

IN THE SUPERIOR COURT OF THE STATE OF DELAWARE
IN AND FOR SUSSEX COUNTY

STATE OF DELAWARE

v.

MCARTHUR M. RISPER, JR.,

Defendant

I.D. NO. 1805007714

FILED PROTHONOTARY
SUSSEX COUNTY
2019 APR 12 P 12:32

ORDER

Upon Defendant's Motion to Suppress Evidence. Granted.

AND NOW TO WIT, this 12th day of April, 2019, upon consideration of Defendant's Motion to Suppress evidence seized from two cell phones, **IT APPEARS THAT:**

1. On July 2, 2018, McArthur M. Risper, Jr. ("Defendant") was charged with First Degree Murder and Conspiracy in the First Degree.
2. A Superior Court Judge reviewed and granted two search warrants for the Verizon Wireless records of two cellular phones belonging to Defendant.
3. On December 21, 2018, Defendant filed two motions to suppress any and all evidence found in relation to the two search warrants for two separate cell phone numbers that belonged to Defendant. The State of Delaware ("the State") responded to both of Defendant's motions. Both of the Defendant's motions, for each individual cell phone number, were essentially identical. In turn, the State's responses to both motions were also essentially identical.

4. Defendant challenges the search warrant that authorized the State to search two cell phones seized from Defendant. The State cited witness statements that placed Defendant at the scene of the homicide on May 11th, 2018. The warrant authorized the State to search:

Any and all IP connection logs, any and all cell site tower location information including cell site(s) activation(s), numbers dialed, incoming numbers/chirp numbers/direct connects/walkie talkie if needed, subscribers electronic serial number(ESN), and all billing information/accounts notes, for the specified cellular/wireless telephones, or any telephone numbers revealed the original records and engineering map showing all cell site tower locations, sectors and orientations, and a list of any and all applicable cellular sites, numbers, locations, addresses and or latitude and longitude of any said sites, including RTT, (Round Trip Tracking) data. Also, that cellular sites, lists, latitude and longitude be provided via electronic mail in an electronic format if applicable and/or possible. Subscribers, ESN, and billing information for any other cellular/wireless telephones on this account or that may be identified from these records. Should this cellular/wireless number/equipment which is the current target of this order have changed during the requested periods, Mobile Identification Number (MIN/MESN) or combination have been changed by the subscribers during the course of this order, this order will apply to any other MIN's/MESN's. Finally, that this order will apply to any and all companies which may provide and /or carry wireless telecommunication services for the target mobile number equipment. This may be required because of number portability and/or if the original carrier was modified due to roaming and/or other considerations/reasons from Friday May 11, 2018 at 0100 hours Eastern Standard Time (EST) to Monday May 14, 2018 at 1500 hours Eastern Standard Time (EST) for cell phone (302) xxx-xxxx, on the Verizon network, by way of Verizon Wireless Legal Compliance.¹

5. Defendant contends that the evidence seized from the two cell phones was obtained in violation of his rights under the Fourth and Fourteenth Amendments to the United States Constitution and Article I, §6 of the Delaware Constitution. The parties agree that the Court's analysis is limited to the four corners of the search warrant to determine its validity.²

¹ Def.'s Mot. to Suppress, Ex. A at 1-2 (September 7, 2018) (emphasis added) (hereinafter Search Warrant).

² Def.'s Mot. to Suppress at 1.

6. Defendant contends that (1) the search warrants failed to describe the items to be searched for and seized with particularity; (2) the search warrants are overly broad; and (3) the search warrants failed to place a reasonable temporal restriction on the officer's search of cell phone information.³ Specifically, Defendant argues that a warrant, no matter its target, must both describe the things to be searched with sufficient particularity and be no broader than the probable cause on which it is based.⁴ Defendant contends that, the search warrant authorized the search of GPS or Round Trip Tracking ("RTT") location information and personal information such as numbers dialed when the state only gave probable cause for RTT information.⁵ Furthermore, Defendant contends that the time frame of the homicide was brief, roughly 8:07 p.m. on May 11th, and that the search warrant authorized a search over four days making the temporal restriction overbroad.⁶
7. The State responds that the warrant supports a finding of probable cause, a logical nexus and permissible scope. The State, in the affidavit of probable cause, provides that Defendant was identified by photo line-up as being one of the shooters, Defendant was in possession of a vehicle that matched the description of the getaway vehicle from the homicide scene, and that Defendant used his cell phone to communicate with various people over the time period stated in the warrant.⁷ The State contends that the warrant clearly limits the State's search of Verizon's records to cell site location data, and therefore plead with particularity what was to be searched, making a general search impossible.⁸ As to the temporal scope of the warrant, the State contends that the temporal limitation was

³ *Id.* at 9-10.

