time CSLI allows for more accurate surveillance than historical CSLI because it reveals the cell phone's actual current GPS location, which is transmitted promptly to the service provider via cell signal, and then forwarded to law enforcement, with the location information's accuracy generally within a range of thirty meters. Brief for Appellant at 23 (citing N.T. 1/6/2017, at 87, 97).

Accordingly, Appellant asks this Court to hold that *Carpenter's* Fourth Amendment warrant requirement for the acquisition of historical CSLI also applies to the collection of real-time CSLI in this case.[14] Notably, the Commonwealth offers no argument on the issue, as it does not dispute that *Carpenter's* warrant requirement extends to the Commonwealth's collection of Appellant's real-time CSLI. Brief for Appellee at 7 n.1.[15]

B. Analysis

Upon independent review of the inquiry, we agree with the parties and the Superior Court that *Carpenter's* warrant requirement for the collection of historical CSLI, which provides "a comprehensive chronicle of the user's past movements," applies with equal force to the collection of real-time CSLI in the instant case. *Carpenter*, 138 S.Ct. at 2211. Mirroring the analysis in *Carpenter*, we reach this conclusion based on our findings that: (1) Appellant has an expectation of privacy in his location and physical movements as revealed by the Commonwealth's collection of real-time CSLI over a period of months, which society is prepared to accept as reasonable; and (2) Appellant did not voluntarily disclose his CSLI to a third party and abandon that expectation of privacy under the third-party doctrine.

---

[14] Appellant additionally asserts that Article I, Section 8 of the Pennsylvania Constitution guarantees a stronger privacy right than the Fourth Amendment, which independently requires a warrant for the collection of real-time CSLI. Brief for Appellant at 23 (citing *Commonwealth v. Rushing*, 71 A.3d 939, 947, 963 (Pa. Super. 2013), *rev'd on other grounds*, 99 A.3d 416 (Pa. 2014) (holding that under Article I, Section 8, the defendant has a legitimate expectation of privacy that the government would not surreptitiously track his real-time CSLI; thus, police are required to obtain a warrant supported by probable cause to acquire real-time CSLI)). Because we ultimately conclude that *Carpenter's* Fourth Amendment warrant requirement extends to the collection of real-time CSLI in this case, further discussion of Article I, Section 8 in connection with this issue is unnecessary.

[15] The American Civil Liberties Union, the American Civil Liberties Union of Pennsylvania, and the Electronic Frontier Foundation have filed an *amicus* brief in support of Appellant's position on this issue.

As Appellant cogently notes, the acquisition of 108 days of his real-time CSLI implicates the same privacy concerns that arose from the government's acquisition of continual historical CSLI in *Carpenter.* The *Carpenter* Court found that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts." *Id.* at 2217. The Court explained that similar to the GPS monitoring of a vehicle for 28 days in *Jones*, which constituted a search for purposes of the Fourth Amendment, "the time-stamped data [retrieved through historical CSLI] provides an intimate window into a person's life." *Carpenter*, 138 S.Ct. at 2217.

The same is true here, where the continual real-time CSLI provided an intimate window into Appellant's personal endeavors, revealing a wealth of information about his patterns of activity, associations with other individuals, and the privacies of his daily life. As the facts presented demonstrate, real-time phone-location tracking affords law enforcement an investigative tool that did not exist before the cell phone age, *i.e.*, the power to determine Appellant's precise location and follow him continuously without detection, achieving near perfect surveillance of his location over the course of a lengthy criminal investigation as occurred here. This state action provided a comprehensive chronicle of Appellant's physical movements to the same extent found in *Carpenter*, which intruded upon his reasonable expectation of privacy. Indeed, it is unreasonable for society to expect that law enforcement may secretly manipulate our cell phones to compel the device to reveal our physical movements over a period of time.

We further agree with Appellant that he did not waive his legitimate expectation of privacy in his real-time CSLI under the third-party doctrine, as he never voluntarily disclosed his daily physical movements and locations to his wireless carrier. As the *Carpenter* Court clarified, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data;" thus, the government's

acquisition of the information from a third party "does not overcome [an individual's] claim to Fourth Amendment protection." *Carpenter*, 138 S.Ct. at 2220. In this regard, the collection of location information in real time may be more invasive than historical CSLI due to the process by which it is obtained, *i.e.*, with law enforcement requesting the real-time surveillance exclusively for criminal investigative purposes, as opposed to wireless service providers collecting the CSLI for general operational purposes, as occurs with historical CSLI.

