

Virginia State Crime Commission
Virginia ALPR Opinions
November 14, 2024

Opinions denying a defendant's motion to suppress a warrantless search of ALPR data:

- *Commonwealth v. Eddie Robinson*, Norfolk Circuit Court (July 26, 2024).
 - Charges: burglary (x9), felony attempt to obtain money by false pretenses, felony larceny of lottery tickets, grand larceny (x2), petit larceny (x7), and possession of a firearm by a convicted felon.
- *Commonwealth v. Jonah Leon Adams*, Chesterfield County Circuit Court (Aug. 1, 2024).
 - Charges: aggravated murder of multiple persons, aggravated murder of a person under age 14 (x3), murder - first degree (x4), use of a sawed off shotgun in a crime (x4), use of a firearm in a felony (x4), armed burglary with intent to commit murder, and wear body armor while committing a crime (x4).
- *Commonwealth v. Isaiah Roberson*, Norfolk Circuit Court (Aug. 23, 2024).
 - Charges: murder - first degree, murder - second degree, and use of a firearm in the commission of a felony.
- *U.S. v. Kumiko L. Martin, Jr.*, Federal Eastern District Court (Oct. 11, 2024).
 - Charges: robbery, use of a firearm by brandishing during and in relation to a crime of violence, and possession of a firearm by a convicted felon.
- *Commonwealth v. Javon Jerome Reap*, Norfolk Circuit Court (Oct. 16, 2024).
 - Charges: murder - second degree, conspiracy to commit second degree murder, and use of a firearm in the commission of a felony.

Opinion granting a defendant's motion to suppress a warrantless search of ALPR data:

- *Commonwealth v. Jayvon Antonio Bell*, Norfolk Circuit Court (May 10, 2024).
 - Charges: robbery by using or displaying a firearm, use of a firearm in felony, and conspiracy to commit robbery by using or displaying a firearm.

Virginia Supreme Court holding that the Fairfax County Police Department's use of ALPR to passively collect data did not violate Virginia's Government Data Collection and Dissemination Practices Act (§§ 2.2-3800 to 2.2-3809):

- *Neal v. Fairfax County Police Department*, 299 Va. 253, 849 S.E.2d 123 (Va. Sup. Ct., Oct. 22, 2020).

Commonwealth v. Robinson

Circuit Court of the City of Norfolk, Virginia

July 26, 2024, Decided

Criminal Docket Nos.: CR24000221 and CR24000402

Reporter

2024 Va. Cir. LEXIS 104 *

Commonwealth v. Eddie Robinson

Counsel: [*1] David A. Johnson, Esquire, Norfolk
Commonwealth's Attorney's Office, Norfolk, Virginia.

Christopher M. Bettis, Esquire, Norfolk Public
Defender's Office, Norfolk, Virginia.

Judges: David W. Lannetti, Judge.

Opinion by: David W. Lannetti

Opinion

Today the Court rules on Defendant Eddie Robinson's "Motion to Suppress" evidence, consisting of an image of Robinson's vehicle obtained without a warrant by an automated license plate reader ("ALPR") and, as a result, all subsequent searches of Robinson's residence and property (the "Motion to Suppress"). More specifically, Robinson claims that obtaining the image without a warrant violated his constitutional rights under the U.S. Constitution and the Constitution of Virginia, as well as section 19.2-266.2 of the Code of Virginia.¹ The Court finds that although Robinson has standing to challenge the constitutionality of the image taken of his vehicle, obtaining the image did not, under the unique circumstances present here, violate a reasonable expectation of privacy. Therefore, the Court DENIES the Motion to Suppress.

¹ Although Robinson in the introduction of his Motion asserts claims under the Fourth and Fourteenth Amendments of the U.S. Constitution; Article I, Sections Eight, Ten, and Eleven of the Constitution of Virginia; and section 19.2-266.2 of the Code of Virginia, his argument in the Motion and at the related suppression hearing focused entirely on "the Fourth Amendment." For the purposes of this Motion, the Court analyzes Robinson's claims under the Fourth. Amendment of the U.S. Constitution and [Article 1, Section 10 of the Constitution of Virginia](#).

Background

According to Robinson, and not contested by the Commonwealth, the Norfolk Police Department installed 172 automatic license plate reader ("ALPR") cameras made by Flock Safety ("FLOCK") within [*2] the City of Norfolk in May 2023. See Clanna Morales, *How Norfolk Police Use 172 Automatic License Plate Reading Cameras*, *The Virginian Pilot* (June 19, 2023). The cameras are motion activated and capture still images of passing vehicles. *Id.* Because the FLOCK system records the time associated with each image, a vehicle's movement can be "tracked" from camera to camera. Additionally, unlike previous ALPR cameras that only recorded license plate numbers, the FLOCK system can "document details about the make, model and color of the vehicle, as well as alterations, like a roof rack, bumper sticker or damage to the car." *Id.* The Norfolk FLOCK system is programmed to retain vehicle images and physical descriptions on remote computer servers for 30 days. *Id.* One stated purpose of the system is for Norfolk police to be "able to go back and search for a vehicle if a crime is reported after the fact." *Id.*

At the hearing, Detective Gross of the Norfolk Police Department testified generally about the Norfolk FLOCK system. He stated that the 172 individual cameras are stationary and normally capture images of only a single lane of traffic. He indicated that all Hampton Roads police departments have [*3] FLOCK systems and that police departments can share information from their systems with neighboring jurisdictions. No special training is needed to use the system, and all Norfolk Police Department officers have access to the FLOCK system. Gross claimed that the FLOCK system does not provide any personal information about the owner of a vehicle but, rather, provides information only about vehicles. He testified that the FLOCK cameras are motion activated and provide still images but not video.

On November 19, 2023, at approximately 4:00 AM, an intruder broke into a Quick Serve Food Store ("Quick

Serve"), located in the City of Norfolk, and took items from the store, including lottery tickets. The owner of the store provided to the Virginia Lottery a list of the stolen ticket numbers, which were placed on a stolen-ticket database.

An investigator with the Virginia Lottery was informed that an attempt to cash one of the lottery tickets had been made on November 29, 2023, at approximately 9:17 AM at a Miller's Store BP ("Miller's") located in the City of Norfolk. The investigator then collected surveillance footage from Miller's, which depicted a person both attempting to cash the lottery [*4] ticket and operating a white BMW SUV (the "Vehicle") with a flag attached to one of the driver's side windows. However, the vehicle license plate number could not be seen in the surveillance footage.

Gross received the information from the investigator and then searched the database of images associated with two or three FLOCK cameras located near Miller's during a several-hour time frame around the lottery ticket cashing event. As a result, Gross was able to access an image of the Vehicle and ascertain the Vehicle's license plate number.² With that information, he ultimately determined that Robinson was the registered owner of the Vehicle. Through Gross's investigation, he subsequently concluded that Robinson matched the description of the person who tried to cash the lottery ticket at Miller's, as well as the description of the person who broke into the Quick Serve. Based on this information, Norfolk police detectives obtained an arrest warrant for Robinson, a search warrant authorizing attachment of a tracking device to Robinson's vehicle, a search warrant to search Robinson's residence, and a search warrant to search

² After the hearing, Robinson filed an "Addendum to Motion to Suppress" (the "Addendum") in which he pointed out that, upon a review of *previously received* discovery, he located a search warrant affidavit where Gross referred to *multiple* images of the Vehicle in several different locations and indicated that the Vehicle "was in the nearby vicinity of some of the previous commercial burglaries" with which Robinson ultimately was charged. Addendum Mot. Suppress Attach. 1. Hence, contrary to his assertions at the hearing that only a single image of the Vehicle was at issue, Robinson now claims that Gross relied on multiple images. However, the Court does not consider the arguments in the Addendum, as Robinson could have presented them at the hearing. Of note, even if the Court were to consider them, the outcome would be unchanged.

the Vehicle.³ As a result, Robinson was suspected of nine separate [*5] commercial burglaries that occurred over a seven-month period, including the Quick Serve burglary.

Robinson ultimately was charged with nine counts of commercial burglary, attempting to obtain by false pretenses more than \$1,000, larceny of lottery tickets valued at more than \$1,000, two counts of grand larceny, seven counts of petit larceny, and possession of a firearm by a convicted felon. A hearing on the Motion to Suppress was held on July 22, 2024. At the conclusion of the hearing, the Court took the matter under advisement.

