

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA

v.

Criminal No. 3:23-cr-150

KUMIKO L. MARTIN, JR.,

Defendant.

MEMORANDUM OPINION

This matter is before the Court on the MOTION TO SUPPRESS EVIDENCE DERIVED FROM THE FLOCK CAMERA SYSTEM ("the MOTION"), ECF No. 16, and DEFENDANT'S BRIEF IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE DERIVED FROM THE FLOCK CAMERA SYSTEM ("SUPPLEMENTAL MOTION"), ECF No. 67, (collectively, "the MOTIONS") as well as the opposing and supplemental briefs, ECF Nos. 22, 67, 70, & 72. The MOTION, the SUPPLEMENTAL MOTION, the briefs, the evidence, and the arguments of counsel have been considered, and, for the reasons set forth below, the MOTION, ECF No. 16, and SUPPLEMENTAL MOTION, ECF No. 67, will be denied.

I. BACKGROUND

The INDICTMENT charges Kumiko L. Martin, Jr. ("Martin" or "Defendant") with three counts: (1) 18 U.S.C. § 1951, Hobbs Act Robbery; (2) 18 U.S.C. § 924(c), Use of a Firearm by Brandishing During and in Relation to a Crime of Violence; and (3) 18 U.S.C. § 922(g)(1), Possession of Firearm by Convicted Felon. ECF No. 1.

By the MOTIONS, Martin asks the Court to suppress evidence that led to his arrest on those charges, arguing that the Government conducted an unconstitutional search without a warrant in violation of the Fourth Amendment. ECF No. 16. For the reasons set forth below, the Court holds that no unconstitutional search occurred.

II. FINDINGS OF FACT

The testimony, exhibits offered at the evidentiary hearings and within the briefs, and cited materials provide the facts upon which the Court decides the MOTIONS. The facts are established by a preponderance of the evidence.

On April 22, 2023, at approximately 8:27 A.M., two victims were robbed at gunpoint near the intersection of 48th Street and Dunston Avenue ("Dunston Robbery") in Richmond, Virginia. The victims described the robber to police as a Black male who wore a facemask and threatened them with a blue handgun. ECF No. 22, at 2. Surveillance cameras at a nearby Valero Gas Station (the "Valero cameras") captured footage of the robber fleeing the scene in a four-door Acura sedan with a moonroof and stickers in the rear passenger windows. Id.; ECF No. 64, at 78-79.¹ The Valero cameras' footage did not capture the Acura's license-plate number. ECF No.

¹ The Valero cameras were privately-owned surveillance cameras. Privately-owned surveillance cameras from other stores in the area, including a beauty salon and 7-Eleven, also recorded the Dunston Robbery. ECF No. 22, at 2.

22, at 2. Richmond Police Department ("RPD") Detective Eric Sandlin reviewed the footage and sent to local law enforcement the details and pictures captured by the Valero cameras in a vehicle-of-interest flyer in the counties surrounding Richmond. Id. That information was also given to RPD Master Patrol Officer Richard Redford for further investigation. Id. at 3.

Using the details about the Acura that were obtained from the Valero cameras, Officer Redford accessed the Flock Safety ("Flock") database to attempt to identify the vehicle's license-plate number. ECF No. 64, at 78. Flock is a technology company that uses cameras to obtain information about the exterior of motor vehicles and temporarily stores that data to assist law enforcement in solving and responding to crime. ECF No. 16-1, ¶ 10; Why Flock, Flock Safety (last visited Sept. 16, 2024, 1:57 PM), <https://www.flocksafety.com/why-flock>. Flock relies on traditional automatic-license-plate-reader (ALPR) technology to capture and analyze vehicles' license plates. ECF No. 16-1, ¶¶ 10-12. Traditional ALPRs use high-speed, high-resolution cameras to automatically capture images of vehicles' license plates. Id. ¶¶ 12, 14. Those images are then automatically converted into alphanumeric text and uploaded onto searchable databases by using infrared illumination, computer vision, and optical character recognition to accurately identify exact license-plate numbers. Id. ¶¶ 12-26. In addition to license-plate numbers, the Flock

database also contains the time, date, and location when the picture was taken; and other information such as make, model, and color of the vehicle. Id. ¶ 29. Police can use all of this information to locate vehicles suspected of use in crimes. Id. ¶¶ 27, 30.

Flock augments and integrates this traditional ALPR technology with additional information about the exterior of the photographed vehicles that helps to more accurately identify vehicles. Id. at 6. Unlike ALPRs, photographs by Flock cameras are uploaded in full to a Cloud database that records and stores the captured data. ECF No. 65, at 5-6. This searchable data includes the photograph's date, time, and location as well as the vehicle's license plate (and absence, temporariness, or obstruction thereof), the plate's state- and/or country-of-origin, body type, make, model, color, and other "unique identifiers" such as visible toolboxes, bumper and window stickers, roof racks, and damage to the exterior of the vehicle. Id. at 9. Flock updates the software to provide additional metrics for use in querying and reviewing the database. See id. at 17, 23-25; ECF No. 64, at 16; ECF No. 16-1, ¶ 39. However, the foregoing describes the metrics that are currently available and that were used in the query and review conducted by Officer Redford in this case.

The information captured depends upon the type of Flock camera used—some of which have video and audio capabilities. ECF No. 16-

1, ¶¶ 34-38. Flock's flagship product, the Falcon, which was accessed and used by Officer Redford, is a stationary camera affixed to a pole without zoom, tilt, pan, audio, or video capabilities.² ECF No. 65, at 4-5, 10; ECF No. 16-1, ¶¶ 34-36. Falcon cameras use motion-detection technology to take snapshots of vehicles at a single point in time as they pass by the fixed camera's field of vision. ECF No. 65, at 5, 10, 25-28. However, the technology is not perfect. Oftentimes a car will pass by a Flock camera without the camera taking and recording a photograph. ECF No. 56, at 38, 47. Other times, the technology may mistake specific information captured in the photograph, such as confusing a "V" for a "W" or an "O" for a "0." ECF No. 64, at 89.

The cameras are not designed to capture pictures of humans but may do so incidentally. ECF No. 65, at 11, 18-19, 39. If that occurs, however, the database does not allow searches based on biometric or other human-based characteristics that would allow law enforcement to scan for individuals. Id. at 11-12, 39.

Flock coordinates with its customers, such as police departments, to create "deployment plans," which determine what type of camera to use and where to place those cameras. ECF No. 65, at 12-13. Flock's customers purchase the cameras and any data

² All pictures of Defendant's car were taken by Flock's Falcon cameras and therefore are only still photographs. ECF No. 74, at 19, 29.

they record. Flock installs the cameras as well as maintains and stores all data captured on its own servers. Id. at 13, 15-16. Most customers choose to place cameras in high-traffic areas or areas with greater criminal activity. Id. at 13-14. Consequently, cameras are not typically placed in a linear, ordered fashion that tracks movements of the cars but, instead, are placed in strategically chosen locations. Id. at 13, 25-26. That is the tracking system involved here.³

Flock creates a "network" between its cameras. Id. at 25; ECF No. 64, at 10, 35. This means that individual Flock customers can choose to connect their cameras and can share the data that they capture. ECF No. 64, at 35-36. So long as customers give their consent, other customers can access this data from Flock cameras in different jurisdictions or across the country. ECF No. 65, at 37-39. For instance, a police department like the RPD can access the data captured by Flock cameras owned by private and public entities such as homeowners' associations, private companies, schools, and other organizations in the Richmond area or in other jurisdictions. ECF No. 64, at 36.