Accordingly, we hold that Appellant had a legitimate expectation of privacy in his continuous real-time CSLI; thus, the *Carpenter* rationale requiring a warrant pursuant to the Fourth Amendment for the collection of historical CSLI equally applies here.[16] Under these circumstances, the Commonwealth's acquisition of real-time CSLI must comply with longstanding Fourth Amendment constitutional protections applicable to search warrants.[17]

VII. Issue II

A. The Parties' Arguments

Appellant argues that the Commonwealth's warrantless retrieval of 108 days of his real-time CSLI did not comply with the Fourth Amendment's constitutional protections

---

[16] We leave for another day whether the Fourth Amendment requires the Commonwealth to obtain a warrant for its collection of CSLI that was not acquired on a continual basis over a period of time, as that issue was not presented in *Carpenter* or in this appeal. As did the High Court in *Carpenter*, this Court decides "no more than the case before us." *Carpenter*, 138 S.Ct. at 2220 n.4.

[17] Respectfully, as our holding requires the Commonwealth to comply fully with Fourth Amendment constitutional protections applicable to search warrants when collecting real-time CSLI, there is no support for Justice Wecht's position that our "decision will countenance an intolerable number of unconstitutional invasions of privacy until the issue returns to this Court." (Wecht, J., Concurring and Dissenting Opinion at 3-4). Our holding in this regard is not compromised by our refusal, *infra*, to entertain the merits of a waived facial constitutional challenge to Section 5773. Read in its entirety, this decision compels the Commonwealth to apply Section 5773 in a constitutional manner consistent with this opinion or face suppression of the real-time CSLI acquired.

elucidated in *Carpenter* because the Section 5773 orders authorizing the acquisition of, *inter alia*, real-time CSLI data are not the functional equivalent of a warrant. Significantly, Appellant's Fourth Amendment challenge is based not on the orders themselves, but on the statutory language upon which the orders were issued, which, Appellant submits, is akin to the text of the federal statute in *Carpenter* deemed insufficient to establish probable cause.

Specifically, Appellant characterizes the primary concern in *Carpenter* as emanating from the statutory standard authorizing federal authorities to acquire CSLI based upon "specific and articulable facts showing that there are reasonable grounds" to believe that the information sought was "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). He emphasizes the *Carpenter* Court's holding that this language falls woefully short of establishing probable cause. *See* Brief for Appellant at 26 (quoting *Carpenter*, 138 S.Ct at 2221 (stating that the "Court usually requires 'some quantum of individualized suspicion' before a search or seizure may take place . . . [and] [u]nder the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation -- a 'gigantic' departure from the probable cause rule") (citation omitted)).

Likewise, Appellant maintains, Section 5573 of the Wiretap Act lacks the requisite individualized suspicion for a warrant as it requires only "probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted phone." 18 Pa.C.S. § 5773(b)(1)(i). He acknowledges that Section 5573 employs the phrase "probable cause," while the federal statute in *Carpenter* required "specific and articulable facts showing reasonable grounds." Appellant submits, however, that the jurisprudential defect in both statutes is not the quantum of suspicion involved (*i.e.*, probable cause versus reasonable grounds); rather, both statutes permit a search

predicated on a judicial determination regarding the likelihood that the surveillance will shed light on a criminal investigation, and not a nexus between the proposed search and particularized criminal activity required to demonstrate probable cause. *See* Brief for Appellant at 28 (citing *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983) (explaining the totality of the circumstances test for probable cause as whether "there is a fair probability that contraband or evidence of a crime will be found in a particular place")).

Appellant explains that a requisite element of probable cause is particularity or specificity, which is lacking in both the federal statute in *Carpenter* and Section 5773 of Pennsylvania's Wiretap Act, as they both require a relevancy standard relating to the existence of a criminal investigation, and not a nexus to particularized criminal activity. This failure, he asserts, allows for the search to be defined exclusively by the executing officers' subjective determination of what might be relevant to a criminal investigation, affording law enforcement *carte blanche* access to monitor the location of the cell phone without any limitation as to time of day or geographic location, including private residences.

Challenging the Superior Court's conclusion that the requisites for probable cause set forth by the High Court in *Dalia* were satisfied here, Appellant argues that there was no judicial determination of probable cause that the targeted cell phone was being used in connection with any specific offenses or would lead to evidence of a particular crime or contraband. He further asserts that there was no finding of probable cause as to the identity of the cell phone's user and whether that individual would be engaged in criminal activity in the locations and/or times that the cell phone signal was to be monitored. Moreover, Appellant contends that there was no language in the orders limiting the surveillance evidence to evidence of specified criminal activity.