Positions of the Parties

Robinson's Position

Robinson argues that suppression of the Vehicle images is appropriate because the relevant FLOCK system images were unconstitutionally obtained without a warrant. Br. Supp. Mot. Suppress 4. Specifically, Robinson argues that the Norfolk Police Department violated his constitutional rights to be free from unreasonable searches by using the FLOCK system to record an image of his vehicle while in the vicinity of Miller's, storing those images, and later accessing those images without a warrant and developing Robinson as a suspect based on obtaining the Vehicle's license plate number from the [*6] FLOCK system. More generally, he asserts that the system is unconstitutionally intrusive because Norfolk's 172 cameras can track the location and identifying information of vehicles throughout the City of Norfolk. *Id.* at 1. This information—which includes the license plate, make, model, color, damage, and any modifications to the vehicles—can then be stored for 30 days and accessed by any Norfolk Police Department officer. *Id.* The stored data also can be shared with other jurisdictions. *Id.*

Robinson contends that the ability to retroactively view the images invades an individual's reasonable expectation of privacy and that officers therefore—

³ Robinson does not challenge the validity of these warrants other than as "fruits of the poisonous tree." [Wong Sun v. United States, 371 U.S. 471, 487-88 \(1963\)](#). Rather, for purposes of the suppression hearing, he contends only that use of the FLOCK system constitutes a search that, absent exigent circumstances, requires a warrant.

absent exigent circumstances—should be required to obtain a warrant before accessing FLOCK system images. *Id.* at 2. Robinson argues that the cameras reveal details of Robinson's life that would otherwise be unknown to a police officer watching in real time because individuals can be documented and tracked throughout the entire city. *Id.* Although Robinson concedes that short-term monitoring of vehicles on a public street might be within an individual's expectation of privacy, he asserts that the prolonged storage of recorded images for thirty days [*7] extends well past this expectation. *Id.* at 3. Robinson asserts that because the information about Robinson and his vehicle were acquired retroactively, Detective Gross needed to first obtain a warrant, which he failed to do. *Id.* at 4. Because Gross failed to obtain a warrant to access the image from the FLOCK system, Robinson moves to suppress "any evidence obtained as a result of the unlawful tracking and surveillance of the Defendant's vehicle and all subsequent searches of the Defendant's residence and property." Mot. Suppress 1.

The Commonwealth's Position

The Commonwealth argues that (1) Robinson lacks standing to challenge use of the FLOCK system and, alternatively, (2) use of the FLOCK system does not constitute a search. Br. Opp. Mot. Suppress 1. The Commonwealth asserts that the capturing, storing, and accessing of FLOCK system images does not violate the Fourth Amendment because a Norfolk police officer could obtain the same information by standing roadside to observe and document **license plates** and characteristics of passing cars. *Id.* at 3-4. Further, the Commonwealth argues that the inherent public nature of driving on a roadway abates reasonable privacy expectations. *Id.* at 3. Finally, [*8] the Commonwealth challenges Robinson's standing due to a lack of ownership interest in both the **license plate** affixed to the Vehicle and the public highway on which he operated the Vehicle. *Id.* at 5.

Analysis

Legal Standard

A defendant seeking to suppress evidence bears the burden of proving factual circumstances giving rise to a reasonable expectation of privacy, which is the burden of persuasion. [Testa v. Commonwealth, 55 Va. App.](#)

[275, 282 n.3, 685 S.E.2d 213, 216 n.3 \(2009\)](#). In response, the Commonwealth has the burden to prove admissibility of the seized evidence by a preponderance of the evidence. See [Colorado v. Connelly, 479 U.S. 157, 168 \(1986\)](#).

The United States Supreme Court has held that, as a general rule, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specially established and well-delineated exceptions." [Katz v. United States, 389 U.S. 347, 357 \(1967\)](#).

Evidence obtained in violation of the U.S. Constitution is ordinarily inadmissible in the criminal trial of a defendant. See, e.g., [Gates v. Commonwealth, 30 Va. App. 352, 355, 516 S.E.2d 731, 732-33 \(1999\)](#).

Discussion

As an initial matter, the Court finds that Robinson has standing to challenge the constitutionality of the FLOCK system. The Commonwealth argues that because Robinson lacks any ownership interest in the Vehicle **license plate** or the public road upon [*9] which he drove, he has no right to assert Fourth Amendment protection over the "reading of the **license plate**." The Court disagrees. First, the image taken was of Robinson's vehicle, not of Robinson. An individual's car is considered a personal "effect" under the Fourth Amendment and, therefore, may be protected under the Fourth Amendment. See [United States v. Jones, 565 U.S. 400, 404, \(2012\)](#) ("It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment."). Second, Robinson appears to be challenging the recording of the image, not the specific information discerned from the image. Hence, the Court finds that Robinson has standing to bring the Motion.

"The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." [Kyllo v. United States, 533 U.S. 27, 33 \(2001\)](#) (quoting [U.S. Const. amend IV](#)). In [Katz v. United States, 389 U.S. 347, 361 \(1967\)](#), the U.S. Supreme Court held that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Id.* However, the Supreme Court has also held that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject

of Fourth Amendment protection." [Id. at 351](#). Additionally, "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement [*10] officers to shield their eyes when passing by a home on public thoroughfares." [California v. Ciraolo, 476 U.S. 207, 213 \(1986\)](#). Indeed, the Court has held that "visual observation is no 'search' at all." [Kyllo, 533 U.S. at 32](#).

The U.S. Supreme Court has recognized certain advances in technology since *Katz* and has determined, under the specific circumstances provided in those cases, what constituted a reasonable expectation of privacy in light of these advances. As a general proposition, it has held that individuals have a reasonable expectation of privacy "in the whole of their physical movements." [Carpenter v. United States, 585 U.S. 296, 310 \(2018\)](#). Invading this privacy expectation qualifies as a search and/or seizure under the Fourth Amendment and normally requires a warrant supported by probable cause. [Id. at 304](#).

In [United States v. Knotts, 460 U.S. 276, 285 \(1983\)](#), the Supreme Court held that the warrantless placement of a monitoring "beeper," a type of tracking device, in the defendant's car did not invade his expectation of privacy under the Fourth Amendment. In that case, a tracking device was placed in a five-gallon drum that was later purchased by the defendant. [Id. at 277](#). The defendant then put the drum in his car and drove from Minnesota to Wisconsin. *Id.* The police used the signal emitted from the tracking device to follow the defendant. *Id.* At one point, the police lost sight of the [*11] defendant and needed air surveillance to assist them in re-locating the tracking signal. *Id.* The defendant argued that such monitoring of his movements without a warrant constituted an illegal search and violated any reasonable expectation of privacy. *Id.* The Supreme Court disagreed:

The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways. We have commented more than once on the diminished expectation of privacy in an automobile: "One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. 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. at 281](#) (quoting [Cardwell v. Lewis, 417 U.S. 583, 590](#)

[\(1974\)](#)). Based on this reasoning, the Court held as follows:

A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he [*12] 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](#).

Although *Knotts* remains good law, in more recent cases the Supreme Court has cautioned that advances in technology must be considered carefully to prevent diminishing Fourth Amendment protections. See, e.g., [Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 359 \(4th Cir. 2021\)](#) (noting that the U.S. Supreme Court, in [United States v. Jones, 565 U.S. 400 \(2012\)](#), recognized that "there will sometimes be tradeoffs between public safety and privacy. Striking the proper balance is even more challenging when dealing with rapidly changing technologies . . . that courts may struggle to understand. If we do not proceed with care, there is a risk we will 'embarrass the future.'" (quoting [Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 \(1944\)](#))).