At the time of the Dunston Robbery on April 22, 2023, 188 Flock cameras, owned by both public and private entities, covered

³ Without extensive camera coverage in an area, it is not typically possible to determine the exact route that a car travels throughout a day. Id. at 26-28. The tracking kind of camera coverage is not involved in this case.

an area that includes Richmond City, Chestfield County, Hanover County, Henrico County, and Colonial Heights. Id. at 23-24. Specifically, Richmond City had 66 and Chesterfield County had 52 Flock cameras at the time of the Dunston Robbery. ECF No. 74, at 17-18, 28.⁴

Flock cameras operate twenty-four hours a day, seven days a week, ECF No. 64, at 43, and—if working properly—photograph every vehicle that passes them. ECF No. 16, at 1. The retention period that Flock stores the data depends on customer contracts and the laws of the relevant jurisdiction. ECF No. 65, at 14-15; ECF No. 74, at 52-57. Some jurisdictions prohibit retention for longer than a week, whereas others allow retention for up to five years. ECF No. 64, at 47. In Virginia, the retention duration is 30 days. Id. at 44; ECF No. 65, at 15, 32. And, that is the retention duration for the vehicle information at issue in this case. ECF No. 74, at 57.

Consequently, when Officer Redford queried the Flock database for vehicles that matched the description of the Dunston Robbery suspect's car obtained from the Valero cameras, the Flock system limited its results to the 30 days preceding April 22, 2023. ECF No. 22-1, ¶ 6. Officer Redford's query returned 2,500 results

⁴ At the time of RPD Lieutenant Nicholas Castrinos' testimony on July 3, 2024, the number of Flock cameras in Richmond City had increased from 66 to at least 97 to 100. ECF No. 56, at 42; ECF No. 74, at 19, 28.

(photographs), which is the maximum that Flock's system shows per search. ECF No. 56, at 17. Officer Redford then manually reviewed those 2,500 pictures and found two of the suspect's vehicle, which Officer Redford was able to identify based on the unique stickers in the car's rear windows. ECF No. 22-2, at 3; ECF No. 56, at 17-18; ECF No. 64, at 89-90. Unlike the Valero security-camera footage, the Flock pictures also identified the vehicle as gold with a Virginia license-plate number of UAL-6525. ECF No. 22, at 3.

On April 23, 2023—the day after the Dunston Robbery—Chesterfield County police officers responded to an attempted breaking and entering, as well as an armed robbery, near the Dunston Robbery location. Id. at 2. The attempted breaking and entering occurred at a convenience store ("Your Store") at approximately 10:15 P.M. Id. Chesterfield Detective Joshua Hylton obtained security footage from the Your Store's private surveillance cameras that showed the suspect fleeing toward Reams Road after failing to have unlocked the door to the Your Store. Id. About 10 minutes after the attempted breaking and entering at the Your Store, an armed robbery occurred at a BP Gas Station ("BP"), that was located approximately three miles away from the Your Store on Reams Road. Id. The robber at the BP brandished a firearm and stole the victims' iPhones, laptop, credit cards, payroll checks, cash, and car keys. Id. at 3. Detective Hylton

reviewed footage from the BP's private security cameras, which showed the suspect wearing a yellow jacket, ski mask, and reddish-pink glove and wielding a small blue- or teal-colored gun. Id. Detective Hylton also reviewed footage from a private security camera at a nearby Food Lion, which recorded a sedan resembling the Acura pulling into the BP parking lot as well as a man in a yellow jacket exiting the car, entering the BP, and exiting and running back to the car a few moments later. Id. Upon reviewing the footage, Detective Hylton noted that the BP robber's height, weight, and clothing matched that of the Your Store perpetrator. Id.

Later, Detective Hylton searched the Flock database for images of the sedan near these crimes. Id. at 4. His search returned a picture taken by a Flock camera of an Acura with the license-plate number UAL-6525 driving on Reams Road shortly before the BP robbery. Id.; ECF No. 22-2, at 4.

Detective Hylton learned that the RPD was simultaneously investigating the Acura for the Dunston Robbery, and he began to coordinate his investigation with that of the RPD. ECF No. 22, at 4. The RPD and Chesterfield PD investigating officers traced the Acura's registration to a Breona Reid, who lived at an apartment at Lamplighter Court in Chesterfield, Virginia. Id. Then, the investigators discovered that the two pictures that Officer Redford had found on the Flock database that displayed the gold

Acura with license-plate number AUL-6525 were taken by a Flock camera located at the intersection of Stella Road and Lamplighter Court on April 22, the day of the Dunston Robbery. Id.; ECF No. 74, at 20, 30-31. Those pictures were taken at 6:21 A.M. and 8:44 A.M., the latter of which was just 17 minutes after Richmond police officers were alerted to the Dunston Robbery. Ms. Reid's Lamplighter Court address is approximately 6.8 miles, or a 13-minute drive, from the Valero near the Dunston Robbery. ECF No. 22, at 4.

Based on this information, RPD Detective Sandlin applied for a warrant to place a GPS-tracking device on Ms. Reid's Acura. Id. Magistrate Judge Robert Hearn signed the warrant on April 26, 2023, authorizing GPS tracking of the vehicle. ECF No. 64-7, at 1. On May 3, 2023, at approximately 3:25 A.M., Chesterfield police officers attached the GPS to the Acura after RPD had failed to do so. ECF No. 64, at 80; ECF No. 16, at 4.

On May 4, 2023, another robbery occurred at a Tobacco Hut on Midlothian Turnpike in Richmond, Virginia. ECF No. 64, at 80. Officers examined the Tobacco Hut's private security-camera footage, which showed the robber wearing latex gloves and carrying a blue- or teal-colored handgun. ECF No. 22, at 4. This footage also showed the robber exiting the Tobacco Hut and entering an Acura with distinctive rear-window stickers, which quickly drove off. Id.

Officers then checked the GPS-tracking data from the GPS placed on the Acura registered to Ms. Reid and discovered that the Acura was at the Tobacco Hut location before and during the robbery. ECF No. 64, at 80. The GPS tracking information showed that the Acura was then located at the Lamplighter Court apartment. Id. at 81. Chesterfield police officers surveilled the Acura that morning until they saw the driver—a man matching the robber's description—enter the Lamplighter Court apartments then return to the Acura and drive off. ECF No. 22, at 5. Officers conducted a felony traffic stop, identified the Acura's driver as Martin, and arrested him. Id.

Officers transported Martin to the RPD's Third Precinct Station where RPD Detective Marley Williams read Martin his *Miranda*⁵ rights. Id. Martin signed a form indicating that he understood his rights and that the police were interviewing him regarding the robberies and the attempted breaking and entering. Id. He waived his rights and made a statement admitting to Detective Hylton that he had committed the Tobacco Hut robbery for money to pay rent that he owed to Aaron's—a rent-to-own furniture store. Id. However, while Martin admitted to participating in the Your Store breaking-and-entering and the BP robbery, Martin

⁵ Miranda v. Arizona, 384 U.S. 436 (1966).

claimed that his father was the perpetrator.⁶ Id. He admitted to using the blue/teal firearm to rob the Tobacco Hut and that it belonged to Breona Reid. Id. He stated that the gun and some clothing that he wore during the crime were at Ms. Reid's Lamplighter Court apartment and gave consent to Detective Hylton to search the premises. Id.

Based on this confession, the private businesses' security footage, and the images of the Acura retrieved from the Flock database, RPD Detective Sandlin applied for a search warrant to search Ms. Reid's Lamplighter Court apartment. Id. at 5-6. Magistrate Judge C. Lawrence signed the warrant on May 4, 2023, allowing officers to search Ms. Reid's apartment. ECF No. 64-8, at 1. Officers executed the warrant later that day and found and confiscated a blue handgun, ammunition, wigs, clothing, and money. Id. at 2; ECF No. 22, at 6.

