No. 24-

IN THE

Supreme Court of the United States

RASHAWN TYRIQ PERKINS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

MARK BODNER, ESQ.
Counsel of Record
4041 University Drive, Suite 403
Fairfax, Virginia 22030
(703) 385-6667
rendob@gmail.com

Counsel for Petitioner

335315

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

QUESTIONS PRESENTED

Petitioner was arrested by law enforcement officers based upon real time location data collected from his cell phone or other device through his social media account provider. This data was seized pursuant to a search warrant that authorized collection over a thirty day period. The warrant did not describe a nexus between the location data expected to be seized and criminal activity or evidence of crime. The officer that made application for the search warrant executed it.

The questions presented are:

1. Whether the court of appeals correctly determined that a search warrant for collection of real time location data from Petitioner's cell device over a period of thirty days did not violate the particularity requirements of the Fourth Amendment.

2. Whether the court of appeals correctly determined that the search warrant for seizure of real time location data from Petitioner's cell device over a thirty day period was not so facially deficient as to prevent an objective law enforcement officer's reasonable reliance upon its validity to search pursuant to the Fourth Amendment.

TABLE OF CONTENTS

Page

TABLE OF APPENDICES

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes & Other Authorities:

PETITION FOR A WRIT OF CERTIORARI

Rashawn Tyriq Perkins (Perkins) respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra* at 1a) is unpublished. The district court's conclusions of law disposing of the motion to suppress is unpublished but set forth in an excerpt of the transcript of its ruling from the bench. (App. *infra*, 9a)

JURISDICTION

The court of appeals entered judgment on October 11, 2024. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides in pertinent part:

> "[t]he right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."

STATEMENT

A confidential informant identified Petitioner as a participant in two robberies that occurred in the same locality on the same date. With the informant's statements and other information, including photographs from Petitioner's Facebook, social media account, the lead officer, Detective Andrea, applied for and received a warrant from a Fairfax County,

Virginia Circuit Court judge to search Petitioner's Facebook account for real time location data, without geographic limits, for a period of thirty (30) days. The Court also granted authority to employ a pen register and trap and trace device to receive real time electronic signals from the Facebook service provider collected from Petitioner's cell phone or other device.

Detective Andrea's application for the search warrant, and the warrant itself did not describe the proposed geographic areas to be searched. Nor did they identify what evidence of crime or criminal activity law enforcement expected to find in Petitioner's real time location data connected to the robbery offenses under its investigation. Based on the real time location data delivered by the Facebook service provider Fairfax County police established surveillance at a location where they then observed Petitioner to be staying overnight. With this information police secured a second search warrant. Upon execution of this second warrant they arrested Petitioner for the robberies. A third search warrant issued based upon the two earlier warrants. Virginia prosecution gave way to federal charges.

Following denial of Petitioner's motion to suppress evidence seized pursuant to the first Facebook search warrant and two subsequent search warrants the District Court convicted Petitioner of these and other robberies and firearms charges. Petitioner contended that the first Facebook warrant was overbroad. The second warrant issued without a showing that there was a nexus between the offenses charged and evidence sought in that warrant. The warrant lacked particularity required by the Fourth Amendment.

In its unpublished opinion the Fourth Circuit Court of Appeals affirmed Petitioner's convictions. The Court disagreed with Petitioner's arguments that the Facebook warrant was overbroad, lacked particularity and failed to show a nexus between the crimes alleged and the location information to be seized. Assuming without deciding that the Facebook warrant was invalid the Court held that the good faith exception to the exclusionary rule justified admission of the evidence Petitioner sought to suppress. The Court rejected Petitioner's contention that the Facebook warrant was so facially deficient that no reasonable officer could rely on its validity. The Court reasoned that the warrant was sufficiently particularized as it limited ascertainment of location data associated with a single Facebook account over a 30 day period. It added that the unsettled nature of the law concerning the temporal limitations of such warrants would not permit it to say the officers' reliance on the warrant was unreasonable.

A. The initial investigation and issuance of the search warrant for real time location data over a 30 day period

Detective Andrea of the Fairfax County Police noted a suspect's clothing on video footage of the February 5, 2022 robberies of a 7/11 store and Sunoco service station in Herndon, Virginia. He believed such items bore similarity to those observed in robberies that occurred in the same area weeks before. Detective Andrea considered certain items of the clothing as distinctive, including a red hat and black running shoes. A confidential informant identified Petitioner as O1 from the February 5, 2022 robberies wearing items of clothing similar to those that aroused Andrea's interest. The informant advised Andrea that on the day of the robberies O1 showed him a gun and announced his intention to commit a robbery.

Andrea found a photograph of Petitioner on his Facebook social media account wearing a red hat similar to what he had earlier associated with the robberies. In an affidavit submitted in application for a search warrant to search real time location data from Petitioner's Facebook account Andrea related, in pertinent part, "information relevant and material to an ongoing criminal investigation in that it is believed that this information will concern the aforementioned offenses and assist in locating the target of the investigation and potentially result in the recovery of evidence." Court of Appeals Joint Appendix, JA 68

Among the categories of items from Petitioner's Facebook account to be searched for Detective Andrea's attachment A to his affidavit specified:

> 5. Any and all location data to include device GPS signal and connection information, location tags, shared location data, any data collected by Facebook's location services via the user's mobile phone or other device, geo location information attached to activations, historical internet protocol account activations, and all stored location data from third party application, historical internet protocol account activations, historically stored header information, e-mail addresses associated historically with the account, account usage information, and account purchase information, for a time period of February 4, 2022, through February 6, 2022. JA 71-72