In [United States v. Jones](#), the Supreme Court ruled that the warrantless use of a global positioning system ("GPS") tracking device on a car exceeded a reasonable expectation of privacy and, therefore, was unconstitutional. [565 U.S. at 404](#). There, the defendant—Jones—was a narcotics trafficking suspect, which led the local U.S. district court to authorize use of an electronic tracking device on a vehicle registered to Jones's wife. [Id. at 402](#). The device [*13] was subsequently installed and monitored for the next twenty-eight days to track the movements of the vehicle. [Id. at 403](#). Using signals from multiple satellites, the device continuously established the vehicle's location within fifty to 100 feet and communicated that location by cellular phone to a government computer. [Id. at 403](#). The device relayed more than 2,000 pages of data over the four-week period. *Id.* Agents used this information to charge and arrest Jones. [Id. at 402](#). The Court held that the Fourth Amendment protects vehicles such as cars from unreasonable searches and seizures, reasoning that the government "physically occupied" Jones's

vehicle to obtain information through the device without a warrant, which was an impermissible invasion of privacy. [Id. at 404](#). As Justice Sotomayor noted in her concurrence, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." [Id. at 415](#) (Sotomayor, J., concurring). She further recognized that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." [Id. at 430](#) (Sotomayor, [*14] J., concurring) (citing [United States v. Knotts, 460 U.S. 276, 281-82 \(1983\)](#)). Based on the invasion of personal property by the government, the Court held that a reasonable expectation of privacy had been exceeded and that the warrantless search was unconstitutional. [Id. at 404, 413](#).

In *Carpenter v. United States*, the Supreme Court held that the warrantless collection of cell-site location information ("CSLI") from the defendant's wireless cellphone carrier over an extended time period constituted an unconstitutional search. [585 U.S. at 313, 320-21](#). In that case, police arrested the defendant, Carpenter, after he was identified as an accomplice in a robbery. [Id. at 301](#). Police then obtained Carpenter's phone records and location points over a 127-day period, with roughly 100 points of data collected each day. [Id. at 302](#). The Court noted that past cell phone information is "detailed, encyclopedic, and effortlessly compiled" and creates "a detailed and comprehensive record of a person's movements." [Id. at 309](#). The Court further pointed out that "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" [Id. at 311](#) (quoting [Jones, 565 U.S. at 415](#) (Sotomayor, J., concurring)).⁴ The Court [*15] ultimately held that continuously tracking Carpenter's movements over an extended period of time without a warrant invaded a reasonable expectation of privacy and violated his Fourth Amendment rights. [Id. at 316](#).

⁴As the U.S. Court of Appeals for the District of Columbia similarly pointed out, "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." [United States v. Maynard, 615 F.3d 544, 562 \(D.C. Cir. 2010\)](#).

More recently, in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the U.S. Court of Appeals for the Fourth Circuit held that a warrantless aerial surveillance program administered by the Baltimore Police Department was unconstitutional because it violated a community advocate group's Fourth Amendment privacy protection against unreasonable searches.⁵ [2 F. 4th 330, 348 \(4th Cir. 2021\)](#). In 2020, Baltimore City implemented a six-month pilot program utilizing multiple surveillance planes designed to track individuals and vehicles moving to and from crime scenes. [Id. at 333-34](#). Flying specific orbits forty hours a week, the planes were equipped with aerial cameras and captured approximately thirty-two square miles per image per second, or approximately ninety percent of the city daily. [Id. at 334](#). The images were normally retained for at least forty-five days. [Id. at 341](#). The court held that the police were only able to determine what was useful based on retrospectively combing through data collected from continuously recording the public's movements. [Id. at 347](#). The court opined [*16] that the "program 'tracks every movement' of every person outside in Baltimore" and "opens 'an intimate window' into a person's associations and activities." [Id. at 341](#) (quoting [Carpenter, 585 U.S. at 311](#)). Further, "because the data is retained for 45 days—at least—it is a 'detailed, encyclopedic,' record of where everyone came and went within the city during daylight hours over the prior month-and-a-half" [Id. at 341](#). The court ultimately concluded that the program enabled the police to deduce in detail an individual's movements and, hence, its operation required a warrant under the Fourth Amendment. [Id. at 344-45](#).

The question before this Court, then, is whether—under the circumstances present here—the warrantless collection and storage of vehicle **license plate** numbers, identification characteristics, and location information by the FLOCK system constituted an unreasonable search under the Fourth Amendment. The Court finds that it was not.

The FLOCK camera images are of *vehicles*, not individuals, and they offer no insight into where vehicles have traveled between camera locations. Further, the cameras do not capture images of private information⁶

⁵Although federal circuit court opinions are not binding on this Court, the Court finds the analysis therein persuasive.

⁶In 2020, the Supreme Court of Virginia held that images taken with ALPR cameras—similar to the FLOCK camera images at issue in this case—did not contain "personal

or property that an individual might expect to keep private, but instead only record images and catalog vehicle license plate numbers [*17] and physical characteristics that are publicly available to any viewer who might be present at the camera locations. Regarding retention of the images, the Supreme Court has expressly declined to provide any specific guidance as to the image retention period that constitutes a violation of the Fourth Amendment:

The concurrence posits that 'relatively short-term monitoring of a person's movements on public streets' is okay, but that 'the use of longer term GPS monitoring in investigations of most offenses is no good.' That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search [*18] is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

[Jones, 565 U.S. at 412-13](#) (internal citations omitted). But see [Neal v. Fairfax Cnty. Police Dep't, 299 Va. 253, 269, 849 S.E.2d 123, 131 \(2020\)](#) (holding that ALPR-related images are not "personal information" and, therefore, presumably are not subject to a maximum retention period).

With respect to Norfolk's FLOCK system, it needs to be viewed in context. The City of Norfolk has a landmass of more than fifty square miles, <http://www.usa.com/norfolk-va.htm> (last visited July 26, 2024), and more than 2,000 lane-miles of roadway, <https://www.norfolk.gov/1655/Streets-Bridges> (last visited July 26, 2024). The 172 stationary FLOCK cameras, which are typically targeted at a single lane of traffic, capture only a very tiny fraction of the city's

roadways. At most, the system can provide time-stamped images that indicate a vehicle's location at several discrete dates and times.

The Court notes that the recorded Norfolk FLOCK images capture identifying features of vehicles traveling on public streets, including license plate numbers, and not information about the driver, passengers, or property within the vehicles. The images are not kept indefinitely but, rather, are deleted [*19] after thirty days. Although the number and location of the cameras in Norfolk arguably offer a very rudimentary "tracking" capability—if one were to "connect the dots" between camera locations that a vehicle passes by—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. Additionally, the system offers no insight regarding the vehicle driver or the vehicle's movements or location when between cameras; for instance, there is no way of knowing who was driving the vehicle, whether the vehicle stopped at a given location, or whether there was an exchange of vehicle drivers. Considering these facts, the Court finds that the current Norfolk FLOCK system is not analogous to long-term GPS positioning, ongoing CSLI geolocation, or constant aerial surveillance, *i.e.*, arrangements by which the government can continuously track an individual's movements—potentially in both public and private areas—and thereby deduce the activities and routine of individuals.

In fact, in the instant case, *no tracking* of Robinson's vehicle movements took place. Rather, the FLOCK system captured a single [*20] image of the Vehicle, which an observer at that camera location could have seen. The system did not reveal the "whole of [Robinson's] movements" or provide "an intimate window into [Robinson's] life," as only a single image was used by the police to identify Robinson's vehicle and determine the vehicle license plate number. No private information was recorded, and no images were obtained through a trespass of Robinson's personal property. As such, the Court holds that Robinson's reasonable expectation of privacy under the Fourth Amendment was not violated.

The Court is not suggesting that warrantless access to a FLOCK system that incorporates widespread camera use over an extended period of time might not violate an individual's Fourth Amendment rights. With enough cameras, virtually continuous tracking theoretically is possible. And with a sufficient number of recorded images, an individual's routine, habits, and patterns of

information," like the "name, personal number or other identifying particulars of a data subject." [Neal v. Fairfax Cnty. Police Dep't, 299 Va. 253, 264, 849 S.E.2d 123, 128 \(2020\)](#).

travel might be deduced. See [Commonwealth v. McCarthy, 142 N.E.3d. 1090, 1102 \(2020\)](#) (noting that this "aggregation principle for the technological surveillance of public conduct" is sometimes referred to as "the mosaic theory"). Such a system could exceed a reasonable expectation of privacy. However, that is a much different situation than that [*21] present in the case before this Court, which involved only a single recorded image. See, e.g., [United States v. Yang, 958 F.3d 851, 862 \(9th Cir. 2020\)](#) (Bea, J., concurring) (holding that a single ALPR image "did not reveal 'the whole of [the defendant's] physical movement,' and therefore did not infringe on [a] reasonable expectation of privacy").⁷

/s/ David W. Lannetti
David W. Lannetti
Judge

End of Document

To be clear, the Court is analyzing Norfolk's FLOCK system only as currently configured and only under the specific factual circumstances of this case, including the limited number of cameras and the inability to continuously track vehicles. Further, the situation presented to the Court does not involve vehicle tracking but, rather, surrounds a single image of the Vehicle. Based on the current configuration of Norfolk's FLOCK system and the factual circumstances of the instant case, the Court finds that Robinson's Fourth Amendment rights were not violated.⁸ Hence, the Court denies Robinson's motion to suppress evidence.