Finally, and contrary to the conclusion of the intermediate appellate court, Appellant opines that the totality of the circumstances does not establish probable cause to believe that the information obtained would lead to evidence of specific violations of the Crimes Code. In Appellant's view, the trial court order merely found "probable cause" that information "relevant to an ongoing criminal investigation" would be obtained from the CSLI evidence, as that was the only determination that Section 5773 required the trial court to render. Appellant concludes that the Section 5773 orders "fail to effectuate the primary purpose of the warrant: to abolish general searches and seizures." Brief for Appellant at 37.[18]

In response, the Commonwealth asserts that this Court granted allowance of appeal to determine whether the trial court's orders authorizing the search of Appellant's real-time CSLI comported with the Fourth Amendment, as interpreted by the High Court's decision in *Carpenter*. Nevertheless, it submits, Appellant's arguments focus not on the trial court's orders authorizing the search of his real-time CSLI, but on the statute pursuant to which the orders were issued, *i.e.*, Section 5773 of the Wiretap Act. The Commonwealth contends that Appellant did not present to the trial court a facial challenge to Section 5773 of the Wiretap Act, and maintains that he may not do so in his appeal to this Court because the claim is waived. Brief for Appellee at 9 (citing Pa.R.A.P. 302(a) (providing that "[i]ssues not raised in the trial court are waived and cannot be raised for the first time on appeal")).

Assuming for purposes of argument that the claim is preserved, the Commonwealth contends that Section 5773 comports with the Fourth Amendment and is clearly distinguishable from the federal statute deemed insufficient in *Carpenter*. First, it emphasizes the disparate standards of individualized suspicion required by the two

[18] The Defender Association of Philadelphia has filed an *amicus* brief in favor of Appellant in support of this issue.

statutes: "reasonable grounds" in Section 2703 of the SCA at issue in *Carpenter;* and "probable cause" required by Section 5773. Brief for Appellee at 11 (citing *Griffin v. Wisconsin*, 483 U.S. 868, 878-80 (1987) (holding that "reasonable grounds" is a lesser degree of certainty than "probable cause")). The Commonwealth observes that Section 5773 raised the level of individualized suspicion to the constitutional warrant level even prior to the High Court's ruling in *Carpenter*.

Second, the Commonwealth finds "puzzling" Appellant's contention that the Wiretap Act does not require any quantum of suspicion relating to the commission of a particular crime. Brief for Appellee at 14. The Commonwealth argues that the "relevant to an ongoing criminal investigation" language contained in the probable cause standard set forth in Section 5773(b)(1)(i) is not meaningfully different from the standard for criminal search warrants, which requires probable cause to believe that a search of a given location will reveal evidence of a crime. Brief for Appellee at 15 (citing *Illinois v. Gates*, 462 U.S. 213 (1983)).

Third, the Commonwealth refutes Appellant's contention that Section 5773 does not require any nexus between the proposed search and criminal activity. It asserts that the plain text of Section 5773 requires the issuing authority to find that "there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted phone." 18 Pa.C.S. § 5773 (b)(1)(i). Thus, the Commonwealth argues, the statute requires probable cause that evidence of a crime will be found, and that the police identify the targeted phone or phones. More importantly, it submits, Section 5773 requires law enforcement to provide "[t]he identity, if known, of the person who is the subject of the criminal investigation;" *id.* at (b)(1)(iii), as well as a "statement of the offense to which the information likely to be obtained" relates, *id.* at (b)(1)(v). The Commonwealth concludes that these provisions clearly require a nexus between the

search of the CSLI and the alleged criminal activity. Accordingly, the Commonwealth concludes that Section 5773 of the Wiretap Act, unlike Section 2703 of the SCA in *Carpenter*, requires probable cause to believe that evidence of particular criminal activity will be found on the targeted phone, consistent with the Fourth Amendment.