On February 14, 2022 a Fairfax County Circuit Court judge issued a search warrant for real time location data collected from Petitioner's Facebook account for thirty (30) days and a separate search warrant to search his Facebook account for real time location information without temporal limitation. JA 58, 62 In one affidavit Detective Andrea averred that "[t]he object, thing or person to be searched for [x] constitutes evidence of the commission of such offense." JA 65

Neither the affidavits nor the warrants described or identified locations to a particular place or a specific location where law enforcement expected evidence of where

Petitioner's cell phone or other device might be found. The affidavits and warrants did not set forth facts to show a nexus between Petitioner's cell phone or device and criminal activity or that between his location and evidence of a crime. JA 58-74

After collection of pings in real time from Facebook on Petitioner's cell phone or device for nearly a week police conducted surveillance of an apartment near Alexandria, Virginia where officers believed Petitioner returned at night. On February 22, 2022 another Fairfax County Circuit Court judge, relying on an affidavit stating facts based on the real time location pings from Petitioner's cell phone or device and related surveillance information, issued a second search warrant, this time for an apartment at 7971 Audubon Avenue, # 202, Alexandria, Virginia. JA 85-92 During execution of this second search warrant Fairfax County Police arrested Petitioner, seized his cell phone and certain items of his clothing. Based on search of the apartment, and collection of a firearm that was seen thrown from an apartment window near commencement of the February 22nd search, officers requested and obtained a third search warrant for apartment # 202 on February 23rd. JA 97-103 Pursuant to this third warrant police seized another cell phone, a laptop computer and additional clothing items.

B. The District Court proceedings

On April 26, 2022 Petitioner was arrested on a federal complaint and warrant immediately following dismissal of state charges based on the Herndon robberies. *United States v. Rashawn Tyriq Perkins,* United States District Court, Eastern District of Virginia, 1:22-cr-114, docs. 1, 2, 6. On June 23, 2022 an indictment issued with seven counts charging his interference with commerce by robbery in violation of 18 U.S.C. §1951(a), six

counts of using, carrying and brandishing a firearm during a crime of violence in violation of 18 U.S.C. § 924(c)(1)(A)(ii), and two counts of possession of a firearm by a prohibited person in violation of 18 U.S.C. § 922(g)(1). JA 15

Petitioner moved to suppress the evidence seized by law enforcement pursuant to the three search warrants, including the electronic data, the clothing, phones and devices. He maintained that the first (Facebook account) search warrant for the 30 days of prospective location data was overbroad, lacking particularity as to the object of the search. Citing *United States v. Jones*, 565 U.S. 400 (2012) Petitioner argued this search permitted indiscriminate intrusion into his private activities. JA 34, 47-57 He also asserted that by reference to the Facebook warrant for location data the second warrant did not set forth a nexus between the scope of the warrants and the specific criminal activity or location of the evidence expected to be collected. JA 53-55; 217-218

Following the hearing on suppression the District Court entered an Order denying Petitioner's suppression motion. JA 228 The District Court relied on authorities cited by the government determining that a continuous 30 day collection of electronic data was not unreasonable in scope and did not constitute a general search. App., *infra*, 10a. All but one of these authorities involved searches of existing cell site location data, not the prospective collection of real time location data.

The District Court also remarked that had the Facebook location data been excised there would be sufficient basis to find probable cause to search that location. App., *infra*, 11a.

Evidence obtained pursuant to the Facebook search warrant and subsequent searches was introduced at Petitioner's trial. A jury convicted Petitioner on four counts of robbery, four counts of using a firearm in a crime of violence and three counts of possession of a firearm by a prohibited person.

C. The Court of Appeals' Decision

By an unpublished, *per curiam* opinion the Court of Appeals affirmed Petitioner's convictions. App., *infra,* 1a. The Court explained that ordinarily searches conducted pursuant to a warrant "will rarely require any deep inquiry into reasonableness," because where a warrant was issued by a magistrate that suffices to establish that a law enforcement officer acted in good faith in conducting the search. App., *infra* 4a-5a, The Court concluded that the Facebook warrant was not so facially deficient as to show objectively that a reasonably well-trained law enforcement officer would have known that the search was illegal. *United States v. Leon,* 468 U.S. 897, 900, 913. 918 (1984) Assuming without deciding that the search was unlawful the Court declined to apply the exclusionary rule.

The Court then held that the warrant was sufficiently particularized because it was limited to ascertaining location data associated with a single Facebook account over 30 day period. App., *infra,* 5a. Referring to its decision in *United States v. Zelaya-Veliz,* 94 F. 4th 321, 340-41 (4th Cir. 2024) *petition for cert. docketed* July 16, 2024, No. 24-5092. The Court stated that reasonable officers would not know that a temporally unrestricted warrant to search private communications involving certain Facebook accounts was invalid given the "unsettled nature" of whether such warrants require temporal limitations. App., *infra,* 5a.

REASONS FOR GRANTING THE PETITION

1. Conform the law governing privacy accorded cell phone/device data

This Court determined in *United States v. Carpenter*, 585 U.S. 296 (2018) that the Fourth Amendment provides an individual a reasonable expectation of privacy in his movements as recorded over a period of time. This because automatic collection of data through cell phones showing such movement (cell site location information - CSLI) is of such depth and comprehensive reach as to permit an unwarranted intrusion into the most intimate and private aspects of the cell user's life. Though decided on a trespass theory in 2012 *Jones* included two concurring opinions that provided some basis for this ruling.