On November 7, 2023, Martin was indicted and charged with Hobbs Act Robbery under 18 U.S.C. § 1951, Use of a Firearm by Brandishing During and in Relation to a Crime of Violence under 18 U.S.C. § 924(c), and Possession of Firearm by Convicted Felon under 18 U.S.C. § 922(g)(1). ECF No. 1. Martin seeks dismissal of these charges, arguing that the evidence undergirding them was obtained in contravention of the Fourth Amendment, U.S. Const. amend. IV,

⁶ Martin is not charged in this case with the attempted breaking and entering of the Your Store or the BP robbery.

because the officers did not secure a warrant before accessing the Flock database. ECF No. 16, at 1. He filed a Motion to Suppress on February 20, 2024. Id. The Supplemental Motion to Suppress was filed on August 12, 2024. ECF No. 67. These Motions are before the Court after being fully briefed by both parties, ECF Nos. 16, 22, 67, 70, 72, and after several evidentiary hearings where both parties had the opportunity to present expert- and lay-witness testimony. ECF Nos. 56, 64, 65.

III. DISCUSSION

The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Historically, Fourth Amendment doctrine rested in that of common-law trespass, focusing on whether "the government 'obtains information by physically intruding on a constitutionally protected area.'" Carpenter v. United States, 585 U.S. 296, 304 (2018) (quoting United States v. Jones, 565 U.S. 400, 405-06 n.3 (2012)). In 1967, however, the Supreme Court of the United States articulated a new, complementary two-faceted standard to assess whether a search occurred under the Fourth Amendment. Katz v. United States, 389 U.S. 347 (1967). The Katz test requires courts to analyze whether, first, the person "exhibit[s] an actual (subjective) expectation of privacy and, second, that the expectation [is] one that society is prepared to recognize as

'reasonable.'" Id. at 361 (Harlan, J., concurring).⁷ If either the first (subjective) or second (objective) facet is not met, no Fourth Amendment violation has transpired. Id.; see also United States v. Jacobsen, 466 U.S. 109, 113 (1984) (noting that unreasonable searches occur "when an expectation of privacy that society is prepared to consider reasonable is infringed").

The reasonable-expectation-of-privacy standard modernizes Fourth Amendment doctrine and readies it to address challenges imposed by never-ending technological advancements. See Carpenter, 585 U.S. at 305-06. That said, the approach remains historically grounded by inquiring into "what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." Id. at 305 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925) (alterations in original)). The Fourth Amendment aims to protect the "'privacies of life' against 'arbitrary power'" and to "place obstacles in the way of a too permeating police surveillance." Id. (quoting Boyd v. United States, 116 U.S. 616, 630 (1886); United States v. Di Re, 332 U.S. 581, 595 (1948)). Therefore, as technology continues to enhance the "Government's ability to encroach upon areas normally guarded from inquisitive eyes," courts must assure that individuals maintain the "degree of privacy

⁷ While the reasonable-expectation-of-privacy standard derives from Justice Harlan's concurrence and not from the Katz majority, the Supreme Court has adopted that standard as the predominate approach. Jones, 565 U.S. at 406.

against government that existed when the Fourth Amendment was adopted." Id. (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

This analysis oftentimes requires courts to examine not just the expectations of privacy that individuals have in the privacy of their homes but so too those in public. In Knotts v. United States, the Supreme Court addressed whether government officers violated an individual's Fourth Amendment rights by monitoring a beeper's signal that they placed in a drum of chemicals that Knotts' co-conspirator ("Petschen") was transporting. 460 U.S. 276, 277-80 (1983). The beeper—along with traditional visual surveillance methods—allowed police officers to trace the drum as Petschen transported it from his place of work to a secluded cabin where Knotts operated a methamphetamine laboratory. Id. at 278-79. The Court affirmed the denial of Knotts' motion to suppress any evidence of his crimes derived from this warrantless surveillance because it "amounted principally to the following of an automobile on public streets and highways," whereon individuals have a "diminished expectation of privacy." Id. at 281. More particularly, in Knotts, the Supreme Court held that: "A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view." Id. As a result:

A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id. at 281-82 (emphasis added). The beeper merely augmented the inherent sensory faculties of police officers, the exercise of which the Fourth Amendment does not prohibit. Id. at 282. Because the beeper revealed no information that was not otherwise visible "to the naked eye," no unconstitutional search occurred. Id. at 285; see also New York v. Class, 475 U.S. 106, 106 (1986) ("The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search.'" (citing Cardwell v. Lewis, 417 U.S. 583, 588-89 (1974) (plurality opinion) (emphasis added))).

Nearly 30 years later, the Supreme Court addressed whether placing a GPS-tracking device on a vehicle and using that device to track the vehicle's movements on public streets constituted a search within the meaning of the Fourth Amendment. Jones, 565 U.S. at 402, 404. Officers used the GPS to record Jones' vehicle's movements over a four-week period, with the GPS indicating the vehicle's location at any given moment within 50-100 feet. Id. at 403. The Court did not discuss whether Jones had a reasonable expectation of privacy in the vehicle's locations on the "public

roads, which were visible to all." Id. at 406. Instead, it held that a search occurred under the trespass-theory of the Fourth Amendment because placing the GPS on Jones' car constituted a physical intrusion on a constitutionally protected area necessitating a warrant. Id. at 406 n.3.

When deciding Jones, the Court did not disturb Knotts' holding that individuals lack a reasonable expectation of privacy in their vehicles' movements when in the public sphere. Id. at 408-09, 412.⁸ So it was that, in Jones, the Supreme Court observed:

This Court has to date not deviated from the understanding that mere visual observation does not constitute a search. See Kylo, 553 U.S. at 31-32, 1215 S. Ct. 2038. We accordingly held in Knotts that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U.S. at 281, 103 S. Ct. 1081.

Jones, 565 U.S. at 412 (alterations in original). At the same time, Jones reserved for the future an assessment of whether the use of "electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." Id.

In Carpenter v. United States, the Supreme Court again had to address what protections from increasingly advanced surveillance

⁸ The Court also noted that it had not decided Knotts on a trespass theory, even though its facts closely resembled those in Jones, because "Knotts did not challenge [the physical] installation" of the beeper on his vehicle. Consequently, the Court "specifically declined to consider its effect on the Fourth Amendment analysis." Jones, 565 U.S. at 409.

technology the Fourth Amendment provides to individuals in the public sphere. 585 U.S. at 309. In Carpenter, police officers requested—without a warrant—cell-site location information (“CSLI”) from the Defendant’s cell-service providers (MetroPCS and Sprint). Id. at 301-02.⁹ CSLI provides an approximate location of a cellular device based on discrete location pings continuously sent to cell towers, regardless of whether the person is in public or private places. Id. at 301. Those pings automatically occur by the nature of the phone being turned on, without any affirmative action taken by the user to record, release, or send that data to cell servicers. Id. at 315. The servicers turned over Carpenter’s CSLI to the police. That data included 127 days’ worth of Carpenter’s movements from MetroPCS and two days’ worth from Sprint, which totaled 12,898 location pings “cataloging Carpenter’s movements” for an average of 101 data points per day. Id. at 302.¹⁰ Based on this data, police were able to place Carpenter at and near the scenes of various robberies for which they then arrested and charged him. Id. at 301-03.

⁹ The officers did apply for court orders under the Stored Communications Act, 18 U.S.C. § 2703(d), to obtain these records, which creates a different standard than the probable cause standard necessary for a warrant under the Fourth Amendment. The Court held that such orders were insufficient to access CSLI under the Fourth Amendment. Carpenter, 585 U.S. at 302, 317.

¹⁰ While MetroPCS only disclosed 127 days of data and Sprint only 2 days, officers originally requested 152 days and 7 days of data, respectively. Id. at 302.