Turning to the trial court orders issued pursuant to Section 5773, the Commonwealth likewise finds them to be consonant with Fourth Amendment guarantees. It asserts that Appellant does not challenge this Court's jurisprudence establishing that an order issued under the Wiretap Act may serve as the functional equivalent of a warrant for constitutional purposes. Brief for Appellee at 10 (citing *Commonwealth v. Alexander*, 708 A.2d 1251, 1256 (Pa. 1998) (plurality) (rejecting the defendant's contention that an order issued by a neutral judicial authority, which found probable cause for the interception of an oral communication under the Wiretap Act, could not satisfy the warrant requirement); *Commonwealth v. Brion*, 652 A.2d 287, 289 (Pa. 1994) (holding that the probable cause/warrant requirement to obtain an oral communication under the Wiretap Act could be satisfied by a prior determination of probable cause rendered by a neutral, judicial authority); and *Commonwealth v. Melilli*, 555 A.2d 1254, 1258-59 (Pa. 1989) (holding that "a judicial order authorizing the installation of pen registers [under the Wiretap Act] is the equivalent of a search warrant in its operative effect . . . [and] the affidavit and order must comply with the requirements of probable cause")).

Given that orders may constitute search warrants when the requisites of probable cause have been established, the Commonwealth argues that there is no reasonable dispute that probable cause was established here, as found expressly by the trial court in the Section 5773 orders, which were based upon the extensive and detailed affidavit of probable cause accompanying the Commonwealth's application. *See* 18 Pa.C.S. § 5772(b)(3) (requiring that an application for a Section 5773 order contain an "affidavit

by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under Section 5773"). Indeed, the Commonwealth asserts, Appellant does not contest this finding of probable cause in his appeal to this Court.

Accordingly, the Commonwealth concludes, the Pennsylvania Wiretap Act is wholly distinguishable from the federal statute at issue in *Carpenter* because it requires the requisite probable cause to search an individual's CSLI. Because the trial court found probable cause for the issuance of the orders at issue, and that conclusion is not disputed herein, the Commonwealth requests that we affirm the judgment of the Superior Court, which affirmed Appellant's judgment of sentence.[19]

In his reply brief, Appellant responds to the Commonwealth's claim that he did not preserve in the trial court a facial challenge to Section 5773. He clarifies that he is not requesting a declaration that Section 5773 is unconstitutional but, rather, seeks the same relief sought in *Carpenter*, *i.e.*, a declaration that the orders authorizing the collection of CSLI evidence, which were issued pursuant to a particular wiretap statute, fail to satisfy the warrant requirement. *See* Reply Brief for Appellant at 18 (stating "Appellant does not and has not challenged the constitutionality of Section 5773."). Thus, he argues, the presumption of constitutionality applicable to duly-enacted legislation is not germane to his suppression issue.

Somewhat inconsistently, Appellant reiterates his position that Section 5773's requirement of probable cause violates the Fourth Amendment, as the statutory text requires only probable cause that the search will uncover evidence "relevant to an ongoing criminal investigation," and not evidence of particularized criminal activity. He

[19] The Pennsylvania District Attorney's Association and the Office of the Attorney General of Pennsylvania each have filed *amicus* briefs in support of the Commonwealth's position on this issue.

further discounts the Commonwealth's reliance on this Court's decisions in *Alexander*, *Brion*, and *Melilli*, which acknowledged that orders issued by a neutral judicial authority could potentially satisfy the Fourth Amendment's requisites for a warrant. Appellant contends that those cases did not examine the particular issue of whether Section 5773 provides constitutional safeguards equivalent to that of a warrant.

Finally, while Appellant does not concede expressly that the orders establish probable cause required for a warrant, he acknowledges that the affidavit of probable cause demonstrated the Commonwealth's belief that he "may have been a transporter of drugs, a drug mule if you will;" that telephone numbers registered to his name had been in contact with individuals involved in drug transactions within several days of those transactions; and that he was or had been involved with transporting drugs from Atlanta, Georgia, to Norristown, Pennsylvania. *Id.* at 4.

B. Analysis

In examining whether the orders authorizing the collection of Appellant's real-time CSLI comply with the Fourth Amendment, we begin our analysis with a review of the protections guaranteed by that provision. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

This constitutional mandate makes clear that search warrants may only issue upon probable cause. "Probable cause exists where the facts and circumstances within the affiant's knowledge and of which he has reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that a search should be conducted." *Commonwealth v. Leed*, 186 A.3d 405, 413 (Pa. 2018). In considering

an affidavit of probable cause, the issuing authority "must apply the totality of the circumstances test which requires it to make a practical, common-sense decision whether, given all of the circumstances set forth in the affidavit . . . including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Commonwealth v. Johnson*, 42 A.3d 1017, 1031 (Pa. 2012) (internal quotations and citations omitted). Reiterating that courts should interpret warrants in a commonsense manner, the High Court has cautioned against invalidating warrants by interpreting them in a hyper-technical fashion. *Illinois v. Gates*, 462 U.S. at 236.