Carpenter addressed the government's collection and use of stored or existing CSLI.

The Court of Appeals' affirmance of the validity of the warrant for the collection of Petitioner's real time location information over a thirty (30) day period conflicts with *Carpenter's* recognition of Fourth Amendment protection in Petitioner's expectation of privacy in his movements. See also *Katz v. United States,* 389 U.S. 347 (1967) The affidavit upon which the Facebook warrant issued did not connect a thirty day collection period with expected discovery of criminal activity or evidence. Detective Andrea, the affiant, asserted that law enforcement expected to locate Petitioner, which then could potentially lead to the discovery of criminal evidence. JA 68.

No principled distinction exists between the Fourth Amendment privacy interest this Court identified for Carpenter from that Petitioner held in his real time movements over a period of thirty days. This Court should bring the law into conformity.

The Facebook warrant is not an arrest warrant. Detective Andrea's supporting affidavit identified Petitioner. The warrant did not particularly describe the places to be searched or the person or things to be seized. The affidavit did not set out a nexus between the information to be searched and the criminal activity or evidence sought in the data expected to be taken. The affidavit and resulting Facebook warrant lacked particularity in the description of the objects to be searched and seized as required by the Fourth Amendment.

2. <u>Eliminate open-ended collection of real time location data by giving effect to the Fourth Amendment requirement of particularity in search warrants connecting evidence sought to the offense alleged</u>

The Court of Appeals ruled that Petitioner's Facebook account was the subject of the search. The Court stated the warrant was "sufficiently particularized as it was cabined to ascertaining location data associated with a single Facebook account over a 30-day period." App., *infra,* 5a. The Facebook account had no intrinsic, informational value to law enforcement. That account served as a conduit through which signal data reflecting the real time location of Petitioner's cell phone or device was seized. The location data was the subject of the warrant. By identifying the Facebook account as the subject of the search the Court of Appeal's decision elided the Fourth Amendment requirement of particularity in the warrant.

Even so, the Court did not determine that the warrant established a nexus between the Facebook account and suspected criminal activity or evidence.

The Court of Appeals' decision does not address or mention this Court's ruling in *Carpenter.* Petitioner's privacy interests in the expansive scope and intrusive nature of real

time location data collected from his device, in places public and private, limited only by a thirty day period is the same as in *Carpenter.* Three decisions of the District Court for the Eastern District of Michigan explain why data seized from Petitioner contravened the Fourth Amendment requirement of particularity in real time location data searches. They also demonstrate that such searches can be designed to meet constitutional bounds. Two of these decisions issued more than four years before this Court decided *Carpenter*. Ultimately these first two, earlier decisions denied suppression on the good faith grounds provided by *Leon*.

United States v. Powell, 943 F.Supp.2d 759 (E.D. Mich. 2013) involved a drug conspiracy. The Court noted the distinction between the use of historical CSLI and collection of real time location data. *Powell* determined "if the government intends to track an individual over a long period of time, and cannot show that the individual will be, for example, in public, non-protected locations for the duration of the tracking, then the warrant application should set forth facts that warrant intrusion into protected locations that the individual may frequent." *Powell* at 778 And " . . . the government should have to demonstrate a nexus between a suspect, the phone and criminal activity, as well as the criminal activity and suspect's location in protected areas, rather than mere probable cause that the person is engaged in criminal activity." *Powell* at 779

United States v. White, 62 F.Supp.3d 614, 628, affirmed, 679 Fed. App'x. 426 (6th Cir. 2017), judgment vacated on other grounds , —— U.S. ——, 138 S. Ct. 641, 199 L.Ed.2d 522 (2018) is another drug case. There agents procured long term GPS and cell monitoring warrants for White's cell phone. The *White* Court asked, if law enforcement anticipates a

suspect will commit a crime some place at some future date does it have probable cause to track him every where he goes? The Court answered "[N]o, 'lest general warrants be revived and the Fourth Amendment's particularity requirement be eviscerated.'" *White* at 627

Speaking to real time location data *Powell* and *White* anticipated *Carpenter's* recognition of Fourth Amendment protection against comprehensive data collection over a lengthy period. *Powell* distinguished the application of *Jones* because the Court's majority ruling was premised on a trespass theory, the physical attachment of a GPS tracker to Jones' vehicle as the means of collection. *Powell* at 776

More recently the same Court in *United States v. Griggs,* 2:20-cr-20403-1 (E.D. Mich., July 22, 2021) followed the lead of *Powell.* doc. 38 An Ohio court issued a warrant authorizing officers to use a "ping cell site location" to track the defendant's location. The District Court granted defendant's motion to suppress stating that the "Government failed to show a definite nexus between the suspected drug activity and the cellphone to be tracked." *Griggs*, doc. 38 at 8.