⁴ *Id.* at 10.

⁵ *Id.*

⁶ *Id.* at 12.

⁷ State's Resp. at 1.

⁸ *Id.* at 6.

confined to the date of the homicide through the date Defendant turned himself in to the Delaware State Police. The State further contends that these facts establish the necessary nexus that Verizon Wireless records would yield relevant information as to his whereabouts just prior to the crime, at the time of the crime, and after the crime, up until the date he turned himself in.⁹

8. When dealing with search warrants concerning cellular phone information calls for “particular sensitivity” and a carefully designed scope needs to be set forth in the warrant itself.¹⁰ This is because when the Government tracks the location of a cell phone it achieves near perfect surveillance.¹¹ A search of such information would invade a defendant’s reasonable expectation of privacy in the whole of his physical movements as apart from disconnecting the phone from the network, and there is no way to avoid leaving behind a trail of location data.¹² Therefore, the Government must generally obtain a warrant supported by probable cause before acquiring such [GPS location] records.¹³ “[T]he items to be searched and search (sic) for must be described ‘as particularly as possible.’”¹⁴
9. The issuing judge or magistrate will initially determine whether probable cause exists for a search warrant. This determination “will be paid great deference by a reviewing court.”¹⁵ This Court will review the decision of the judge or magistrate issuing the search warrant to

⁹ *Id.* at 9.

¹⁰ *Bradley v. State*, 2019 WL 446548, at *6 Del. Super Ct. February 4, 2019) (citing *Buckham v. State*, 185 A. 3d 1, 18-19 (Del. 2018)).

¹¹ *Carpenter v. US*, 138 S. Ct. 2206, 2218 (2018).

¹² *Id.* at 2219-2220.

¹³ *Id.* at 2221.

¹⁴ *State v. Anderson*, 2018 WL 6177176 at *4 (Del. Super. Ct. November 5, 2018) (quoting *Wheeler v. State*, 135 A. 3d 282, 296 (Del. 2016)).

¹⁵ *Jensen v. State*, 482 A. 2d 105, 11 (Del. Super. Ct. 1984).

insure, looking at the “totality of the circumstances,” that a substantial basis for issuance of the warrant existed.¹⁶

10. When determining the sufficiency of a search warrant, the Court is limited in its analysis to the information provided “within the four-corners of the affidavit[.]”¹⁷ Thus, “sufficient facts must appear on the face of the affidavit so that an appellate court can verify the factual basis for the [Superior Court Judge or magistrate’s] determination regarding the existence of probable cause.”¹⁸ The Court must also consider the information in the affidavit under a totality of the circumstances.¹⁹ “[R]easonable inferences [may be drawn] from the factual allegations in the affidavit.”²⁰ Defendant bears the burden of establishing that the warrant was unlawful.²¹

11. The Court finds that issuance of the search warrant was improper because, assuming arguendo that the search warrant contained probable cause and a logical nexus to the crime, the search warrant was far broader than any possible probable cause finding on which the warrant was based.

12. Here, the search warrant provides, at best, probable cause for the search of RTT location information. However, the search warrant authorizes a search and seizure of information broader than GPS location information. Specifically, the search warrant allows the State to search “numbers dialed, incoming numbers/chip numbers/direct connects/walkie talkie if needed, subscribers electronic serial number, and all billing information/accounts notes,

¹⁶ *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

¹⁷ *LeGrande v. State*, 947 A. 2d 1103, 1107 (Del. 2008).

¹⁸ *Dorsey v. State*, 761 A. 2d 807, 811 (Del. 2000).

¹⁹ *LeGrande*, 947 A. 2d at 1107-08.

²⁰ *State v. Westcott*, 2017 WL 283390, at *2 (Del. Super. Ct. January 23, 2017) (quoting *Bradley v. State*, 51 A. 3d 423, 431 (Del. 2012)).