Conclusion

Based on the above, the Court finds that although Robinson has standing to challenge the constitutionality of the warrantless use of Norfolk's FLOCK system, a reasonable expectation of privacy was not exceeded. Therefore, the Court DENIES Robinson's "Motion to Suppress" evidence. [*22]

The Clerk is directed to prepare an Order incorporating the Court's ruling. Any objections shall be filed with the Court within seven days.

⁷ See *supra* note 5.

⁸ The Court recognizes that another judge of this Court held that the warrantless use of Norfolk's FLOCK system, in substantially the same configuration and under arguably analogous facts, was unconstitutional. See [Commonwealth v. Bell, No. CR23-1500-00/01/02, 2024 Va. Cir. LEXIS 77 \(May 10, 2024\)](#). However, that case is not binding on the Court, and each case is determined based on its respective unique set of facts.

Commonwealth of Virginia

JUDGES

STEVEN C. MCCALLUM
DAVID E. JOHNSON
EDWARD A. ROBBINS, JR.
JAYNE A. PEMBERTON
M. DUNCAN MINTON, JR.
STEVEN B. NOVEY

JOHN F. DAFFRON, JR.
WILLIAM R. SHELTON
MICHAEL C. ALLEN
HERBERT C. GILL, JR.
HAROLD W. BURGESS, JR.
T.J. HAULER
FREDERICK G. ROCKWELL, III
LYNN S. BRICE
RETIRED



COUNTY OF CHESTERFIELD
CITY OF COLONIAL HEIGHTS

JUDGES' CHAMBERS
POST OFFICE BOX 57
CHESTERFIELD, VIRGINIA 23832-0057
(804) 748-1333

TERESA L. RYAN
ADMINISTRATOR OF JUDICIAL OPERATIONS

TWELFTH JUDICIAL CIRCUIT

August 1, 2024

Melissa H. Hoy, Esq.
Deputy Commonwealth's Attorney
Chesterfield County
P.O. Box 25
Chesterfield, VA 23832

My'chael D. Jefferson-Reese, Esq.
Chief Public Defender
5601 Ironbridge Parkway, Suite 200
Chester, VA 23831
Counsel for Defendant

Re: *Commonwealth v. Jonah Leon Adams- CR23F01043-01 to CR23F01043-21*

Enclosed is Judge Johnson's Ruling on Defendant's Motion to Suppress Mass Surveillance License Plate Reader Camera Records.

Respectfully,

A handwritten signature in black ink, appearing to read "Abbey Lahnston".

Abbey Lahnston, Law Clerk to the
Honorable David E. Johnson, Judge

12th Judicial Circuit
County of Chesterfield
Judge's Chambers
P.O. Box 57
Chesterfield, VA 23832

Virginia:

IN THE CIRCUIT COURT FOR THE COUNTY OF CHESTERFIELD

COMMONWEALTH OF VIRGINIA

v.

JONAH LEON ADAMS,
Defendant.

CR23F01043-01—21

Ruling on Defendant's Motion to Suppress Mass
Surveillance License Plate Reader Camera Records

Judge David Johnson
Twelfth Judicial Circuit
August 1, 2024

Defendant moved this Court to suppress records from the License Plate Reader (LPR) mass surveillance cameras. The Court reviewed Defendant's memorandum in support of his motion and the Commonwealth's response thereto. The Court heard argument on July 23, 2024, denied the Defendant's motion, and stated it would issue a written opinion detailing its ruling.

Facts

On November 18, 2022, at approximately 4:45 a.m., Chesterfield County police officers responded to a 911 call at the home of Joanna Cottle at 4275 Laurel Oak Road. Upon arrival, the police found the back sliding glass door shattered and discovered that Joanna Cottle and her three children had been shot to death. During the subsequent investigation, the police reviewed a neighbor's home surveillance video which showed a dark color or black sedan passing 4165 Laurel Oak Road. The vehicle headed in the direction of the Cottle residence at 4:26:57 a.m. and then headed away from the Cottle residence at 4:57:22 a.m., at a high rate of speed.

Upon further investigation, the police learned that in 2018 Ms. Cottle sought and was granted an emergency protective order for acts of violence the Defendant allegedly committed against her. Thus the police determined that the Defendant was a potential suspect. Police intelligence analysts ran the name “Jonah Adams” through several databases. They located a vehicle – a Ford F-150, Maryland license DV23644 – associated with the Defendant. The Defendant’s license information was confirmed through the Maryland DMV. In addition, the investigation revealed a 2016 Mazda previously registered to the Defendant, but without current Virginia registration. Once this information was confirmed, authorized police personnel ran the Maryland tag number, DV23644, through the LPR system. The search was confined to a 26-hour period, encompassing the time of the crime. This search resulted in four hits of a dark color/black sedan, consistent with a Mazda, displaying the Maryland tag. Police subsequently located the Defendant at his Maryland apartment complex with three vehicles: a Ford F-150 with only its rear tag affixed (DV23644), a black Mazda with no tags affixed, and a Blue Kia registered to his wife.

Analysis

LPR mass surveillance cameras capture images of passing vehicles’ license plates. The cameras can be stationary or mounted on a police vehicle. The Chesterfield County police operate approximately twenty-two LPRs. The cameras are generally mounted and, in this case, specifically mounted on Chesterfield County owned property. The images captured by the LPR system are maintained for a limited period of time and therefore, the LPR system is not designed as a tracking tool. The Defendant in his motion alleged that “this dragnet system ... indiscriminately” collects data from passing vehicles for storage in a cloud database and that “[t]he police appear able to trawl the Flock camera database at their whim.” Def.’s Mot. ¶¶ 2, 4. Defendant stated that law enforcement officers “made use of this technology following ... their discovery of the deaths of

four people” and “nearly instantaneously” gathered information on vehicles owned by the Defendant. Def.’s Mot. ¶¶ 5-6. The Commonwealth provided notice to the Defendant of its intention to introduce into evidence records from its “Flock surveillance grid.” Def.’s Mot. ¶ 8-9. Defendant argued that this “easy and invasive surveillance” violates “one’s reasonable expectation of privacy in their physical movements” and is a presumptively invalid search. Def.’s Mot. ¶ 9. The Defendant moved this Court to suppress the evidence from the license plate readers. This Court denied the motion for the reasons detailed herein.

The Supreme Court of the United States “uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action.” *United States v. Knotts*, 460 U.S. 276, 280 (1983) (internal citations and quotation marks omitted); *see Illinois v. Andreas*, 463 U.S. 765, 771 (1983). This inquiry, the Court continued, “normally embraces two discrete questions. The first is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy ... The second question is whether the individual’s subjective expectation of privacy is one that society is prepared to recognize as reasonable.” *Knotts*, 460 U.S. at 280-81 (internal citations and quotation marks omitted); *see Carpenter v. United States*, 585 U.S. 296, 304 (2018). Applying this standard, the question for this Court is whether the Defendant had an actual (subjective) expectation of privacy in the license plate information on his vehicle which society is prepared to recognize as reasonable.

It is well settled that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” *Knotts*, 460 U.S. at 281 (internal citations and quotation marks omitted). “One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one’s residence or

as the repository of personal effects. 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.* The driver of an automobile willingly, knowingly, and, on occasion, enthusiastically exposes his car to the public. And “[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351 (1967).

An examination of the statutes codified in Va. Code §§ 46.2-300, *et seq.*, provides numerous reasons as to why it would not be reasonable for a Virginia motorist to have an expectation of privacy in license plate information. A license plate is required to be affixed to an automobile. Va. Code § 46.2-716(A) (“Every license plate shall be securely fastened to the motor vehicle, trailer, or semitrailer to which it is assigned”). A license plate is a prerequisite to legally operate a motor vehicle on the roads and highways of the Commonwealth. Va. Code § 46.2-711 (F) (“No vehicles shall be operated on the highways in the Commonwealth without displaying the license plates required by this chapter”). License plates are assigned by the Division of Motor Vehicles to individual drivers. *See* Va. Code §§ 46.2-711, 720, 722. It strains credulity to argue that a person who, on the one hand, has no reasonable expectation of privacy in his vehicular movements, would, on the other hand, have a reasonable expectation of privacy in the license plates permitting him to make such vehicular movements. The very purpose of the license plate is to identify the vehicle openly for the enforcement of laws relating to safety and the operation of motor vehicles.