Ths *Griggs* court refused the Government's contention that the *Leon* good faith exception warranted saving the fruits of that search. It noted the lack of a connection between the drug offense alleged and Griggs' cell phone. It held that the executing officer's reliance on the warrant was objectively unreasonable. *Griggs,* doc. 38 at 10

3. Specify that *United States v. Leon's* exception to the exclusionary rule does not apply where there is no nexus between the real time location data sought and criminal activity or evidence. No objective officer could reasonably, in good faith, rely on the validity of such a facially deficient warrant

The Facebook search warrant was open-ended in authorizing the collection of location data from Petitioner's devices. Excepting the thirty day time limitation, selection of the data to be seized from the devices while moving in public or private locations over such an extended time was left unlawfully to the complete discretion of the executing officer. *Stanford v. Texas,* 379 U.S. 476, 485 (1965) citing *Marron v. United States,* 275 U.S. 192, 196 (1927) This is further evidenced by the return on the warrant which lists only Virginia Code Section 19.2-70.3(K) as the inventoried content of the seizure. JA 63 It shows no itemization of any matter or information seized.

The District Court for the Eastern District of Michigan in *Griggs* granted suppression of the evidence seized in its search over the Government's opposition stating that its affidavit failed to tie the drug trafficking crime to the defendant's cell phone. *Griggs*, doc. 38 at 10 The Court observed " . . . surreptitious Government tracking of an individual is far more intrusive than a subpoena or records request for historical data and requires a much higher legal standard to authorize it." *Griggs*, doc. 38 at 12

Detective Andrea noted in his affidavit for the Facebook warrant he had more than twenty years experience as a police officer, fourteen years of which he served as a detective. He recounted his extensive experience with warrants and searches involving federal and state investigations. JA 66 With due regard to *Jones* and *Carpenter* no objective officer executing a search warrant as vague in the description of its object, and as intrusive as the

Facebook warrant was here, over a thirty day period of constant monitoring, could reasonably rely on its validity.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted

/s/ Mark Bodner
Mark Bodner, Esq.
Counsel of Record
4041 University Drive, Suite 403
Fairfax, Virginia 22030
(703) 385-6667
rendob@gmail.com

Counsel for Petitioner

APPENDIX

TABLE OF APPENDICES

Page

UNPUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 23-4106

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

RASHAWN TYRIQ PERKINS,

Defendant - Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Michael Stefan Nachmanoff, District Judge. (1:22-cr-00114-MSN-1)

Submitted: September 30, 2024 Decided: October 11, 2024

Before NIEMEYER and GREGORY, Circuit Judges, and TRAXLER, Senior Circuit Judge.

Affirmed by unpublished per curiam opinion.

ON BRIEF: Mark Bodner, Fairfax, Virginia, for Appellant. Jessica D. Aber, United States Attorney, John C. Blanchard, Jacqueline R. Bechara, Assistant United States Attorneys, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee.

Unpublished opinions are not binding precedent in this circuit.

PER CURIAM:

Rashawn Tyriq Perkins was convicted, following a jury trial, of four counts of interfering with commerce by robbery, in violation of 18 U.S.C. § 1951(a); four counts of using, carrying, and brandishing a firearm during a crime of violence, in violation of 18 U.S.C. § 924(c)(1)(A)(ii); and three counts of possessing a firearm as a convicted felon, in violation of 18 U.S.C. § 922(g)(1). On appeal, Perkins challenges the district court's denial of his motion to suppress based on an allegedly defective search warrant and the court's imposition, at sentencing, of a special condition of supervised release requiring that he participate in mental health treatment. We affirm.

In early 2022, following a tip from a confidential informant, law enforcement officers began investigating Perkins in connection with several robberies in Northern Virginia. They secured a search warrant requiring Facebook to disclose for 30 days and on an ongoing basis the real-time physical location data associated with Perkins' Facebook account. The Facebook warrant led law enforcement officers to Perkins' residence on Audubon Avenue in Alexandria, Virgina, where, pursuant to a second search warrant, they found evidence connecting Perkins to the robberies. Following indictment, Perkins moved to suppress evidence from the Facebook and Audubon search warrants, arguing that the Facebook warrant was overbroad and had led directly to the discovery of the evidence at Audubon Avenue. The district court held a suppression hearing and denied Perkins' motion, finding that the warrants were not overbroad and were supported by probable cause.

Perkins was subsequently convicted, following a jury trial, of the above-noted charges, and the district court sentenced him to 336 months' imprisonment plus one day. The court also pronounced, as a special condition of his supervised release, that Perkins would "be subject to drug testing and treatment and mental health treatment and counseling as directed by [the United States Probation Office ("Probation")] if [Probation] deem[s] it to be necessary." (J.A. 894).* A written judgment followed, which contained several special conditions of supervision. Special Condition 4 stated that Perkins "shall participate in a [substance abuse] program approved by [Probation]" if he tests positive for controlled substances or shows signs of alcohol abuse. (J.A. 901). Special Condition 5 stated that Perkins "shall participate in a program approved by [Probation] for mental health treatment." (J.A. 901).

I.

Perkins first challenges the district court's denial of his motion to suppress, arguing that the Facebook warrant was overbroad, lacked particularity, and failed to show a nexus between the crimes alleged and the items to be seized. Additionally, he asserts that the good faith exception to an otherwise invalid warrant does not apply.

The Fourth Amendment, which protects individuals from unreasonable searches, provides that "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. To deter police misconduct, evidence seized in

* "J.A." refers to the joint appendix filed by the parties in this appeal.

violation of the Fourth Amendment generally is inadmissible at trial. *United States v. Andrews*, 577 F.3d 231, 235 (4th Cir. 2009). This is the exclusionary rule. However, under the good faith exception to that rule, such evidence is nevertheless admissible if it was "obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause." *United States v. Leon*, 468 U.S. 897, 900, 913, 918 (1984).