Carpenter moved to suppress the CSLI showing his movements, arguing that the government seized the CSLI without a warrant in contravention of the Fourth Amendment. Id. at 302. The Supreme Court agreed, holding that an individual has a reasonable expectation of privacy in the "whole of their physical movements." Id. at 311 (citing Jones, 565 U.S. at 430 (Alito, J., concurring in judgment); id. at 415 (Sotomayor, J., concurring)). It reasoned that CSLI's ability to create and disclose an "all-encompassing record" of the phone-holder's whereabouts provides an "intimate window into a person's life, revealing not only [their] particular movements, but through them [their] 'familial, political, professional, religious, and sexual associations.'" Id. (quoting Jones, 565 U.S. at 415 (Sotomayor, J., concurring)). Just like the GPS-tracking in Jones, tracking one's phone using CSLI "is remarkably easy, cheap, and efficient compared to traditional investigative tools." Id. Further, the Court found that the "retrospective quality of the data . . . gives police access to a category of information otherwise unknowable" by traditional methods of surveillance. Id. at 312. And, critically, the Government need not even target a specific person for investigation—tracking by CSLI runs against everyone, providing police with a record of an eventual suspect's whereabouts for up to five years in the past. Id. at 312-13. Together, this evidence led the Court to hold that the Government violated Carpenter's

reasonable expectation of privacy in the whole of his physical movements. Id. at 313.

A brief look at Carpenter is in order to refresh our understanding of what it held, and why and how the Court limited the reach of its decision. First, we must keep in mind the question that was presented and decided. On that point, the Court said:

This case presents the question 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.

Id. at 300 (emphasis added). Second, there is the Court's response on that point, which was: "The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment." Id. at 320. Third, there is the why. On that score, the Court explained that:

[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individuals' car for a very long period.

Id. at 310 (quoting Jones, 565 U.S. at 430 (Alito, J., concurring in judgment) (emphasis added) (internal quotation marks omitted)). Therefore, the Court concluded that: "Allowing government access to cell-site records contravenes that expectation." Id. at 311. The analytical construct employed by the Court to reach that result was to examine the technological system by which the CSLI was collected and stored and to assess the extent of the surveillance

effected by that technological system. That, of course, is the construct that applies to Martin's challenge to the Flock system.

Perhaps realizing the potential far-reaching consequences of its decision, the Court was careful to note that its decision was "a narrow one." Id. at 316. In the narrowness of its holding, the Court made sure to detail the subtle, yet critical, distinctions between the type of surveillance at issue in Carpenter versus that in Knotts and Jones. Unlike the GPS tracking in Jones and the beeper tracking in Knotts, cellphones (and their CSLI) "track[] nearly exactly the movements of [their] owner[s]," acting as "almost a 'feature of human anatomy.'" Id. at 311 (quoting Riley v. California, 573 U.S. 373, 385 (2014)). Further, unlike vehicles, which individuals "regularly leave," cellphones are "compulsively" carried by their owners at practically all times. Id. While tracking a car on public thoroughfares may reveal its driver during that travel, a cellphone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." Id. (contrasting Riley, 573 U.S. at 395 (discussing the proliferation and pervasiveness of cellphone use) with Cardwell, 417 U.S. at 590 (noting that a "car has little capacity for escaping public scrutiny")). Therefore, tracking a cellphone's location "achieves near perfect surveillance" equivalent to

"attach[ing] an ankle monitor to the phone's user," which is not present when monitoring vehicular travel. See id. at 311-12.

Further, in explaining that its decision in Carpenter was "a narrow one," the Court specified that:

We do not express a view on matters not before us . . . We do not disturb the application of Smith [v. Maryland, 442 U.S. 735 (1979)] and [United States v.] Miller [425 U.S. 435 (1976), the so-called third-party doctrine cases,] or call into question conventional surveillance techniques and tools, such as security cameras.

Id. at 316. And, in explaining how the facts differed from those in Knotts, the Court in Carpenter noted that "this case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence complied every day, every moment, over several years." Id. at 315 (quoting id. at 388 (Gorsuch, J., dissenting)).

Three years later, the United States Court of Appeals for the Fourth Circuit, sitting en banc, applied Carpenter's reasoning in Leaders of a Beautiful Struggle v. Baltimore Police Department to hold that government officials' warrantless access to an aerial surveillance system that allowed them to deduce the "whole of individuals' movements" constituted an unconstitutional search under the Fourth Amendment. 2 F.4th 330, 333 (4th Cir. 2021) (en banc). There, the Baltimore Police Department ("BPD") employed the third-party Aerial Investigation Research ("AIR") program to monitor crimes in the city. Id. at 334. AIR's planes surveilled

city residents during almost all daylight hours, weather permitting, and captured a total "estimated twelve hours of coverage of around 90% of the city each day." Id. The cameras' resolution was limited to one pixel per person or vehicle, meaning they could magnify to where people and cars were individually visible, but "only as blurred dots or blobs." Id. The planes transmitted this data to servers where it was stored for 45 days. Id.

The Fourth Circuit hinged its analysis on Carpenter's solidification of the line "between short-term tracking of public movements . . . and prolonged tracking that can reveal intimate details through habits and patterns. The latter form of surveillance invades the reasonable expectation of privacy that individuals have in the whole of their movements and therefore requires a warrant." Id. at 341. It held that the AIR program more closely resembled the CSLI surveillance in Carpenter and GPS surveillance in Jones than it did the beeper surveillance in Knotts. Id. AIR's constant surveillance "yield[ed] a 'wealth of detail,' greater than the sum of . . . individual trips" and hence allowed law enforcement to retroactively deduce inherently intimate details of everyone's lives. Id. at 342 (quoting Jones 565 U.S. at 415-17 (Sotomayor, J., concurring)). The Fourth Circuit dismissed the Government's arguments that accessing AIR's database was constitutionally sound because it only showed people as

anonymous blobs and did not surveil at night. Id. Even with these breaks in the surveillance chain—which resembled similar gaps in coverage in Carpenter and Jones—the court found that law enforcement could still assemble a picture of the whole of an individual’s movements throughout their daily life. Id. at 342-43. That, the Court of Appeals held, violated the reasonable expectation of privacy that individuals possess in the whole of their movements, thereby applying Carpenter’s holding to the AIR system used in Baltimore. Id.

IV. ANALYSIS

Martin seeks to suppress the evidence and the fruits of RPD officers’ warrantless access to the Flock database as an unconstitutional search in violation of the Fourth Amendment. ECF No. 16, at 1; ECF No. 67, at 1. He argues that the Government accessing this data violated his reasonable expectation of privacy in the whole of his movements akin to Carpenter and Beautiful Struggle. ECF No. 67, at 9. He grounds this argument in the facts that the Flock system’s twenty-four-seven operation, 30-day retention period, practice of photographing all vehicles—even those of non-criminal suspects—in its vision, and network connectivity with data from Flock cameras in other jurisdictions collectively provide law enforcement with a means to intrude into individuals’ private lives that Carpenter and Beautiful Struggle prohibited absent a warrant. ECF No. 16, at 6. Further, Martin

notes that Flock's technical ability to "track" individuals continues to increase, with additional cameras being installed to cover more geography and routine software updates being implemented. ECF No. 67, at 8-9; ECF No. 72, at 4. The theory upon which the MOTIONS rest is that Flock's technological capabilities are the equivalent of the CSLI in Carpenter by noting that Flock captures an individual's movements "anytime they get in a car" just as wireless providers capture an individual's CSLI "anytime a person makes a call." Id. at 8. He also analogizes to Beautiful Struggle, where the AIR program constantly monitored individuals' movements and stored that data for 45 days, by claiming that "Flock cameras effectively record the movement of all driver-operated vehicles in the Richmond region and maintain that information for at least 30 days." Id.

To support his claim that he possessed a reasonable expectation of privacy in his movements, Martin argues that Carpenter and Beautiful Struggle evolved the traditional Katz test to a balancing test that the Supreme Court "seeks to achieve in light of advancing technology." Id. at 9. According to Martin, this purportedly new balancing test would require courts to consider the totality of a new surveillance technology's "ability to surpass ordinary expectations of law enforcement's capacity and . . . to provide enough information to deduce details from the whole of a person's movements." Id. Essentially, he asks this Court

to consider various factors that seemed important in Carpenter and Beautiful Struggle—such as the efficiency, ease, expense, and duration of the surveillance—together to decide if and when too much surveillance is enough to violate the Fourth Amendment. Based on the record in this case and using this proposed test, Martin asserts that he had a reasonable expectation of privacy because Flock’s cameras could track “the whole of his movements” in the United States. Id. at 7-8.