Federal and state cases have consistently concluded that a license plate is an object which is constantly exposed to public view and in which a person has no reasonable expectation of privacy. *See, e.g., United States v. Matthews*, 615 F.2d 1279, 1285 (10th Cir. 1980) (License plates are “in plain view on the outside of the car” and are “subject to seizure” because there is no

reasonable expectation of privacy); *Olabisiomotosho v. City of Houston*, 185 F.3d 521, 529 (5th Cir. 1999) (“A motorist has no privacy interest in her license plate number”); *United States v. Batten*, 73 F. App’x 831, 832 (6th Cir. 2003) (not reported in the Federal Reporter) (“[T]here is no case law indicating that there can be any reasonable expectation of privacy in license plates which are required by law to be displayed in public on the front and rear of any vehicle on a public street”); *United States v. Ellison*, 462 F3d 557, 561 (6th Cir. 2006) (“[T]he very purpose of a license plate number ... is to provide identifying information to law enforcement officials and others”); *United States v. Diaz-Castaneda*, 494 F3d 1146, 1152 (9th Cir. 2007) (“when police officers see a license plate in plain view, and then use that plate to access additional non-private information about the car and its owner, they do not conduct a Fourth Amendment search”); *People v. Bushey*, 29 N.Y.3d 158, 163 (2017) (“Because the purpose of a license plate is to readily facilitate the identification of the registered owner of the vehicle for the administration of public safety, a person has no reasonable expectation of privacy in the information acquired by the State for this purpose and contained in a law enforcement or DMV database”); *see also New York v. Class*, 475 U.S. 106, 112-114 (1986) (Federal and state governments have an important regulatory interest in requiring the placement of the vehicle identification number in an area ordinarily in plain view from outside the passenger compartment of an automobile. Therefore, there is no reasonable expectation of privacy in VIN); *United States v. Miranda-Sotolongo*, 827 F3d 663, 668 (7th Cir. 2016) (“observing and recording the registration number was not a search within the meaning of the Fourth Amendment”).

For these reasons, this Court finds that a person has no reasonable expectation of privacy in his license plates.

This Court does not lightly dismiss the Defendant’s comment that “[t]echnology is making it easier and easier for the government to keep tabs on citizens.” Counsel for Defendant indulged in slightly exaggerated rhetoric in describing the LPR as a “revolutionary ... dragnet system ... indiscriminately collecting data ... for storage in a cloud database,” but Counsel does not exaggerate the potential danger in the government’s use of such systems. As the Supreme Court of Virginia recently noted: “Modern technology enables governments to acquire information on the population on an unprecedented scale. National, state, and local governments can use that information for a variety of administrative purposes and to help apprehend dangerous criminals. But knowledge is power, and power can be abused.” *Neal v. Fairfax County Police Department*, 299 Va. 253, 263 (2020). But even the work of the most elaborate technological innovation depends on the supervision of a rational being. It is human vigilance, human thought, and human actions (insignificant perhaps at times, but irreplaceable nevertheless) that determine the role, the influence, and the worth of modern technology. In this instance, vigilance, thought, and actions placed proper parameters around the LPR system and allowed it to properly function in a constitutional republic.

This Court found that the Defendant had no subjective expectation of privacy in the license plate information on his vehicle. Accordingly, the Court denied the motion.



FOURTH JUDICIAL CIRCUIT OF VIRGINIA
CIRCUIT COURT OF THE CITY OF NORFOLK

EVERETT A. MARTIN JR.
JUDGE

150 ST. PAUL'S BOULEVARD
NORFOLK, VIRGINIA 23510

August 23, 2024

Gordon C. Ufkes, Esq.
Office of the Commonwealth's Attorney
800 E. City Hall Avenue, Suite 600
Norfolk, Virginia, 23510

C. Thomas James, Esq.
Office of the Public Defender
125 St. Paul's Boulevard, Suite 600
Norfolk, Virginia, 23510

Re: Commonwealth of Virginia v. Isaiah Roberson
Criminal Nos.: CR24-93; CR24-711

Dear Mr. Ufkes and Mr. James:

This case came before me on August 19, 2024, on the defendant's motion to suppress.

The Crime & the Manhunt

On September 26, 2023, at about 11:20 p.m., the Norfolk police received a report of a person suffering gunshot wounds at the Motel 6 at 853 North Military Highway. The victim, Christopher Armbrister,¹ was pronounced dead at the scene.

Police investigators reviewed surveillance video at the motel that showed two men getting out of a car in the motel's parking area and walking toward the motel. They approached Armbrister. One man hit him; the other displayed a firearm and shot him once. Armbrister tried to run away from them, but he was hit by a second bullet and fell to the ground near the main entrance to the motel lobby. The assailants returned to the car; it left the motel's parking area; it turned south on North Military Highway. The car's license plate could not be seen on the motel's surveillance video, but from the video the police could identify the make of the car as a Hyundai from a grill or trunk ornament; Investigator Frear was somehow able to determine the model. A Flock camera installed at the intersection of Military Highway and Poplar Hall Drive, which is less than ½ mile south of the Motel 6, recorded license plate number TSF – 6600 on a Hyundai Elantra that passed by it at 11:19 p.m.

¹ The name comes from the indictment for murder.

After the police entered this license plate number into its Flock camera database, they found that other cameras had detected the Hyundai Elantra westbound on Northampton Boulevard at Premium Outlets Boulevard at 12:58 a.m. the next day and northbound on 4th View Street at Staten Avenue at 1:07 a.m. Patrol officers found the Hyundai Elantra at a Budget Inn at 9601 4th View Street. The police later obtained search warrants for a room of the inn, the Hyundai Elantra, and another car. They discovered incriminating evidence, which Roberson, by this motion, seeks to suppress as the fruit of an illegal search.

The Camera System

The City of Norfolk has installed 174 Flock cameras (the “camera system”) at various locations on public streets throughout the city. They are mostly on the city’s principal streets. According to the testimony of Michael Molina, Vice President – Legal and General Counsel of Flock Group, Inc., each camera only takes a still picture of the rear of a passing vehicle. If a vehicle is moving slowly, a camera may take up to 3 still photographs of it. Ninety percent of Flock’s cameras can record a motor vehicle’s license plate, make, model, color, and distinctive characteristics but have a range of only 10 to 15 feet.² The cameras will only take photographs of 1 or 2 lanes of a street. The City of Norfolk owns the cameras and the data they collect. The camera system creates a searchable database of vehicle photographs that are stored for 30 days and then deleted. Mr. Molina also testified that the cameras do not capture images of the driver of an automobile or any passengers.³ Commonwealth exhibits 1-3 corroborate this. The cameras have no audio capability; they cannot record conversations within the passing vehicles. The camera system does not track vehicles. It only records that a certain vehicle passed by a certain camera on a certain day at a certain time. It does not record where the vehicle goes after it passes the camera, nor what the driver or passengers may do. It does not take photographs of pedestrians on adjacent sidewalks.

The Motion & the Response

The gist of the written motion is that the camera system allows the Norfolk Police Department to obtain a “detailed, effortless, encyclopedic tracking of [Roberson’s] movements,” and a photographic record of all motor vehicles being operated in Norfolk. Roberson complains it allowed the police to obtain the license plate number and direction of travel of the suspect vehicle, which violated his reasonable expectation of privacy and his rights under the Fourth Amendment of the federal constitution.⁴

² Mr. Molina also testified the strongest lens available has a range of 250 feet. He did not know the type or types of lenses on Norfolk’s cameras.

³ Mr. Molina testified that a Flock camera will take a photograph of a passing bicycle or motorcycle, but as for its ability to identify the operator only the back of the operator will appear.