We review the district court's factual findings for clear error and its legal conclusions de novo when assessing a decision on a motion to suppress. *United States v. Kehoe*, 893 F.3d 232, 237 (4th Cir. 2018). When a district court denies the motion, we view the evidence in the light most favorable to the Government. *United States v. Shrader*, 675 F.3d 300, 306 (4th Cir. 2012). In cases where a defendant challenges both the existence of probable cause and the applicability of the good faith exception, we may proceed directly to the good faith analysis without first deciding whether the warrant was supported by probable cause. *United States v. Legg*, 18 F.3d 240, 243 (4th Cir. 1994).

Ordinarily, "searches conducted pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004) (internal quotation marks omitted). There are, however, four circumstances in which the good faith exception will not apply:

> (1) when the affiant based his application on knowing or reckless falsity; (2) when the judicial officer wholly abandoned his role as a neutral and detached decision maker and served merely as a "rubber stamp" for the

> police; (3) when the affidavit supporting the warrant was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) when the warrant was so facially deficient that the executing officers could not reasonably have presumed that the warrant was valid.

United States v. Wellman, 663 F.3d 224, 228-29 (4th Cir. 2011). In assessing whether the exception applies, our analysis is "confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal" in light of "all of the circumstances." *Leon*, 468 U.S. at 922 n.23.

Assuming without deciding that the Facebook warrant was invalid, we conclude that the good faith exception to the exclusionary rule applies. The Facebook warrant was not "so facially deficient" that no reasonable officer could have relied on its validity. *See Wellman*, 663 F.3d at 228-29. On the contrary, the warrant was sufficiently particularized as it was cabined to ascertaining location data associated with a single Facebook account over a 30-day period. *Compare United States v. Zelaya-Veliz*, 94 F.4th 321, 340-41 (4th Cir. 2024) (holding Court could "not say" that reasonable officers would have known that temporally unrestricted warrant to search private communications involving certain Facebook accounts was invalid given the "unsettled nature" of whether such warrants require temporal limitations), *petition for cert. docketed*, No. 24-5092 (U.S. July 16, 2024), *with United States v. Lyles*, 910 F.3d 787, 794-96 (4th Cir. 2018) (declining to apply good faith exception where three marijuana stems pulled from defendant's trash were used to support "astoundingly broad" general warrant).

II.

Next, Perkins raises two challenges to the special condition of his supervised release requiring that he participate in mental health treatment. First, he argues that the district court committed an error under *United States v. Rogers*, 961 F.3d 291 (4th Cir. 2020). Second, he asserts that the district court impermissibly delegated to Probation the core judicial function of deciding whether he was to be subject to mental health treatment. At sentencing, the district court announced that Perkins would be "subject to drug testing and treatment and mental health treatment and counseling as directed by Probation if [Probation] deem[s] it to be necessary." (J.A. 894). The written judgment that followed mandated that Perkins participate in (1) a substance abuse program approved by Probation if he tests positive for controlled substances or shows signs of alcohol abuse and (2) a mental health treatment program approved by Probation.

"A defendant has the right to be present when he is sentenced." *Rogers*, 961 F.3d at 296. Accordingly, under *Rogers*, "a district court must orally pronounce all non-mandatory conditions of supervised release at the sentencing hearing." *United States v. Singletary*, 984 F.3d 341, 344 (4th Cir. 2021). That said, "so long as the defendant is informed orally that a certain set of conditions will be imposed on his supervised release, . . . a later-issued written judgment that details those conditions may be construed fairly as a clarification of an otherwise vague oral pronouncement." *Rogers*, 961 F.3d at 299 (internal quotation marks omitted). Thus, "where the precise contours of an oral sentence are ambiguous, we may look to the written judgment to clarify the district court's intent." *Id.* On the other hand, "if a conflict arises between the orally pronounced sentence and the

written judgment, then the oral sentence controls." *Id.* at 296. We review *Rogers* challenges de novo. *Id.*

As the Government correctly points out, the district court's statement at the sentencing hearing is susceptible to at least two meanings—either Probation had discretion to decide whether Perkins must participate in drug and mental health treatment, or it had the authority to instruct Perkins to participate in such treatment if certain conditions were met. Because both readings are reasonable, we conclude that the district court's oral pronouncement was ambiguous and that the written judgment subsequently clarified the ambiguity. Accordingly, there was no *Rogers* error.

Finally, Perkins argues that the district court, at sentencing, impermissibly delegated to Probation the core judicial function of deciding whether he was to be subject to mental health treatment. To be sure, "[a] court can't delegate core judicial functions such as the authority to decide . . . whether a defendant must attend a treatment program." *United States v. Van Donk*, 961 F.3d 314, 327 (4th Cir. 2020) (cleaned up). Again, however, the district court's oral pronouncement was ambiguous. Its written judgment, meanwhile, clarified any ambiguity. It foreclosed a reading of impermissible delegation by establishing that Probation was tasked with requiring Perkins to participate in a substance abuse treatment program only under certain conditions, namely, if he tested positive for controlled substances or showed signs of alcohol abuse, and with requiring him to participate in mental health treatment. Therefore, the district court did not impermissibly delegate to Probation a core judicial function.

III.

Therefore, we conclude, first, that the good faith exception to the exclusionary rule applies to the Facebook warrant. Second, the district court did not commit a *Rogers* error, nor did it impermissibly delegate a core judicial function to Probation. We accordingly affirm. We dispense with oral argument because the facts and legal contentions are adequately presented in the materials before this court and argument would not aid the decisional process.