The Government disputes Martin’s characterizations of Carpenter and Beautiful Struggle and argues that accessing the Flock database that showed his vehicle’s movements on public thoroughfares is materially different than CSLI at issue in Carpenter and the AIR program in Beautiful Struggle. ECF No. 22, at 1. Further, the Government argues that Martin has demonstrated neither a subjective nor an objective expectation of privacy in his movements under the facts of this case. Id. at 6-7. Alternatively, the Government argues that, even if the Court were to decide that a warrantless search did in fact occur, the evidence should not be suppressed because the Government relied in good faith on valid search warrants and binding caselaw at the time of the search. Id. at 7.

The Government first contends that “Martin’s motion neither identifies nor describes any evidence supporting a subjective expectation of privacy.” Id. (citing ECF No. 16, at 1-6). Next,

the Government argues that, even if Martin "could show that he had such an expectation, it would not have been objectively reasonable." Id. The Government focuses on three main "possibilities" where a potential reasonable (objective) expectation of privacy could exist. Id.; ECF No. 71, at 7. The first possibility, the Government posits, is the expectation of privacy in Martin's car's license-plate number. The Government argues that, because state law requires their public display, license plates cannot provide the basis for a reasonable expectation of privacy. ECF No. 22, at 8 (citing Class, 475 U.S. at 114; United States v. George, 971 F.2d 1113, 1120 (4th Cir. 1992) ("[O]ne does not have a reasonable expectation of privacy in the visible exterior parts of an automobile that travels the public roads and highways.")). Second, the Government relies on Knotts and Cardwell to argue that Martin could not have a reasonable expectation of privacy in pictures of his car while it was on public roads because he "voluntarily conveyed" his movements to "anyone who wanted to look." Id. at 8-9 (citing Knotts, 460 U.S. at 281; Cardwell, 417 U.S. at 590).

Third and finally, the Government contends that Martin did not have a reasonable expectation of privacy in the "totality of his movements" within the reach of Carpenter and Beautiful Struggle because the Flock system is unlike the systems at issue in Carpenter and Beautiful Struggle. Id. at 9. The Government relies

on a focused reading of the facts to dispute Martin's contention that police can use Flock to "track" or "monitor" Martin's movements. Id. That's because the law enforcement officers in this case only saw three photographs of Martin's car in their search of Flock's database. There is no indication that Flock recorded any other photographs of Martin's car within the timeframe for which police searched. Id. at 9-10. The Government cites to cases from other jurisdictions in which courts have held that similar ALPR databases do not raise Fourth Amendment reasonable-expectation-of-privacy concerns. Id. at 10-12 (citing United States v. Rubin, 556 F. Supp. 3d 1123, 1124 (N.D. Cal. 2021) (denying motion to suppress location data of Defendant's vehicle obtained by a warrantless search that put him at the scene of a robbery because there was "no reason to believe that the database provided a detailed log of [the Defendant's] movements" and therefore "revealed little more than where [the Defendant] was probably living"); United States v. Porter, 2022 WL 124563, at *1 (N.D. Ill. Jan. 13, 2022) (denying motion to suppress location data of the Defendant's vehicle obtained by a warrantless search that put him at the scene of various robberies because "the database query response did not reveal intimate details of [the Defendant's] daily life, nor did it track his every movement"; instead, it merely "produced images of [the Defendant's] vehicle at public locations")); see also, e.g., United States v. Jiles, 2024 WL

891956, at *16-19 (D. Neb. Feb. 29, 2024); United States v. Bowers, 2021 WL 4775977, at *2-4 (W.D. Pa. Oct. 11, 2021). Unlike in Carpenter and Beautiful Struggle, where law enforcement accessed vast amounts of data about the defendants' movements and therefore intimate details of their lives, three snapshots taken of Martin's vehicle in the public sphere do not provide such an intrusive window into Martin's life. Id. at 12-16; ECF No. 71, at 12-17. To further support this contention, the Government relies on a recent decision by the Fourth Circuit, which held that no Fourth Amendment search occurred where law enforcement accessed, without a warrant, voluntarily disclosed cellular location data of a defendant's "individual trip viewed in isolation." United States v. Chatrie, 107 F.4th 319, 330-31 (4th Cir. 2024).

In his final Reply Brief, Martin refutes all of the Government's contentions respecting his claimed reasonable expectation of privacy. ECF No. 72, at 1-6. He argues that Flock's capabilities are far more than those of traditional ALPRs in cases like Rubin and Porter—where officers already had a license-plate number before accessing the ALPR systems. Instead, Martin argues, like cell-towers with CSLI, Flock's "network of cameras" capture every person's vehicle and its movements across the United States. Id. at 2, 4. He also relies on dicta in Knotts and Carpenter that Flock would fall into some forms of 24-hour surveillance that the Supreme Court noted might produce constitutional concerns. Id. at

3. In particular, he says that: “[T]he Carpenter Court explicitly distinguished the Knotts holding when it highlighted its earlier reservation in Knotts that ‘different constitutional principles may be applicable if twenty-four hour surveillance of any citizen of this country [was] possible.’” Id. (citing Carpenter, 585 U.S. at 310 (quoting Knotts, 460 U.S. at 284)). Lastly, Martin again asserts that “Flock’s broad surveillance system,” with its at least 188 cameras and twenty-four-seven surveillance abilities, does record enough of his movements that it is sufficiently akin to the systems in Carpenter and Beautiful Struggle to be governed by those cases. Id. at 4-5.

* * *

To prevail on a motion to suppress, a defendant must demonstrate, by a preponderance of the evidence, the existence of an expectation of privacy that was reasonable and that was infringed. Katz, 389 U.S. at 361 (Harlan, J., concurring); Rawlings v. Kentucky, 448 U.S. 98, 104 (1980); United States v. Castellanos, 716 F.3d 828, 832-33 (4th Cir. 2013). To begin, Carpenter and Beautiful Struggle cannot reasonably be read as casting off decades of precedent in the Fourth Amendment arena for a newfound balancing test as Martin argues, ECF No. 67, at 9, and the Court declines the invitation to do so here. Martin must therefore demonstrate that he had both a subjective and an objective expectation of privacy in his movements in this case. Katz, 389 U.S. at 361

(Harlan, J., concurring). For the reasons that follow, he has not done so. Therefore, the MOTIONS are denied.¹¹

A. Subjective Expectation of Privacy

Courts, including the Supreme Court, often do not discuss clearly (and sometimes not at all) the facts supporting an individual's subjective expectation of privacy. This has led some to suggest that the subjective facet of Katz's reasonable-expectation-of-privacy standard has become a hollow shell, with the sole focus now on the objective facet. Carpenter, 585 U.S. at 346 (Thomas, J., dissenting) (citing Orin S. Kerr, Katz Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015)); see Morgan Cloud, Pragmatism, Positivism, and Principles in Fourth Amendment Theory, 41 UCLA L. Rev. 199, 250 (1993) ("Conceptually, [Katz's] first prong is perhaps the most nonsensical premise in fourth amendment law. The first prong cannot mean what it literally says. The scope of a fundamental constitutional right cannot depend upon the subjective beliefs of an individual citizen."). As a conceptual notion, that view may have some merit, but, in practice, a district court is obligated to apply the standard as laid out in Katz and as instructed

¹¹ Because no Fourth Amendment search occurred, it is not necessary to address whether the Government's argument that the Good Faith exception to a warrantless search applies in this case.

thereupon by the released decisions of the Fourth Circuit and the Supreme Court. Therefore, assessment of the MOTIONS must begin by determining whether Martin has shown that he had a subjective expectation of privacy in the exterior of his vehicle and its relevant movements in plain view to any who would look as captured by the Flock cameras.