⁴ He also bases the motion on §§ 8, 10, and 11 of Article I of the Constitution of Virginia. He does not specify the particular clauses of §§ 8 and 11 upon which he relies, but I assume it is the due process clause of each. Section 10 prohibits searches and seizures under general warrants, not warrantless searches and seizures; it merely adopts the common law on the subject. *McClannan v. Chaplain*, 136 Va. 1, 14-5, 116 S.E. 495, 498 (1923). At common law, an illegality in the mode of procuring evidence was no ground for excluding it. 4 Wigmore, *Treatise on the Anglo American System of Evidence in Trials at Common Law*, § 2183 (5th ed. 1923); Greenleaf, *Law of Evidence*, § 254(a) (11th ed. 1863). Neither the common law nor these sections of our constitution have ever been held by our Supreme Courts to provide suppression of evidence as a remedy for a violation. *Hart v. Commonwealth*, 221 Va. 283, 268 S.E.2d 806 (1980); *Hall v. Commonwealth*, 138 Va. 727, 121 S.E. 154 (1924). The requirements of the Virginia

The Commonwealth claims Roberson has no expectation of privacy in the exterior of an automobile or its license plate, which is owned by the Department of Motor Vehicles, while the automobile is on a public highway. Furthermore, it continues, the camera system gives the police no more information than they could obtain by having an officer stand on the street and observe passing motor vehicles. Lastly, it denies the camera system tracks all of a person's movements over an extended time.

At the hearing, Roberson conceded he had no expectation of privacy in the exterior of the Hyundai Elantra. His complaint is the tracking of his movements and the police department's accessing the camera system data without a search warrant. But as the alleged tracking of his movements is based on photographs of the exterior of the car in which it appears he was traveling, the issues cannot be cleanly divorced.

*The Fourth Amendment, the Exterior of Motor Vehicles,
and the Movement of Suspects before 2012*

Well into the 20th Century, Fourth Amendment jurisprudence was tied to common law trespass. *Kyllo v. United States*, 533 U.S. 27, 31 (2001). "Visual surveillance was unquestionably lawful because 'the eye cannot by the laws of England be guilty of a trespass.'" *Id.*, at 31-2 (quoting *Boyd v. United States*, 118 U.S. 616, 628 (1886); *Entick v. Carrington*, 19 How. St. Tr. 1029, 1066, 2 Wils. K.B. 275, 95 Eng. Rep. 807 (C.P. 1765)).

However, in *Katz v. United States*, the Supreme Court extended Fourth Amendment protection beyond trespassory acts by the police to those areas in which, as Justice Harlan stated in his concurrence, a person seeks to preserve something and has a reasonable expectation of privacy which society recognizes. 389 U.S. 347, 361 (1967). The Court famously held in *Katz*: "For the Fourth Amendment protects people, not places." *Id.* at 351. Less famous is the sentence that immediately follows: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Id.*

Even after *Katz*, the Supreme Court has often stated that automobiles do not have the same Fourth Amendment protections afforded to homes. There are several reasons for the distinction. The mobility of an automobile may create an exigency that would make obtaining a search warrant an impossibility. Automobiles are subject to regular inspections and licensing. Police officers regularly stop automobiles for equipment violations. Most important, the purpose of an automobile is transportation on public roads where it and its occupants are visible to anyone who cares to look. *South Dakota v. Opperman*, 428 U.S. 364, 367-68 (1976).

In *Cook v. Commonwealth*, Cook had parked his car on a public street and left a bag in it that contained hashish. 216 Va. 71, 216 S.E.2d 48 (1975). The Court held it unnecessary to determine if the warrantless search of the inside of the car was lawful because the defendant only contended the police conducted an illegal search of the car by looking into it. The Court rejected the argument.

constitution are substantially the same as the Fourth Amendment. *Lowe v. Commonwealth*, 230 Va. 346, 348, n.1, 337 S.E.2d 273, 275 (1985).

It is not unlawful, but entirely lawful, for a police officer who is on a public street or sidewalk to look, either deliberately or inadvertently, into an automobile parked on the street and to observe what is exposed therein to open view. (citation omitted).

Such police action does not constitute a search in the constitutional sense.

Id. at 73, 50.

In *United States v. Knotts*, the police suspected Knotts and others were manufacturing methamphetamine. 460 U.S. 276 (1983). A co-defendant had been seen purchasing a precursor chemical from a chemical supply company, so the police put a transmitting device in a container of that chemical, which the co-defendant later purchased. The police followed the automobile with the container by visual surveillance and monitoring of the beeper. The beeper signal eventually became stationary, and the police obtained and executed a search warrant for that place, where they discovered a drug laboratory. Knotts moved to suppress the evidence, claiming the warrantless monitoring of the beeper was an unlawful search, as he had a reasonable expectation of privacy. The Supreme Court disagreed.

The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways....

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. The Court reserved whether different constitutional principles might apply to “dragnet-type law enforcement practices” such as “twenty-four-hour surveillance” of a citizen without judicial supervision. *Id.* at 283-84.

A little more than two years later, the Supreme Court decided *New York v. Class*, 475 U.S. 106 (1986). The police observed Class speeding and driving a car with a cracked windshield, both traffic violations under New York law. After stopping Class, an officer opened a door of the car to move some papers to obtain the vehicle identification number (“VIN”). In doing so, he saw the handle of a gun protruding from beneath the driver’s seat. Class was charged with unlawful possession of a weapon and he moved to suppress the gun as evidence.

The Court observed that a federal regulation required the VIN to be legible from outside the car, and

In addition, it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile... The exterior of a car, of course, is thrust into the public eye, and thus to examine it does not constitute a 'search.'

Id. at 114.

United States v. Jones
565 U.S. 400 (2012)

The police obtained a warrant to attach an electronic tracking device to Jones's car within 10 days. They attached it on the 11th day and tracked the car's movements for 28 days. The device established the car's location to within 50 to 100 feet, and transmitted that data to a government computer. The device relayed more than 2000 pages of data over the period. Jones sought to suppress the evidence obtained through the tracking device.

The Supreme Court affirmed the suppression of the evidence. In doing so it revived the trespassory view of the Fourth Amendment that had fallen into disuse after *Katz*. The Court noted that the government had obtained information by "physically occup[ying] private property," *Id.* at 404, by "physically intruding on a constitutionally protected area," *Id.* at 406, n. 3, and by "attaching the device to the Jeep, officers encroached on a protected area." *Id.* at 410. See *Entick, supra* ("By the laws of England, every invasion of private property, be it ever so minute, is a trespass").

The Court distinguished *Knotts*, as that case had been decided only on the ground that no reasonable expectation of privacy existed. A trespassory claim was not at issue. *Id.* at 408-09. The Court distinguished *Class* because the government conceded in *Jones* that the officers did more than conduct a visual inspection of the car. *Id.* at 410. In discussing the "concurrency's insistence on the exclusivity of the *Katz* test," the Court stated: "This Court has to date not deviated from the understanding that mere visual observation does not constitute a search." *Id.* at 412.

Carpenter v. United States
585 U.S. 296 (2018)

Carpenter concerned not visual observation of an automobile, but tracking a person's movements. The question was "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. The Court held that it did.

Carpenter was charged with a series of armed robberies. One suspect had identified a number of accomplices and had given the FBI some of their cell phone numbers. Based on this information, prosecutors obtained court orders to retrieve *Carpenter*'s cell site location data during the period of the robberies from his two wireless carriers. Altogether, the government

obtained 12,898 location points cataloging Carpenter’s movements – an average of 101 data points per day. The showing required to obtain a court order was less than probable cause.

The Court described cell phone location information as “detailed, encyclopedic, and effortlessly compiled.” *Id.* at 309. It described a cell phone as:

— almost a ‘feature of human anatomy,’...— [that] tracks nearly exactly the movements of its of owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years [the period cell-phone companies maintain data], and the police may – in the Government’s view – call upon the results of that surveillance without regard to the constraints of the Fourth Amendment.

Id. at 311–12. The Court noted that a majority of its members had “already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements,” *Id.* at 310, but it placed this limit on its holding: “We do not ... call into question conventional surveillance techniques and tools, such as security cameras,” *Id.* at 316.