In summarizing the plain language of the Fourth Amendment, the United States Supreme Court has explained that there are three prerequisites for a valid warrant: (1) the warrant must be issued by a neutral, disinterested magistrate; (2) the entity seeking the warrant must demonstrate probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense; and (3) the warrant must describe particularly the place to be searched and the items to be seized. *Dalia*, 441 U.S. at 255.

A court reviewing the issuing authority's determination of probable cause examines only whether a substantial basis exists for the issuing authority's finding of probable cause. *Johnson*, 42 A.3d at 1031. An "after-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review," *Illinois v. Gates*, 462 U.S. at 236, as an issuing authority's probable cause determination is entitled to deference.

Relevant here, the United States Supreme Court has not required that the issuing authority label its determination of probable cause a "warrant." In fact, in *Dalia*, the Court upheld a court order authorizing the interception of an oral communication on grounds that it substantively complied with the 4th Amendment's warrant requirement. 441 U.S.

at 256 (stating that the "[t]he April 5 court order authorizing the interception of oral communications occurring within petitioner's office was a warrant issued in full compliance with these traditional Fourth Amendment requirements").

Likewise, as the Commonwealth cogently observes, this Court has held that orders issued pursuant to the Wiretap Act may serve as the functional equivalent of a warrant for constitutional purposes where the protections of the Fourth Amendment were afforded. See *Brion*, 652 A.2d at 289 (holding that the probable cause/warrant requirement to obtain an oral communication under the Wiretap Act could be satisfied by a prior determination of probable cause rendered by a neutral, judicial authority); and *Melilli*, 555 A.2d at 1258-59 (holding that "a judicial order authorizing the installation of pen registers [under the Wiretap Act] is the equivalent of a search warrant in its operative effect . . . [and] the affidavit and order must comply with the requirements of probable cause")). Thus, it is clear that the substance, not the label, determines whether a particular court order constitutes a valid warrant.[20]

Having determined that an order may, under certain circumstances, constitute a warrant, we next examine whether the orders at issue here satisfied the requisites of the Fourth Amendment. In doing so, we focus on the substance of the challenged orders and the requisite affidavit of probable cause of Detective Reynolds, upon which those orders

[20] In limited circumstances, a court order authorizing a search may be more appropriate than a warrant because serving the warrant on the suspect would alert the suspect to the search, defeating the entire purpose of the electronic surveillance. *See Katz v. United States*, 389 U.S. 347, 355 n.16 (1967) (opining that "officers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence"); *Alexander*, 708 A.2d at 1256 n.15 (rejecting as nonsensical the defendant's contention that the affidavit and finding of probable cause for a wiretap interception should have been reduced to a warrant and served on the defendant because once the defendant was aware of the electronic surveillance, he would tailor his conversations to avoid police detection of his criminal activities).

were based.[21] *See* 18 Pa.C.S. § 5772 (b)(3) (requiring an "affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under section 5773").

Initially, the affidavit sets forth Detective Reynold's extensive experience and education in investigating drug trafficking. It also includes Detective Reynold's affirmations that: (1) he is aware that drug traffickers use cellular phones, often times multiple phones, to arrange and discuss the distribution of drugs; (2) drug traffickers have shipments of controlled substances sent to them from source countries, including Mexico; and (3) after drug traffickers smuggle drugs into the United States, they transport them by a variety of means, including by automobile. Affidavit of Probable Cause of Montgomery County Detective Michael J. Reynolds, dated August 28, 2015, at 1-4.

Significantly, the affidavit included the following affirmation by Detective Reynolds:

> I am aware of the circumstances of this case and am personally involved in the investigation of the facts contained in this affidavit. I allege the facts outlined in the following paragraphs to show there is probable cause to believe David Pacheco, and others known and yet unknown have committed, are committing, and will continue to commit offenses including but not limited to their involvement in the Manufacture, Delivery, and/or Possession With Intent to Deliver a Controlled Substance (35 Pa. P.S., Section 780-113); Criminal Conspiracy (18 Pa. C.S.A., Section 903); Dealing in Proceeds of Unlawful Activities (18 Pa. C.S.A., Section 5111); and Criminal Use of Communication Facility (18 Pa. C.S.A., Section 7512).

Id. at 4.