Individuals show a subjective expectation of privacy when they can "demonstrate that [they] personally [have] an expectation of privacy" in that which is searched. Minnesota v. Carter, 525 U.S. 83, 88 (1998) (citing Rakas v. Illinois, 439 U.S. 128, 143-44 (1978)). That demonstration usually entails taking steps to conceal or keep private activities from the public's peering eyes. 1 Wayne R. LaFare, Search and Seizure: A Treatise on the Fourth Amendment § 2.1(c) (6th ed. 2024) (referencing Eric Dean Bender, Note, The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?, 60 N.Y.U. L. Rev. 725, 753-54 (1985)). And, of course, the Fourth Amendment itself tells us that we can expect privacy in our "persons, houses, papers, and effects." U.S. Const. amend. IV. A vehicle can be considered as within the term "effects," but, as explained above, the expectation of privacy in the exterior of a vehicle traveling on public roads is informed by decisional law.

Martin has presented no evidence in the record on his subjective expectation of privacy. As the Government notes in its

Response Brief, ECF No. 22, at 7, Martin does not assert or provide much at all of a factual basis for his subjective expectation of privacy in his vehicle or his movements. Indeed, when pressed at oral argument, Defense counsel cited to only one fact in the evidentiary record that was said to support Martin's subjective expectation of privacy: RPD Detective Sandlin's testimony regarding Martin's arrest on the day of the Tobacco Hut robbery. ECF No. 74, at 6-7. Detective Sandlin testified that, on that day, the police used GPS tracking (authorized by a warrant, which is not challenged) to locate Martin's vehicle at the Lamplighter Court apartment complex. After he exited the complex, Martin entered the Acura, which the officers surveilled for a brief period before making a felony traffic stop and arresting him. ECF No. 22, at 5; ECF No. 64, at 81. The Court cannot understand how that testimony is probative of Martin's subjective expectation of privacy in the exterior of his vehicle traveling on public roads.

The Court sees two possibilities on which Martin might claim a subjective expectation of privacy on these facts. Neither is persuasive. First, it could be that Martin subjectively believed that this surveillance implicated his expectation of privacy in his home. It is quite true that individuals have a constitutionally recognized expectation of privacy in their homes. Silverman v. United States, 365 U.S. 505, 511 (1961) (citing Boyd v. United States, 116 U.S. 616, 626-30 (1886)); Katz, 389 U.S. at 516

(Harlan, J., concurring). This principle extends, in many instances, to the curtilage of the home. California v. Ciraolo, 476 U.S. 207, 212-13 (1986). However, the record here does not demonstrate a warrantless intrusion into the home or curtilage of the home. The police did wait outside the Lamplighter Court apartments to see who would enter the GPS-tracked vehicle, but such wait-and-see surveillance does not implicate expectations of privacy in the home itself. Id. at 213. This leads to the second potential basis for Martin's claimed subjective expectation of privacy: one while driving his vehicle. However, here too, well-established precedent forecloses such a possibility. There is simply no expectation of privacy in the exterior of one's vehicle, Class, 475 U.S. at 106, or while driving it on public thoroughfares. Knotts, 460 U.S. at 281-82.

On this record, it cannot be said that Martin has established a subjective expectation of privacy while driving his car on public roads. And, if the traditional formulation of Katz is applied, that ends the inquiry and the MOTIONS can be denied for that reason.

Ordinarily, it is preferable to articulate a single basis for decision and, conversely, to refrain from making alternative holdings. Karsten v. Kaiser Found. Health Plan of the Mid-Atl. States, Inc., 36 F.3d 8, 11-12 (4th Cir. 1994). However, considering that the subjective facet of the Katz test is not oft-

discussed and is not addressed by the majority opinion in Carpenter or Beautiful Struggle, see generally Carpenter, 585 U.S. 296; Beautiful Struggle, 2 F.4th 330, it is preferable in this case to analyze the MOTIONS under the objective expectation of privacy facet of Katz as well. To that we now turn.¹²

B. Objective Expectation of Privacy

Individuals have an objective expectation of privacy when they can demonstrate that the expectation is one that "society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361 (Harlan, J., concurring). Courts must decide what exactly is society's modern understanding of the interests it views deserve "protection from government invasion." Oliver v. United States, 466 U.S. 170, 178 (1984). As Justice Harlan instructed, this requires considering whether surveillance practices constitute "more extensive intrusions that significantly jeopardize [individuals'] sense of security" than necessary. White, 401 U.S.

¹² The Court also takes note of the significant body of scholarly work and judicial precedent that suggest that the subjective facet of the Katz framework should not end the Fourth Amendment analysis but instead that courts should also consider the objective facet. See LaFave, supra § 2.1(c); Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384 (1974); United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must . . . transcend the search for subjective expectations Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present."); Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

at 786-87 (Harlan, J., dissenting). Martin has not met his burden to demonstrate that he had an objective expectation of privacy warranting suppressing the evidence at issue.

Martin alleges that society has not accepted constant government monitoring and tracking of individuals' movements that he alleges occurred in this case. He relies principally on Carpenter and Beautiful Struggle. In those cases, the Supreme Court and the Fourth Circuit, respectively, held that individuals do possess a reasonable expectation of privacy in the "whole of their physical movements." Carpenter, 585 U.S. at 310 (referencing for support Jones, 565 U.S. at 430 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in judgment); id. at 415 (Sotomayor, J., concurring)); Beautiful Struggle, 2 F.4th at 342. Martin argues that these cases adopted a new "balancing test" that considers factors such as the ease, efficiency, expense, duration, and retrospective nature of the surveillance technique to decide whether accessing that technology violates one's reasonable expectation of privacy in their movements. But that is not what the Supreme Court or the Fourth Circuit said, and this Court declines to accept that proposition here. Indeed, more recently, the Fourth Circuit addressed a similar set of facts under this theory, which has become known as the "Mosaic Theory" of the Fourth Amendment, and explicitly rejected it. Chatrie, 107 F.4th at 333-35. Carpenter, Beautiful Struggle, and Chatrie all instruct that

the traditional test under Katz is to be used to assess whether Martin has established that he had a reasonable expectation of privacy in his movements.

The record in this case is meaningfully different from the facts in both Carpenter and Beautiful Struggle. In Carpenter, law enforcement officials obtained over 100 days of location data from Carpenter's cellphone to place him at the charged-robberies' locations. With that data, police were able to see Carpenter's (almost) exact position at practically any given time of day. Wherever his cellphone went, it recorded those movements. Carpenter, 585 U.S. at 301-03. It not only captured his movements while traveling in the public square, where he would typically not receive Fourth Amendment protection, see Knotts, 460 U.S. at 281-82, but so too his movements into, out of, and between private locations and buildings. Carpenter, 585 U.S. at 302-03.¹³ In total, this allowed officers to view almost 13,000 "location points cataloging Carpenter's movements." Id. at 302. Such an "all-encompassing record" provided an "intimate window into [Carpenter's] life, revealing not only his particular movements,

¹³ While an individual "does not surrender all Fourth Amendment protection by venturing into the public sphere" and those things that an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," Carpenter, 585 U.S. at 310 (quoting Katz, 389 U.S. at 351-52), it remains true that those protections at least do not extend to one's driving a vehicle on the public thoroughfares. Knotts, 460 U.S. at 281-82.

but through them his 'familial, political, professional, religious, and sexual associations.'" Id. at 311 (quoting Jones, 565 U.S. at 415 (Sotomayor, J., concurring)).

Beautiful Struggle involved a similar all-encompassing surveillance program that allowed law enforcement to track and monitor every Baltimore resident's movements during daylight hours, every day. 2 F.4th at 333-34. That monitoring began once individuals left their homes. Whether they drove or walked somewhere, it followed them to each new garage entered or door knocked on. It only ceased once night fell—typically when individuals were already back at home for the night. Id. at 334-45, 343. This monitoring persisted, day in and day out, so that law enforcement could "use AIR data to track a person's movements from a crime scene to, eventually, a residential location where the person remains. They could then look through time and track movements from that residence. They could use any number of context clues to distinguish individuals and deduce identity." Id. at 343. Allowing the police warrantless access to such technology and data "open[ed] 'an intimate window' into a person's associations and activities" and therefore violated Plaintiffs' reasonable expectations of privacy in the "whole of their movements." Id. at 342 (quoting Carpenter, 585 U.S. at 311-13).