AFFIRMED

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA,	:	
	:	
Plaintiff,	:	Criminal Action
	:	No. 1:22-cr-00114-MSN-1
v.	:	
	:	
RASHAWN TYRIQ PERKINS,	:	September 1, 2022
	:	10:00 a.m.
	:	
Defendant.	:	
	:	
.....	:	

TRANSCRIPT OF MOTION PROCEEDINGS
BEFORE THE HONORABLE MICHAEL S. NACHMANOFF,
UNITED STATES DISTRICT COURT JUDGE

APPEARANCES:

For the United States:	UNITED STATES ATTORNEY'S OFFICE JOHN C. BLANCHARD, AUSA NICHOLAS J. PATTERSON, AUSA 2100 Jamieson Avenue Alexandria, VA 22314
For the Defendant:	ROBINSON LAW PLLC BRET DANWILL OFFAN LEE, ESQUIRE 10486 Armstrong Street Fairfax, VA 22030
Court Reporter:	Diane Salters, B.S., CSR, RPR, RCR Official Court Reporter United States District Court 401 Courthouse Square Alexandria, VA 22314 Email: Dianesalters.edva@gmail.com Telephone: (301) 338-8033

Proceedings reported by machine shorthand. Transcript produced by computer-aided transcription.

committed these robberies, including information that led to their public Facebook profiles, and Detective Andrea did make efforts to corroborate information; in fact, corroborated information regarding physical description of the robbers, the article of clothing, the very distinctive shoes that I find the Court correctly weighed in determining probable cause, his criminal history, and information regarding the vehicle associated with 02. All of these were done prior to seeking the warrant. I find that had additional information been provided, it would not have changed the calculus, looking at the totality of the circumstances, and that probable cause would still have been established.

I find that the argument on overbreadth, which is detailed in the pleadings, although less was devoted to it at oral argument, must be rejected in keeping with the long line of cases that have found that similar searches and ability to track for the 30-day period that was requested here must be followed. And the government cites a number of cases, including *Liburd*, *Westley*, *Sharp*, *Shah*, *Ray*, and *Alford*, all of which stand for the proposition of that despite the fact that these are broad searches and there is no doubt that the nature of the internet, Facebook, and the ability to collect information that is broad in scope does not make it a general warrant, and that, here, it was tied to the government's effort to recover evidence and find the location of the defendant in this case for a limited period of

time; and so I find that it was appropriate, and I reject the argument on overbreadth.

Likewise, the evidence supporting the affidavits for the searches of Audubon were supported by probable cause. Having found that the warrant was not in any way defective, the information from Facebook that identified that particular building for a period of five days or more where the defendant was located, in addition to the physical surveillance, the efforts to identify the specific apartment through the cameras, the efforts and observations of the defendant going in and out of that apartment and the building and wearing a hat -- all that matched the hat from the robbery, the red hat -- all amounted to sufficient probable cause. Likewise, I find that even if one were to excise the information from Facebook, that there would be sufficient basis to find probable cause to search that location.

And so for all of those reasons, I deny the motion to suppress, I deny the request for the *Franks* hearing, and I find that the evidence collected pursuant to those warrants does not need to be suppressed and was constitutionally obtained.

Is there anything else that I need to address with regard to this matter on the part of the government?

MR. BLANCHARD: No, sir, Your Honor.

THE COURT: Thank you.

Mr. Lee, is there anything else that I need to address?

MR. LEE: Yes, Your Honor. The defense, for purposes

pursuant to this section shall be reasonably compensated for reasonable and actual expenses incurred in providing such facilities and assistance. The expenses shall be paid out of the criminal fund.

H. When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain a pen register or trap and trace device installation without a court order, in addition to any real-time location data obtained pursuant to subsection E of § 19.2-70.3, in the following circumstances:

1. To respond to a user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession, (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent, or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted;

4. To locate a child who is reasonably believed to have been abducted or to be missing and endangered; or

5. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of pen register and trap and trace data, or real-time location data pursuant to subsection E of § 19.2-70.3, concerning a specific person and that a court order cannot be obtained in time to prevent the identified danger.

No later than three business days after seeking the installation of a pen register or trap and trace device pursuant to this subsection, the investigative or law-enforcement officer seeking the installation shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the reasons why the installation of the pen register or trap and trace device was believed to be important in addressing the emergency.

I. No cause of action shall lie in any court against a provider of a wire or electronic communication service, its officers, employees, agents or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order issued pursuant to this section. Good faith reliance on a court order, a legislative authorization or a statutory authorization is a complete defense against any civil or criminal action based upon a violation of this chapter.

History.
1988, c. 889; 2002, cc. 588, 623; 2005, c. 934; 2016, c. 231; 2018, c. 667.

§ 19.2-70.3. Obtaining records concerning electronic communication service or remote computing service.