Other Rulings in this Court

This is an issue of third impression in this Court. Judge LeCruise held the camera system and the storage of license plate and location information constituted a search under the Fourth Amendment. *Commonwealth v. Bell*, Criminal No. CR23-1500, 2024 Va. Cir. Lexis 77 (May 10, 2024). On a somewhat different factual record, which appears to include taking judicial notice of certain facts, Judge Lannetti reached the opposite conclusion. *Commonwealth v. Robinson*, Criminal Nos. CR24-221, 24-402, 2024 Va. Cir. Lexis 104 (July 26, 2024). It is not the least bit surprising that different judges on different factual records can reach different conclusions on the same legal issue. The factual record here appears to be more developed than that before either Judge LeCruise or Judge Lannetti.

*Is the camera system a dragnet?
Is it a search?*

I think it is neither. The photographing of the Elantra was clearly not a trespassory act, as in *Jones*. Nor, as Roberson concedes, did he have a reasonable expectation of privacy in the exterior of the Elantra or its license plates. By driving on public streets, the driver exposed the exterior of the Elantra and its license plates to anyone who cared to look.

Unlike the electronic device the police attached to the car in *Jones*, the camera system does not follow a vehicle. It takes a still picture of a vehicle that passes by it (assuming the camera covers that lane of travel). Here, the camera system produced three photographs of the Elantra over a period of one hour and 48 minutes. Each location was several miles from the other locations. The police had no idea where the Elantra went in the time between the taking of each photograph. They did not know who may have gotten into or out of the Elantra over that period of time.

Unlike the cell site location information at issue in *Carpenter*, the camera system does not track a person. The photographs the cameras take do not show images of the driver or any passenger or who gets in or out of a vehicle. The camera system does not provide the police with a comprehensive chronicle of a person's movements. It simply is not the "dragnet type" surveillance system the Court reserved decision on in *Knotts* and confronted in *Carpenter*.⁵ Nor is it comparable to what was at issue in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F. 4th 330 (2021).

With respect to the police obtaining access to the data system without a search warrant, I am aware of no authority requiring the police to obtain a search warrant to search their own data, and Mr. James cited none. The data obtained in *Carpenter* was owned by cell phone providers.

"[V]isual observation is no 'search' at all," *Kyllo, supra*, at 32. What is complained of here is nothing more than a visual observation, albeit one made easier and more reliable by modern technology. The photographing of the Hyundai Elantra with Virginia license plate TSF-6600 by the camera system on September 26-27, 2023, was not a search within the meaning of the Fourth Amendment. I overrule the motion to suppress. The Clerk will prepare the appropriate order.

Sincerely yours,



Everett A. Martin, Jr.
Judge

EAMjr./arc

⁵ If each camera has a range of 15 feet and covers 2 lanes of travel, 5220 lane-feet (174 x 15 x 2), or a little less than 1 lane-mile, of Norfolk's streets is under Flock surveillance. If each camera has a range of 250 feet, 87,000 lane-feet (174 x 250 x 2), or a little less than 17 lane-miles of Norfolk's streets are under Flock surveillance. Norfolk has about 2,200 lane-miles of streets. <https://www.norfolk.gov/1655/Streets-Bridges> (last visited August 22, 2024).

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. Chatrue, 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

VIRGINIA: IN THE CIRCUIT COURT OF THE CITY OF NORFOLK

Commonwealth of Virginia,

Plaintiff,

v.

Case No. CR24-0776-00, -01, -02

Javon Jerome Reap,

Defendant.

ORDER

THIS MATTER comes before the Court for hearing on two motions that were filed by the Defendant on September 18, 2024. Upon consideration of the arguments of counsel and the accompanying briefs by the Defendant, as well as the Commonwealth's opposition brief to the Defendant's filed Motion to Suppress and a Motion in Limine the Court now rules on these Motions.

The Defendant's Motion in Limine is GRANTED in part. The Commonwealth shall be limited to only two police witnesses who will be permitted to give opinion evidence as to the identification of the Defendant. The witnesses may not testify as to known or suspected bad acts committed by the Defendant.

The Court DENIES the Defendant's Motion to Suppress. The Defendant was a passenger of the vehicle in question and therefore lacks standing to pursue a Fourth Amendment unreasonable search action. *See Rakas v. Illinois*, 439 U.S. 128, 148–49, 99 S. Ct. 421, 433 (1978). Additionally, even if the Defendant were to have had standing, a person does not have a subjective or objective reasonable expectation of privacy in the exterior of their vehicle or their movements on public roads as captured by the Flock camera system. *See United States v. Martin*, 2024 U.S. Dist. LEXIS 186377 (E.D. Va. Oct. 11, 2024).

Pursuant to Rule 1:13 of the *Rules of Supreme Court of Virginia*, endorsements of this Order are hereby waived. The Clerk shall send certified copies of this Order to counsel of record in this case.

ENTERED: 10/16/24



Judge



JAMILAH D. LECRUISE
JUDGE

FOURTH JUDICIAL CIRCUIT OF VIRGINIA
CIRCUIT COURT OF THE CITY OF NORFOLK

Received

MAY 16 2024

Public Defenders Office
Norfolk Virginia
150 ST. PAUL'S BOULEVARD
NORFOLK, VIRGINIA 23510

VIRGINIA: IN THE CIRCUIT COURT OF THE CITY OF NORFOLK

COMMONWEALTH OF VIRGINIA,

v.

CASE NO: CR23001500-00; 01; 02

JAYVON ANTONIO BELL

Defendant.

ORDER GRANTING DEFENDANT'S MOTION TO SUPPRESS

This matter comes before the Court on the Defendant's Motion to Suppress pursuant to the Fourth and Fourteenth Amendments of the United States Constitution; Article I, Section Eight, Ten and Eleven of the Constitution of Virginia; and §19.2-266.2 of the Code of Virginia. Specifically, the Defendant moves the Court to suppress the photographs of the vehicle the Defendant was driving from the FLOCK Automated License Plate Reader (ALPR) system as well as the Defendant's incriminating statement as fruit of the poisonous tree because the Norfolk Police Department (NPD) did not seek a warrant to obtain the license plate information from FLOCK. The Court finds that inherent in the Defendant's argument is a foundation objection as well. Both counsel for the Commonwealth and the Defendant acknowledge that this is a matter of first impression. For the reasons stated herein, the Defendant's Motion is GRANTED.

The Commonwealth has charged the Defendant with one count of Robbery by Using of Displaying a Firearm in violation of Virginia Code §18.2-58, one count of Using a Firearm in the Commission of a Felony (First Offense) in violation of Virginia Code §18.2-53.1, and one count of Conspiracy to Commit Robbery by Using or Displaying a Firearm in violation of Virginia Code §18.2-58/18.2-22. On April 29, 2024, a suppression hearing was held in the Norfolk Circuit Court.

According to the Defendant's motion, and not contested by the Commonwealth, the Norfolk Police Department installed 172 license plate camera readers though out the city of Norfolk in 2023. Clanna Morales, *How Norfolk Police use 172 automatic license plate reading cameras*, The Virginian Pilot, June 19, 2023. The cameras are able to track the locations of vehicles within city limits by license plate number and other physical descriptions with the data being kept for 30 days. *Id.* Every officer from the Norfolk Police Department may access the FLOCK system, which shares its data with other police departments. *Id.*

Investigator Oyola testified on direct examination generally about the FLOCK system used in Norfolk and stated that a suspect vehicle in a robbery in the neighboring jurisdiction of Chesapeake was recorded on the Norfolk FLOCK. He said that FLOCK is no different from the redlight camera system Norfolk already utilizes and has utilized for years although FLOCK is a much newer system. Investigator Oyola describes it as “real time intelligence to combat crime.” He further stated that all of Hampton Roads police departments have FLOCK systems and police departments can share information within the systems from neighboring jurisdictions. No special training is needed and all officers in the Norfolk Police Department have access to the FLOCK system. Investigator Oyola claimed that FLOCK does not provide any personal information about the owner of a vehicle but the license plate information only. The cameras of the system are motion activated and it provides still photographs to police but not video.

Oyola testified that there was a robbery in Chesapeake and an independent witness provided a license plate number to Chesapeake Police. More specifically, Detective Rocca from the Chesapeake Police Department stated to Oyola that the witness described a gray Dodge minivan leaving the video game store and the Norfolk Police Department was able to stop the minivan on South Military Highway in Norfolk after using the FLOCK system. Investigator Oyola stated that after communication with the Chesapeake detective, he ran the vehicle through the FLOCK system and discovered a “hit” with the Dodge minivan alleged to be used in the Chesapeake robbery. He testified that a robbery of a video game store occurred in Norfolk shortly after the one committed in Chesapeake. There was an additional description of two individuals who left the Chesapeake robbery in the minivan.