Compare Carpenter and Beautiful Struggle with the facts at issue in Chatrie. There, the Fourth Circuit held that Chatrie did

not have a reasonable expectation of privacy in his movements when law enforcement accessed only two hours' worth of his "Location History" data that was voluntarily disclosed to his cellular provider. Chatrie, 107 F.4th at 330. This data placed him at and near the scene of a bank robbery around the time that it occurred. Police charged him with that robbery. Id. at 324-25. Police saw only a snapshot of Chatrie's location on an "individual trip viewed in isolation, which, standing alone, was not enough to enable[] deductions about what [Chatrie] does repeatedly, what he does not do, and what he does ensemble." Id. at 330 (quoting Beautiful Struggle, 2 F.4th at 342 (quoting United States v. Maynard, 615 F.3d 544, 562-63 (D.C. Cir. 2010) (alterations in original))) (internal quotation marks omitted). The Fourth Circuit held that the access to Chatrie's "short-term public movements" was more akin to Knotts—where the Supreme Court found no reasonable expectation of privacy—than to the monitoring in Carpenter, Jones, or Beautiful Struggle. Id. (referencing Knotts, 460 U.S. at 281).¹⁴

¹⁴ The Fourth Circuit also equated Chatrie's circumstances to other Supreme Court cases that held that there was no reasonable expectation of privacy when an individual "voluntarily" revealed their bank records or telephone call logs to banks and telephone companies. Miller, 425 U.S. at 442 (bank records); Smith, 442 U.S. at 742 (telephone call logs). Those cases involve the "third party doctrine," regarding the voluntary disclosure of information to other parties vitiating Fourth Amendment privacy rights, which the Court believes is not at issue in this case other than the extent to which it is implicated in Knotts.

Consequently, Chatrie had no objective expectation of privacy in this information. Id.

No such "dragnet type law enforcement practice[]," Knotts, 460 U.S. at 284, of the kind before the courts in Carpenter and Beautiful Struggle has occurred in this case. Instead, this case far more resembles Knotts and Chatrie. Martin has allegedly engaged in three robberies and one breaking and entering.¹⁵ While private surveillance cameras, such as from a Valero and 7-Eleven, photographed his vehicle at or near Martin's various alleged criminal endeavors, only three Flock cameras captured one picture each of the exterior of the Acura at different locations. ECF No. 22, at 2. Two of those pictures were taken when Martin was leaving and entering the Lamplighter Court apartments on April 22, 2023, allegedly leaving to go to and then returning from the Dunston Robbery. The other photograph was taken by a Flock camera on Reams Road after the failed breaking and entering into the Your Store. Id. at 4. Out of the approximately 2,500 pictures that Officer Redford looked through on the Flock database, those are the only ones that captured Martin's vehicle in the 30-day timeframe in which Flock retains the data. When reviewing the Flock database, police officers could not see the route Martin allegedly took to and from the robberies because the Flock system does not record

¹⁵ To reiterate, however, the Government has only charged Martin with the Tobacco Hut robbery. ECF No. 1.

the totality of one's movements. None of the almost 200 other Flock cameras in the area photographed Martin's vehicle. That, of course, is part of the system's design, not a defect. The Flock system is not meant to "track" or "monitor" the entirety of an individual's movements during a particular car trip, much less through the activities of their daily life. The Flock cameras are "strategically" placed to capture images of locations, not individuals, that are known as historically high-traffic or high-crime areas. ECF No. 65, at 12-14, 25-28. The three individual snapshots of Martin's brief location at specific times hardly rise to the level of persistent, unceasing public surveillance that the courts found troublesome in Carpenter and Beautiful Struggle. The facts in the record simply do not support a reasonable expectation of privacy in Martin's movements within the reasonings of Carpenter or Beautiful Struggle.

Martin, perhaps recognizing the factual weakness of his claim, exhorts the Court to think about the proverbial "big picture" dangers purportedly inherent in Flock. He claims that Flock cameras create an interconnected web, or "network," of cameras that allow law enforcement to track individuals across jurisdictions—even across the entire United States. If more cameras and advanced search capabilities are added, says Martin, this threat will only grow. ECF No. 72, at 2-5. The future is uncertain, however, and courts have been historically inept at

predicting it. Whatever might happen in the future is simply neither known nor now knowable.

In the present and on the record here, Martin never crossed into other jurisdictions to commit his alleged crimes. No Flock cameras captured him in different jurisdictions in Virginia, let alone different states across the country. Further, an individual can take a single trip in Richmond and never pass by a single Flock camera—or, even if they did, the camera may fail to take the vehicle's picture for myriad reasons. ECF No. 56, at 38, 47. To say that a web of these cameras monitors a vehicle's movements across the entirety of the United States, or even over a smaller geographic area covering multiple jurisdictions, is a conclusion that this record does not support. It certainly did not occur in this case. In no sense does the technology, at present, rise to the level of all-encompassing surveillance threatened by GPS tracking, CSLI, or the AIR program.¹⁶

¹⁶ In Commonwealth v. Bell, the Circuit Court of the City of Norfolk, Virginia, reached a different conclusion and thereupon held that law enforcement's access to the Flock database without a warrant violated the defendant's reasonable (objective) expectation of privacy. 2024 Va. Cir. LEXIS 77, at *5-10 (May 10, 2024). However, that decision fell into the same traps that Martin seeks to lay before the Court today. There, the State court found that, by accessing Flock's 172 cameras in the City of Norfolk, Virginia, law enforcement was able to track and monitor individuals' movements throughout the entire city. Id. at *2. To the court in Bell, this constituted a "dragnet over the entire city." Id. at *9 (citation omitted). Much of the reasoning undergirding that decision rests on the court's fears about

Moreover, the Court agrees with the Government that, to the extent Martin claims a reasonable expectation of privacy in his vehicle and license plate, Knotts disposes of that contention. Knotts specifically held that individuals do not have a reasonable expectation of privacy in their vehicle's movements when driving

"the many ways in which [Flock's system] could be abused" in the future. Id. at *8. But that is not the constitutional standard that Katz or Carpenter and Beautiful Struggle require. These cases require courts to consider the facts of the cases at hand to determine whether warrantless access to that technology and data violates individuals' reasonable expectations of privacy—not whether it will do so in the future.

Two more recent decisions from the same State court have come to the opposite conclusion on virtually the same facts. Commonwealth v. Robinson, 2024 Va. Cir. LEXIS 104, at *16-21 (June 26, 2024); Commonwealth v. Roberson, 2024 Va. Cir. LEXIS 126, at *12-14 (Aug. 23, 2024). In Robinson, the State court correctly noted that its inquiry was limited to the "circumstances present here," rather than speculating about the future. 2024 Va. Cir. LEXIS 104, at *16. From there, the court noted that each of the 172 Flock cameras in Norfolk target only "a single lane of traffic [and] capture only a very tiny fraction of the city's roadways." Id. at *18. Those cameras are targeted at vehicles—not individuals—and photograph them at "discrete dates and times," rather than tracking their travels throughout the city. Id. at *17-18. It concluded that the "system does not provide anything close to continuous tracking and relies on a vehicle passing by the relatively few camera locations dispersed throughout the city," which rendered the "FLOCK system . . . not analogous to long-term GPS positioning, ongoing CSLI geolocation, or constant aerial surveillance." Id. at *19. Finally, as does this Court today, the court in Robinson limited its holding to the present facts: how Norfolk's Flock system was "currently configured and only under the specific factual circumstances of th[e] case, including the limited number of cameras and the inability to continuously track vehicles." Id. at *21. The State court in Roberson conducted an identical analysis to that in Robinson and reached the same outcome. 2024 Va. Cir. LEXIS 126, at *13-14.

that vehicle on public streets, highways, and thoroughfares. 460 U.S. at 281-82. Just as in Knotts, Martin drove his vehicle on the public streets of Richmond City and Chesterfield County so that "anyone who wanted to look" could see his location at the times that the Flock cameras took photographs of his vehicle. Id. at 282.