Notably, the affidavit identified Appellant as the target of the investigation, identified the phone number of the targeted phone, and indicated that the phone is possessed and used by Appellant. *Id.* at 5-6. The affidavit based its assertion of probable

[21] As referenced *supra* at n. 6, the multiple orders issued on August 28, 2015, docketed at DA-165-2015, DA-165(A)-2015, DA-166-2015, and DA-227-2015, each contain the same language, save for the target telephone number(s) specified.

cause on various sources, including Detective Reynold's personal participation in the investigation, and information provided by other investigators and law enforcement agencies, such as the Montgomery County Detective Bureau, the Narcotics Enforcement Team, and the DEA. The affidavit further based its assertion of probable cause on information provided by three separate confidential informants who had proven to be reliable in connection with past narcotics investigations that led to the successful arrest and prosecution of several known drug dealers. *Id.* at 6-22. These confidential informants had personal knowledge that Appellant's family members and associates were involved in illegal drug trafficking, and that Appellant played a role in the Mexican drug cartel's activities under investigation by retrieving and transporting both drugs and money. *Id.* Finally, the affidavit stated that forensic analysis of cell phones used by several known or suspected drug traffickers revealed various communications between Appellant's cell phones and those of the drug traffickers on dates when illegal drug transactions were either occurring or about to occur. *Id.* at 22-27.

As noted, on August 28, 2015, the trial court issued the Section 5773 orders which authorized, *inter alia*, Appellant's wireless service providers to send signals or "pings" to the targeted cell phone numbers listed in the district attorney's application, at times as directed by law enforcement, to generate real-time CSLI, and then disclose that CSLI to investigators, revealing Appellant's whereabouts. *Id.* at ¶ 9. The orders stated that based upon the application, filed in conjunction with the aforementioned affidavit of Detective Reynolds, there was probable cause to believe that information relevant to an ongoing criminal investigation would be recovered by authorizing investigators to obtain data relating to the physical location of the targeted cell phones. Trial Court Order, DA-165-1015, 8/28/2015, at ¶ *Id.* at ¶ 1. Significantly, the orders identified Appellant by name as the subject of the investigation and the source of the heroin, *id.* at ¶ 3, and found that the

information likely to be obtained by the electronic surveillance would relate to violations of the Crimes Code, including the manufacture, delivery, and/or possession with the intent to deliver a controlled substance, criminal conspiracy, and criminal use of a communication facility. *Id.* at ¶ 4.

On October 15, 2015, the trial court issued a nearly identical order permitting usage of the various electronic surveillance and tracking methods of the same telephone numbers believed to be utilized by Appellant for an additional 60 days, for a total tracking period of 120 days to investigate the same enumerated violations of the Crimes Code.

Upon careful review, we hold that the district attorney's application and affidavit of probable cause provided a substantial basis for the trial court to conclude that evidence of the enumerated crimes allegedly committed by Appellant would be found in the requested real-time CSLI. As did the Superior Court below, we find that the three requisites for a valid warrant under the Fourth Amendment have been established.

First, the orders were issued by the Montgomery County Court of Common Pleas, which is a neutral, detached, issuing authority. Second, the district attorney demonstrated in its application and affidavit the requisite probable cause to believe that the evidence sought would aid in a particular apprehension or conviction for a particular offense. To be precise, the application and affidavit demonstrated probable cause to believe that the CSLI evidence sought from the targeted cell phones, identified by the phone number attached to them, would aid in the apprehension of Appellant for the specific offenses of manufacture, delivery, and/or possession with the intent to deliver a controlled substance, criminal conspiracy, and criminal use of a communication facility. Thus, the Commonwealth established individualized suspicion and a nexus between the real-time CSLI evidence sought and the identified crimes alleged to have been committed by

Appellant. The Commonwealth additionally demonstrated in the affidavit that Appellant utilized his cell phone in conducting the drug-trafficking activities.

Moreover, Appellant has failed to prove any clearly erroneous fact-finding of the trial court in this regard and, indeed, has acknowledged that the affidavit of probable cause demonstrated the Commonwealth's belief that he "may have been a transporter of drugs, a drug mule if you will;" that telephone numbers registered to his name had been in contact with individuals involved in drug transactions within several days of those transactions; and that he was or had been involved with transporting drugs from Atlanta, Georgia, to Norristown, Pennsylvania. Reply Brief for Appellant at 4.[22]