A. A provider of electronic communication service or remote computing service, which, for purposes of subdivisions 2, 3, and 4, includes a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, excluding the contents of electronic communications and real-time location data, to an investigative or law-enforcement officer only pursuant to:

1. A subpoena issued by a grand jury of a court of the Commonwealth;

2. A search warrant issued by a magistrate, general district court, or circuit court;

3. A court order issued by a circuit court for such disclosure issued as provided in subsection B; or

4. The consent of the subscriber or customer to such disclosure.

B. A court shall issue an order for disclosure under this section only if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation, or the investigation of any missing child as defined in § 52-32, missing senior adult as defined in § 52-34.4, or an incapacitated person as defined in § 64.2-2000 who meets the definition of a missing senior adult except for the age requirement. Upon issuance of an order for disclosure under this section, the order and any written application or statement of facts may be sealed by the court for 90 days for good cause shown upon application of the attorney for the Commonwealth in an ex parte proceeding. The order and any written application or statement of facts may be sealed for additional 90-day periods for good cause shown upon subsequent application of the attorney for the Commonwealth in an ex parte proceeding. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

C. Except as provided in subsection D or E, a provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose the contents of electronic communications or real-time location data to an investigative or law-enforcement officer only pursuant to a search warrant issued by a magistrate, a juvenile and domestic relations district court, a general district court, or a circuit court, based upon complaint on oath supported by an affidavit as required in § 19.2-54, or judicial officer or court of any of the several states of the United States or its territories, or the District of Columbia when the warrant issued by such officer or such court complies with the provisions of subsection G. In the case of a search warrant directed to a foreign corporation, the affidavit shall state that the complainant believes that the records requested are actually or constructively possessed by a foreign corporation that provides electronic communication service or remote computing service within the Commonwealth of Virginia. If satisfied that probable cause has been established for such belief and as required by Chapter 5 (§ 19.2-52 et seq.), the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court shall issue a warrant identifying those records to be searched for and commanding the person seeking such warrant to properly serve the warrant upon the foreign corporation. A search warrant for real-time location data shall be issued if the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court is satisfied that probable cause has been established that the real-time location data sought is relevant to a crime that is being committed or has been committed or that an arrest warrant exists for the person whose real-time location data is sought.

D. A provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, including real-time location data but excluding the contents of electronic communications, to an investigative or law-enforcement officer pursuant to an administrative subpoena issued pursuant to § 19.2-10.2 concerning a violation of § 18.2-374.1 or 18.2-374.1:1, former § 18.2-374.1:2, or § 18.2-374.3 when the information sought is relevant and material to an ongoing criminal investigation.

E. When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain real-time location data without a warrant in the following circumstances:

1. To respond to the user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession; (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent; or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted;

4. To locate a child who is reasonably believed to have been abducted or to be missing and endangered; or

5. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of real-time location data concerning a specific person and that a warrant cannot be obtained in time to prevent the identified danger.

No later than three business days after seeking disclosure of real-time location data pursuant to this subsection, the investigative or law-enforcement officer seeking the information shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the facts as to why the person whose real-time location data was sought is believed to be important in addressing the emergency.

F. In order to comply with the requirements of § 19.2-54, any search of the records of a foreign corporation shall be deemed to have been made in the same place wherein the search warrant was issued.

G. A Virginia corporation or other entity that provides electronic communication services or remote computing services to the general public, when properly served with a search warrant and affidavit in support of the warrant, issued by a judicial officer or court of any of the several states of the United States or its territories, or the District of Columbia with jurisdiction over the matter, to produce a record or other information pertaining to a subscriber to or customer of such service, including real-time location data, or the contents of electronic communications, or both, shall produce the record or other information, including real-time location data, or the contents of electronic communications as if that warrant had been issued by a Virginia court. The provisions of this subsection shall only apply to a record or other information, including real-time location data, or contents of electronic communications relating to the commission of a criminal offense that is substantially similar to (i) a violent felony as defined in § 17.1-805, (ii) an act of violence as defined in § 19.2-297.1, (iii) any offense for which registration is required pursuant to § 9.1-902, (iv) computer fraud pursuant to § 18.2-152.3, or (v) identity theft pursuant to § 18.2-186.3. The search warrant shall be enforced and executed in the Commonwealth as if it were a search warrant described in subsection C.

H. The provider of electronic communication service or remote computing service may verify the authenticity of the written reports or records that it discloses pursuant to this section by providing an affidavit from the custodian of those written reports or records or from a person to whom said custodian reports certifying that they are true and complete copies of reports or records and that they are prepared in the regular course of business. When so authenticated, no other evidence of authenticity shall be necessary. The written reports and records, excluding the contents of electronic communications, shall be considered business records for purposes of the business records exception to the hearsay rule.

I. No cause of actio
electronic communicat
er's officers, employe
information, facilities,
order, warrant, admini
provisions of subsectio

J. A search warra
real-time location data
provide ongoing disclo
exceed 30 days. A co
extensions, not to exce

K. An investigative
obtain electronic comm
electronic device witho
of the device if, in orde
tions or such real-time
cation service or remo
obtain a search warra
law-enforcement office
warrant under the cir
subdivision E 5, the
device shall be conside

L. Upon issuance of
issued under this sect
Commonwealth that t
age of 18 and that not
search warrant, or o
individual, or lead to f
with evidence, the inti
jeopardize an investig
provider of electronic c
to disclose for a peri
warrant, or order and
person, other than an
may be renewed for
subsequent applicatio
proceeding. A court iss
a motion made promp
order if the informati
nature or compliance v
on such provider.

M. For the purpose
"Electronic device"
electronic communicat
mation service, inclu
locational, or direction
"Foreign corporation
place of business is lo
that makes a contrac
resident of the Comm
party in the Commonw
of authority pursuant
wealth. The making
issuance of a certificat
the foreign corporatio

I. No cause of action shall lie in any court against a provider of a wire or electronic communication service or remote computing service or such provider's officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, administrative subpoena, or subpoena under this section or the provisions of subsection E.