Martin attempts to differentiate Knotts and other persuasive precedent on which the Government relies. To distinguish Knotts, he points to Carpenter's supportive citation to dicta in Knotts that states: "[D]ifferent constitutional principles may be applicable if 'twenty-four hour surveillance of any citizen of this country [were] possible.'" Carpenter, 585 U.S. 306-07 (quoting Knotts, 460 U.S. at 283-84) (second alteration in original)). However, while Flock cameras do operate twenty-four hours a day, seven days a week, they do not actually surveil individual citizens for that duration. As has been stated, they do not track or monitor the whole of an individual's movements akin to the aerial monitoring in Beautiful Struggle or provide constant location information of individuals as in Carpenter. The Flock camera system did not surveil anyone, nor does it have that capacity at present. So, the reference to Knotts on which Martin relies has no bearing on the case at hand.

Further, Martin's attempt to distinguish decisions from other courts respecting access to ALPR systems falls flat. The Government

points to several decisions from other circuits that hold that collecting license-plate numbers and accessing ALPR systems do not violate one's reasonable expectation of privacy. See, e.g., Meeks v. McClung, 2023 WL 8791686, at *7 (S.D. W.Va. Dec. 19, 2023); Becerra v. City of Albuquerque, 2023 WL 7321633, at *2 (10th Cir. Nov. 7, 2023); United States v. Miranda-Sotolongo, 827 F.3d 663, 667-68 (7th Cir. 2016); United States v. Diaz-Castaneda, 494 F.3d 1146, 1151 (9th Cir. 2007); United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006). Martin argues that those decisions are inapposite here because law enforcement in those cases had the suspects' license-plate numbers before accessing the relevant ALPR system, whereas, in this case, police officers did not have the Acura's license plate number before accessing the Flock system. ECF No. 72, at 2. That distinction is without meaning here. True, law enforcement did not have the Acura's license-plate number, but they did have other information about Martin's vehicle that was obtainable through naked-eye observation. Police queried the Flock database to look for sedans with distinctive rear-window stickers on the exterior of the vehicle because of information obtained from the Valero's video surveillance. Those stickers are just as open to public viewing as a displayed license plate. "The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search.'" Cardwell, 417 U.S. at 588-89. It is correct that the Flock system provides more

identifiable search characteristics for its database than traditional ALPRs, but all of those vehicle characteristics are just as visible to the public as a license plate. Law enforcement's access to the Flock database based on that information rather than Martin's license-plate number does not suddenly create a reasonable expectation of privacy to that information. In sum, the Court agrees with the other decisions cited by the Government that individuals have no reasonable expectation of privacy in their license-plate number based on the facts in the record.¹⁷

In the modern era, it seems as though many street corners have a camera. Every day, individuals drive past surveillance

¹⁷ The Court recognizes that there has been an explosion of scholarly work on the constitutionality of ALPR systems in the wake of Carpenter. See, e.g., Stephanie Foster, Note, Should the Use of Automated License Plate Readers Constitute a Search After Carpenter v. United States?, 97 Wash. U. L. Rev. 221 (2019); Yash Dattani, Note, Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces, 24 Vand. J. Ent. & Tech. L. 749 (2022); Mark Atwood, Note, Automated License Plate Readers: A Government Tool When Left Unchecked Will Proliferate the Power of the Nanny State by Unconstitutionally Intruding on Our Privacy in Associations, 32 Geo. Mason U. Civ. Rts. L.J. 329 (2022); William K. Rees, Note, Enhancing Law Enforcement or Compromising Privacy? The Problem with South Carolina's Use of Automatic License Plate Readers, 75 S.C. L. Rev. 727 (2024); Samantha E. Talieri Pernicano, Note, In Sight, Out of Mind: A Fourth Amendment Framework for Analyzing Utility Pole Camera Surveillance, 101 U. Det. Mercy L. Rev. 213 (2024). However, while Flock shares, and augments, many features of traditional ALPRs, the use of the Flock database in this case does not rise to the level of surveillance that these scholars argue exists. The Court decides to follow the rather settled caselaw in this area that holds that these systems do not implicate Fourth Amendment concerns.

cameras, including tollbooth cameras, private security cameras, CCTV cameras, ALPRs, traffic light cameras, poll cameras, or Flock cameras. Their installation and use is not particularly new.¹⁸ As a society, we have come to expect the public surveillance of our vehicle as we travel on public roads. We understand that, at any given time in public, a camera may take a picture of our vehicle. While admittedly different in extent, this type of surveillance method is no different than what was possible in the "precomputer age." Jones, 565 U.S. at 418-19 (Alito, J., concurring in judgment). More importantly, these cameras provide no greater

¹⁸ 'Camera on Every Corner': Protection or Invasion?, ABC News (July 27, 2007, 1:00 PM), <https://abcnews.go.com/WN/story?id=3421720&page=1>; Allison Linn, Post 9/11, Surveillance Cameras Everywhere, NBC News (Aug. 23, 2011, 7:38 AM), <https://www.nbcnews.com/id/wbna44163852>; Steve Henn, In More Cities, a Camera on Every Corner, Park and Sidewalk, NPR (June 20, 2013, 2:57 AM), <https://www.npr.org/sections/alltechconsidered/2013/06/20/191603369/The-Business-Of-Surveillance-Cameras>; Liza Lin & Newley Purnell, A World with a Billion Cameras watching You Is Just Around the Corner, Wall St. J. (Dec. 6, 2019, 1:00 AM), <https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402>; Sidney Fussell, The All-Seeing Eyes of New York's 15,000 Surveillance Cameras, Wired (June 3, 2021, 12:01 AM), <https://www.wired.com/story/all-seeing-eyes-new-york-15000-surveillance-cameras/>; Brian X. Chen, Security Cameras Make Us Feel Safe, but Are They Worth the Invasion?, N.Y. Times (last updated Nov. 15, 2022); Chris Horne, Virginia Beach Installs Controversial License Plate Readers, WAVY (last updated May 7, 2024, 1:01 PM), <https://www.wavy.com/news/local-news/virginia-beach/virginia-beach-installs-controversial-license-plate-readers/>;


information other than that which is available "to the naked eye." Knotts, 460 U.S. at 285. The cameras merely augment the same inherent sensory faculties of law enforcement that have existed since the Founding. Id. at 282. And the Flock database simply allows for an efficient review of those exterior images and the information they depict. On this record, RPD and Chesterfield police officers did not violate any reasonable expectation of privacy by accessing the Flock system to review images of the Acura's exterior and using the information thereby obtained to secure the license plate registered to the Acura and then using the license-plate number to locate Martin.

V. CONCLUSION

The Court is cautious to not hinder law enforcement's use of modernizing surveillance capabilities in the public sphere lest the Court "embarrass the future." Carpenter, 585 U.S. at 316 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944) (internal quotation marks omitted)). This Court must rule on the facts as they are and may not speculate about what the future may hold for Flock's capabilities. Today's ruling is limited to the facts of this case as they are at the time of this ruling, including the limited number of Flock cameras in the Richmond area and the limited number of pictures taken of the exterior of Martin's vehicle. Accessing Flock's database, which captured only three photographs of Martin's vehicle during the relevant 30-day period,

did not allow law enforcement to track or monitor the "whole of [Martin's] physical movements," id. at 310, and therefore was not a search under the Fourth Amendment. Consequently, the Court does not consider the Government's alternative argument that the Good Faith exception to the Fourth Amendment's warrant requirement applies. Martin's MOTION, ECF No. 16, and SUPPLEMENTAL MOTION, ECF No. 67, will be DENIED.

It is so ORDERED.

/s/ 

Robert E. Payne
Senior United States District Judge

Richmond, Virginia
Date: October 11, 2024