²¹ See *State v. Sisson*, 883 A. 2d 868, 875 (Del. Super. Ct. 2005); *State v. Dick*, 2004 WL 1172883 at *3 (Del. Super. Ct. 2004).

for the specified cellular/wireless telephones, or any telephone numbers revealed the original records.”²²

13. Defendant relies on the Delaware Supreme Court rulings in *Buckham v. State*²³ and *Wheeler v. State*²⁴ to assert that the search warrant is overly broad and must be suppressed. In *Buckham*, the Court struck down a warrant on the grounds that the “warrant was both vague about the information sought . . . and expressly authorized the search of materials there was no was no probable cause to search.”²⁵ The Court found it particularly troubling that the warrant allowed law enforcement officers to search information that had nothing to do with GPS location information such as incoming/outgoing calls, missed calls, contact history images, photographs and SMS (text) messages.²⁶
14. In *Wheeler*, the Court struck down a search warrant that allowed investigating officers to search through all of the files on a defendant’s computer.²⁷ Defendant had not powered on his computer since 2012 and probable cause in the warrant did not arise until 2013.²⁸ The Court held that the warrant failed to limit the search to the relevant time frame, and was therefore overbroad.²⁹ Specifically, the Court noted that the State unsystematically sifted through defendant’s digital universe, even though [the computer] logically could not have contained material created or recorded during the relevant time period.³⁰
15. Despite the holdings of *Wheeler* and *Buckham* the State maintains that the warrant is sufficiently particular because Defendant’s entire digital universe was not searched and

²² Search Warrant at 1.

²³ *Buckham v. State*, 185 A. 3d 1, 18 (Del. 2018).

²⁴ *Wheeler v. State*, 135 A. 3d 282 (Del. 2016).

²⁵ *Buckham*, 185 A. 3d at 17.

²⁶ *Id.* at 19.

²⁷ *Wheeler*, 135 A. 3d at 304.

²⁸ *Id.* at 305.

²⁹ *Id.* at 304.

³⁰ *Id.* at 305.

that the search warrant seeks records in the possession of Verizon Wireless and not directly from Defendant's phone.³¹ The State relies on *Starkey v. State*³² to assert that the Delaware Supreme Court has upheld a warrant with less specificity than in the present case. In *Starkey*, the search warrant provided for the search of "any and all data stored by whatever means . . . to include but not limited to registry entries, pictures . . . call logs, electronic mail, telephone numbers . . . any other information/data pertinent to this investigation."³³ The Court held that the warrant was not vague as it specifically limited the officer's search of the cell phones to certain types of data, media and files that were "pertinent to this investigation."³⁴

16. However, *Starkey* is distinguishable. The defendant in *Starkey* only raised one claim on appeal, and that is whether the search warrant was defective because it failed to set forth sufficient facts necessary to establish probable cause within the "four corners" of the document.³⁵ Also, this case was decided before both *Wheeler* and *Buckham*, and does not touch on the issue of whether or not the warrant was broader than the probable cause on which it was based. Furthermore, the United States Supreme Court has held that Fourth Amendment protection extends to GPS/RTT location information held by wireless cell phone providers.³⁶

17. This Court need not rule on the issue of temporal scope because Defendant demonstrated that even if the State had probable cause to search the Verizon Wireless records for RTT

³¹ State's Resp. at 4.

³² 74 A. 3d 655 (TABLE) (Del. 2013).

³³ *Id.* at *4.

³⁴ See *id.*; *Fink v. State*, 817 A. 2d 781 (Del. Super. Ct. February 21, 2003).

³⁵ *Starkey*, 74 A. 3d at *1.

³⁶ See *Carpenter*, 138 S. Ct. 2206, 2484 (2018)(holding that "given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome [defendant's] claim to Fourth Amendment protection.").

location information the scope of the warrant was broader than the probable cause in which it was based.

18. Therefore, considering the totality of the circumstances, evidence found relating to the two search warrants relating to Defendant's cell phone numbers must be suppressed.

Defendant's Motion to Suppress is **GRANTED**.

IT IS SO ORDERED.

A handwritten signature in blue ink, appearing to read "Richard F. Stokes", is written over a horizontal line. The signature is stylized and cursive.

Richard F. Stokes, Resident Judge

cc: Prothonotary
Tasha Marie Stevens, Esq.
Caroline C. Brittingham, Esq.
Michael Tipton, Esq.