Third, the applications and affidavits of probable cause provided particular descriptions of the place to be searched and the items to be seized. While Appellant's instant challenge to the Section 5773 orders focuses exclusively upon the probable cause requirement for a valid warrant, he asserts additionally, without elaboration, that the Section 5773 orders "permitted surveillance which far exceeded that for which there was any attempt to establish probable cause and authorized law enforcement to continuously monitor [his] location 24 hours a day, seven days a week for an aggregate of 108 days, without any limitations, geographic or otherwise to account for [his] lawful activities." Brief for Appellant at 16-17. He further suggests that law enforcement obtained his whereabouts "anywhere that he traveled, including behind doors and walls of the private dwellings in which he sought refuge." *Id.* at 18. Respectfully, to the extent that Appellant has preserved a particularity challenge, we are not persuaded by his contentions.[23]

---

[22] We further observe that the Superior Court concluded that Appellant "did not specifically preserve an issue challenging the finding of probable cause" in its appeal before that court. *Pacheco*, 227 A.3d at 372 n.18.

[23] The Superior Court held expressly that Appellant waived any claim that the Section 5773 orders were overbroad, *see Commonwealth v. Pacheco*, 227 A.3d at 370 n.13

The Fourth Amendment "specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the person or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006). The challenged Section 5773 orders authorized a search of information generated by the enumerated telecommunication service providers that related to Appellant's cell phone, which was identified particularly on each Section 5773 order by a separate telephone number. The evidence seized was limited to the CSLI disclosing Appellant's whereabouts. While the aggregate duration of the surveillance authorized by the multiple orders was lengthy, it was supported by the extensive affidavits of probable cause accompanying each Section 5772 application. As referenced throughout, these affidavits set forth specific and articulable facts to believe that Appellant played an integral role in an international heroin distribution organization being investigated by the Montgomery County District Attorney's Office, in conjunction with the Pennsylvania State Police and the DEA, and that disclosure of the CSLI would aid in Appellant's prosecution for enumerated drug offenses. As other courts have recently observed, "defining the permissible parameters of time for CSLI searches that are justified by probable cause is difficult," and each case involves a fact-intensive inquiry that must be resolved based on the particular facts presented. *Commonwealth v. Hobbs*, 125 N.E.3d 59, 71 (Ma. 2019).

(deeming waived Appellant's claim that the Section 5773 orders were overly broad because he failed to include that issue in his concise statement of matters complained of on appeal), and Appellant did not seek allowance of appeal for this Court to review that ruling. It is well-settled that where a claim has been presented to the trial court, but abandoned on appeal, this Court should not pass upon it because "[f]ailure to pursue an issue on appeal is just as effective a forfeiture as is the failure to initially raise the issue." *Commonwealth v. Piper*, 328 A.2d 845, 847 n.5 (Pa. 1974). We address the particularity of the Section 5773 orders only to complete our review of whether they satisfy the three requisites of a valid warrant under the Fourth Amendment, as elucidated in *Dalia*, *supra*.

Moreover, the lack of geographical limitation in the challenged Section 5773 orders does not violate the particularity requirement, as the actual locations tracked by the CSLI evidence were neither searched nor seized. Thus, the Commonwealth was not required to describe with particularity in each Section 5772 application every location where Appellant could be tracked. As the Office of the Attorney General observes in its *amicus* brief, the Section 5773 orders did not grant law enforcement unfettered authority to access conversations and events that transpired inside private residences; rather, they provided law enforcement "only location information and nothing more." *Amicus* Brief of the Office of the Attorney General at 21. We therefore conclude that the particularity requirement for a valid warrant was satisfied. Accordingly, the search of Appellant's real-time CSLI was lawful, as it complied with the traditional requisites of the Fourth Amendment, and Appellant's suppression motion was properly denied.

We are left with Appellant's contention that the orders authorizing the collection of his real-time CSLI violate the Fourth Amendment because they were issued pursuant to Section 5773, which, in his view, fails to set forth a constitutional standard of probable cause. Respectfully, Appellant wants his proverbial cake and to eat it too, as he declares definitively that he is not challenging the constitutionality of Section 5773, *see* Reply Brief for Appellant at 18 (stating that he "does not and has not challenged the constitutionality of Section 5773"), yet seeks to invalidate the orders authorizing the search of his real-time CSLI based exclusively upon the purportedly unconstitutional statutory language in Section 5773.