J. A search warrant or administrative subpoena for the disclosure of real-time location data pursuant to this section shall require the provider to provide ongoing disclosure of such data for a reasonable period of time, not to exceed 30 days. A court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

K. An investigative or law-enforcement officer shall not use any device to obtain electronic communications or collect real-time location data from an electronic device without first obtaining a search warrant authorizing the use of the device if, in order to obtain the contents of such electronic communications or such real-time location data from the provider of electronic communication service or remote computing service, such officer would be required to obtain a search warrant pursuant to this section. However, an investigative or law-enforcement officer may use such a device without first obtaining a search warrant under the circumstances set forth in subsection E. For purposes of subdivision E 5, the investigative or law-enforcement officer using such a device shall be considered to be the possessor of the real-time location data.

L. Upon issuance of any subpoena, search warrant, or order for disclosure issued under this section, upon written certification by the attorney for the Commonwealth that there is a reason to believe that the victim is under the age of 18 and that notification or disclosure of the existence of the subpoena, search warrant, or order will endanger the life or physical safety of an individual, or lead to flight from prosecution, the destruction of or tampering with evidence, the intimidation of potential witnesses, or otherwise seriously jeopardize an investigation, the court may in an ex parte proceeding order a provider of electronic communication service or remote computing service not to disclose for a period of 90 days the existence of the subpoena, search warrant, or order and written application or statement of facts to another person, other than an attorney to obtain legal advice. The nondisclosure order may be renewed for additional 90-day periods for good cause shown upon subsequent application of the attorney for the Commonwealth in an ex parte proceeding. A court issuing an order for disclosure pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

M. For the purposes of this section:

"*Electronic device*" means a device that enables access to, or use of, an electronic communication service, remote computing service, or location information service, including a global positioning service or other mapping, locational, or directional information service.

"*Foreign corporation*" means any corporation or other entity, whose primary place of business is located outside of the boundaries of the Commonwealth, that makes a contract or engages in a terms of service agreement with a resident of the Commonwealth to be performed in whole or in part by either party in the Commonwealth, or a corporation that has been issued a certificate of authority pursuant to § 13.1-759 to transact business in the Commonwealth. The making of the contract or terms of service agreement or the issuance of a certificate of authority shall be considered to be the agreement of the foreign corporation or entity that a search warrant or subpoena, which has

been properly served on it, has the same legal force and effect as if served personally within the Commonwealth.

"Properly served" means delivery of a search warrant or subpoena by hand, by United States mail, by commercial delivery service, by facsimile or by any other manner to any officer of a corporation or its general manager in the Commonwealth, to any natural person designated by it as agent for the service of process, or if such corporation has designated a corporate agent, to any person named in the latest annual report filed pursuant to § 13.1-775.

"Real-time location data" means any data or information concerning the current location of an electronic device that, in whole or in part, is generated, derived from, or obtained by the operation of the device.

History.

1988, c. 889; 2009, c. 378; 2010, cc. 319, 473, 582, 720, 721; 2011, c. 392; 2014, c. 388; 2015, cc. 43, 634; 2016, cc. 549, 576, 616; 2018, c. 667.

Editor's note.

At the direction of the Virginia Code Commission, the reference to "37.2-1000" was changed to "64.2-2000" to conform to the recodification of Title 64.1 by Acts 2012, c. 614, effective October 1, 2012.

CASE NOTES

Applicability. — Defendant's motion to suppress was properly denied because, in part, even if a detective violated 18 U.S.C.S. § 2703 and § 19.2-70.3, those statutes did not provide suppression of the evidence in federal court as a remedy. United States v. Clenney, 631 F.3d 658 (4th Cir. 2011).

Cell phone records were admissible under the business records exception, as a witness testified that they were prepared in the ordinary course of business for all customers with text messaging services and that she was the custodian of those records. Chewning v. Commonwealth, 2014 Va. App. LEXIS 82 (Va. Ct. App. Mar. 11, 2014).

Obtaining cell-site data. — Since a circuit court judge found probable cause to issue the orders for the cell-site data, both of the subject orders met and exceeded the statutory standard and did not violate defendant's Fourth Amendment rights. Reynolds v. Commonwealth, 2014 Va. App. LEXIS 213 (Va. Ct. App. May 27, 2014).

Upon remand from the Supreme Court of the United States, the Court of Appeals of Virginia determined that while Virginia's statute contained the exact language as 18 U.S.C.S. § 2703(d) and the Supreme Court of the United States determined that § 2703(d) fell short of the probable cause required for a warrant, the exclusionary rule did not apply because there was no police or governmental conduct that needed to be deterred at the time it occurred where defendant did not contend that the statutes were invalid at the time the Commonwealth obtained his cell site location information in 2012 and 2015 and both the detectives and the Commonwealth's attorney had a reasonable, good faith belief that their actions were constitutional at the time. Reed v. Commonwealth, 69 Va. App. 332, 819 S.E.2d 446 (2018).

Cell phone records. — Requested cell phone records were relevant and material to the criminal case against defendant because the records concerned a window of time during which defendant was allegedly involved in a drug buy with a known drug dealer and during which time defendant was alleged to have called the drug dealer. Moreover, the records corroborated a police detective's identification of defendant by placing defendant in the general area of the drug buy and connected defendant to the drug dealer through phone calls at the time relevant to the drug buy. Reed v. Commonwealth, 2016 Va. App. LEXIS 233 (Va. Ct. App. Aug. 30, 2016).

CHAPTER 7.
ARREST.

Section