Regardless of Appellant's characterization of his argument to this Court, both parties observe correctly that Appellant did not preserve in the trial court a facial constitutional challenge to Section 5773. As noted, relevant here, Appellant's suppression motion challenged the Commonwealth's acquisition of CSLI on the grounds

that the Commonwealth failed to obtain a search warrant. *See* Supplement to Motion to Suppress Evidence, 11/18/2016, at ¶ 5. He further contended that the Commonwealth's collection of CSLI constituted a constitutionally-prohibited general search. *Id.* at 6. Appellant did not, however, contend that Section 5773 was unconstitutional or tether his suppression arguments to the text of Section 5773 by alleging that suppression was warranted because Section 5773 utilized a standard less than traditional probable cause under the Fourth Amendment. In short, while Appellant challenged the trial court's orders sanctioning the real-time tracking of his cell site location in his suppression motion, he did not contend that the statute pursuant to which the searches were authorized was constitutionally deficient. Accordingly, Appellant waived any facial challenge to Section 5773. *See* Pa.R.A.P. 302(a) (providing that "[i]ssues not raised in the trial court are waived and cannot be raised for the first time on appeal"); Pa.R.Crim.P. 581(D) (providing that a motion to suppress shall "state specifically and with particularity," *inter alia*, "the grounds for suppression"); Pa.R.Crim.P. 575(a)(3) (providing that "[t]he failure, in any motion, to state a type of relief or a ground therefor shall constitute a waiver of such relief or ground").

Accordingly, to the extent Appellant presents a facial constitutional challenge to Section 5773 in his appeal to this Court, we decline to address the waived issue and hold simply that Section 5773 was applied here in a constitutional manner. *See Wolf v. Scarnati*, 233 A.3d 679, 696 (Pa. 2020) (providing that "[i]f a statute is susceptible of two reasonable constructions, one of which would raise constitutional difficulties and the other of which would not, we adopt the latter construction"). We must keep in mind that this Court granted allowance of appeal to address whether the orders authorizing the collection of Appellant's real-time CSLI complied with the Fourth Amendment. As we have answered this inquiry in the affirmative, this appeal is resolved.

Moreover, we reject Appellant's contention that his case is not meaningfully distinguishable from *Carpenter*. There are fundamental distinctions between Section 5773 of the Wiretap Act and the statute at issue in *Carpenter*, 18 U.S.C. § 2703(d), which the High Court held was insufficient to establish probable cause. The most obvious distinction is that Subchapter E of the Pennsylvania Wiretap Act speaks in terms of "probable cause" and requires the Attorney General or district attorney to file with its application "an affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under [S]ection 5773." 18 Pa.C.S. § 5772. As set forth in detail *supra*, it is the affidavit of probable cause in this case that demonstrated that the probable cause standard as required by the Fourth Amendment was satisfied.

The federal statute in *Carpenter*, however, did not require a finding of probable cause or an affidavit attesting to the same.[24] Instead, the federal statute permitted

---

[24] Notably, Section 2703 addresses in subsection (c) the circumstances under which a government entity may require a provider of electronic communication service to disclose a record or other information. 18 U.S.C. § 2703(c). Subsection (c) permits such disclosure when the government obtains a court order under subsection (d). *Id*. Subsection (d) provides:

> (d) Requirements for court order. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d).

authorization for the acquisition of historical CSLI based upon a showing of "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703. Equally significant, the federal statute did not require individualized suspicion or a nexus between alleged criminal activity and the request for collection of CSLI evidence. To the contrary, under Section 5773, an order authorizing the Commonwealth to obtain CSLI evidence must specify, *inter alia*, a statement of the offense to which the information likely to be obtained relates, 18 Pa.C.S. § 5773(b)(1)(v), as well as the identity of the person targeted in the investigation and the person connected to the phone, if known. *Id.* at § 5773(b)(1)(ii), (iii). Accordingly, contrary to Appellant's contentions, the Superior Court's holding, which we affirm herein, did not conflict with the High Court's ruling in *Carpenter*.

VIII. Conclusion

In summary, we hold that because Appellant had a legitimate expectation of privacy in his continuous real-time CSLI, the *Carpenter* rationale requiring a warrant for the collection of historical CSLI applies with equal force here. We further conclude that because the Section 5773 orders authorizing the collection of Appellant's real-time CSLI evidence satisfied the requisites of the Fourth Amendment, they served as the functional equivalent of a warrant. Thus, the search of Appellant's real-time CSLI evidence was constitutional. Accordingly, we affirm the Superior Court's judgment, which affirmed Appellant's judgment of sentence.

Justices Saylor, Todd, Dougherty, and Mundy join the opinion.

Justice Donohue files a concurring and dissenting opinion.

Justice Wecht files a concurring and dissenting opinion.