The Commonwealth’s Attorney asked if Investigator Oyola obtained a search warrant for the FLOCK system and he emphatically replied that he did not need one. He believed the minivan in question that the Defendant was arrested from and during interrogation provided an incriminating statement was used in a video game store robbery in Chesapeake, Norfolk, and Portsmouth within a short timeframe.

On cross examination, Investigator Oyola stated he used the license plate information from the FLOCK system to access the Department of Motor Vehicles database and learned that it was linked to the Defendant’s wife. On redirect examination, Oyola said that he did not know how many redlight cameras were located within the Norfolk city limits but that there are 172 FLOCK cameras installed.

ANALYSIS

The Fourth Amendment safeguards the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, providing no warrants shall issue, but upon probable cause. *U.S. Const. amend IV*. The basic purpose of this Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. *Id.* “[T]he exclusionary rule’s prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures: ‘The rule is calculated to prevent, not to repair. Its purpose is to deter – to compel respect for the constitutional guaranty in the only effectively available way – by removing the incentive to disregard it.’” *United States v. Calandra*, 414 U.S. 338, 347, 94 S. Ct. 613, 38 L. Ed. 2d 561 (1974).

Here, the Court finds the collection and storage of license plate and location information by the FLOCK system constitutes a search within the meaning of the Fourth Amendment and should require a warrant.

The Defendant argues that vehicles in the current technology age are akin to cellular telephones as they reveal the continued location of civilians. The Court agrees. Courts have already determined that the government's acquisition of a defendant's historical cell-site location information (CLSI) from wireless carriers is a search under the Fourth Amendment. *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206 (2018). In such cases, a warrant is required except in exigent circumstances. *Id.* Furthermore, the Court found that an individual maintains a legitimate expectation of privacy in the record of his or her physical movements as captured through cell-site information. *Id.* The Commonwealth argues that vehicles are different because the Defendant did not have a privacy expectation in the public sphere. However, "a person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, what one seeks to preserve as private, even in an area accessible to the public may be constitutionally protected. Individuals have a reasonable expectation of privacy in the whole of their physical movements." *Id.* The FLOCK system collects and records a vehicle's movement data in the same manner as a CSLI.

Like the obtaining and storing of cell-site location data, installing a global positioning system (GPS) device on a vehicle to track a citizen's whereabouts is a search and requires a warrant. *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945 (2012). The Court finds that due to the breadth of FLOCK cameras covering the entire City of Norfolk and the storage component is also akin to a GPS device and requires a warrant.

The Fourth Circuit rejected an aerial surveillance program with data storage because it permitted law enforcement "to deduce from the whole individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment." *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 2021 U.S. App. LEXIS 18868 (2021). Like the aerial surveillance in Baltimore, the highway surveillance program in Norfolk must comply with the warrant requirement. Prolonged tracking of public movements with surveillance serves to invade the reasonable expectation citizens possess in their entire movements and thus requires a warrant. *Id.*

Moreover, the Court cannot overlook the foundational issue this type of system presents. Courts in Norfolk regularly hear testimony from custodians of records for emergency services 911 calls for assistance, the related event chronologies, cellular telephone data, social media information, red light cameras in traffic court matters, and the recently enacted PhotoSafe cameras utilized throughout the city. In each of these instances, the Defendant himself or herself or counsel may cross examine and challenge these witnesses in accordance with court procedural rules that safeguard the reliability of admitted evidence. The Commonwealth regularly presents such witness testimony from custodians of records to lay foundation as to the nature of and how these devices are utilized.

The Court emphasizes that it is perhaps most concerning for the Norfolk Police Department to make warrantless use of this FLOCK system about which the courts of the Commonwealth know so little is due in part to the many ways in which it could be abused. "Modern technology enables governments to acquire information on the population on an unprecedented scale.

National, state, and local governments can use that information for a variety of administrative purposes and to help apprehend dangerous criminals. But knowledge is power, and power can be abused.” *Neal v. Fairfax County Police Department*, 299 Va. 253, 263, 849 SE.2d 123, 127-8 (2020).

Unlike in other jurisdictions where special training is required in order for law enforcement officers to access an ALPR, the Norfolk Police Department does not require such training and all officers have unfettered access to the license plate and location data stored for 30 days. In addition, the neighboring jurisdictions can share FLOCK data with each other very easily. It would not be difficult for mistakes to be made tying law-abiding citizens to crime due to the nature of the FLOCK system and in the event a law enforcement officer would seek to create a suspect where one did not otherwise exist, it would be a simple task and no custodian of record would be presented to the Court for testimony or cross examination. The Court cannot ignore the possibility of a potential hacking incident either. For example, a team of computer scientists at the University of Arizona was able to find vulnerable ALPR cameras in Washington, California, Texas, Oklahoma, Louisiana, Mississippi, Alabama, Florida, *Virginia*, Ohio, and Pennsylvania. (Italics added for emphasis.) Cooper Quintin & Dave Maass, License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech, Electronic Frontier Foundation, (Oct. 28, 2015), <https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive/>. The citizens of Norfolk may be concerned to learn the extent to which the Norfolk Police Department is tracking and maintaining a database of their every movement for 30 days. The Defendant argues “what we have is a dragnet over the entire city” retained for a month and the Court agrees.

The Commonwealth presented the seminal case of *Katz v. United States*, arguing that “what a person knowing exposes to the public...is not subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 353 (1967). The Court finds that times have undoubtedly changed since *Katz* and advances in technology will only continue to provide law enforcement with more avenues to combat crime. However, courts must not neglect the underpinning of the *Katz* decision that, “Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures,” *Id.*

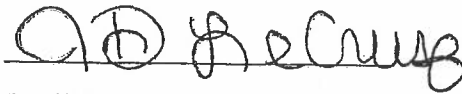
The Commonwealth also argued from *Commonwealth v. McCarthy*, a case from the Supreme Judicial Court of Massachusetts. *Commonwealth v. McCarthy*, 484 Mass. 493, 142 N.E.3d. 1090 (2020) In it, the Court concluded that the defendant’s expectation of privacy was not invaded because there were only four cameras on the ends of two bridges recording license plates with ALPRs and such surveillance was limited and not indicative of the Fourth Amendment. This is not the case in Norfolk with 172 ALPRs through out the jurisdiction.

Furthermore, the Court rejects the Commonwealth’s contention that without the FLOCK evidence, this would be a matter of inevitable discovery, citing *Knight v. Commonwealth*, 71 Va. App. 771, 839 S.E.2d 911 (2020). To establish an inevitable discovery exception, the Commonwealth must show “(1) a reasonable probability that the evidence in question would have been discovered by lawful means but for the police misconduct’ and ‘(2) that the leads making the discovery inevitable were possessed by the police at the time of the misconduct.” *Carlson v. Commonwealth*, 69 Va. App. 749, 763, 823 S.E.2d 28 (2019) (quoting *Commonwealth v. Jones*,

267 Va. 532, 536, 593 S.E.2d 204 (2004). Here, the Court is unconvinced that the Norfolk Police Department would have discovered the Defendant in the suspect vehicle in a way to immediately arrest him before obtaining an incriminatory statement from him without the FLOCK system.

The Defendant's motion to suppress is GRANTED and the Commonwealth's objection is noted for the record. The Clerk is DIRECTED to mail a copy of this Order to counsel of record.

ENTER: May 10, 2024

A handwritten signature in black ink, appearing to read "J.D. LeCruise", written over a horizontal line.

Jamilah D. LeCruise, Judge

Neal v. Fairfax Cty. Police Dep't

Supreme Court of Virginia

October 22, 2020, Decided

Record No. 191127, Record No. 191129

Reporter

299 Va. 253 *; 849 S.E.2d 123 **; 2020 Va. LEXIS 121 ***

HARRISON NEAL v. FAIRFAX COUNTY POLICE DEPARTMENT, ET AL. FAIRFAX COUNTY POLICE DEPARTMENT, ET AL. v. HARRISON NEAL

Prior History: [***1] FROM THE CIRCUIT COURT OF FAIRFAX COUNTY. Robert J. Smith, Judge.

[Neal v. Fairfax Cty. Police Dep't, 2019 Va. Cir. LEXIS 68, 102 Va. Cir. 11 \(Apr. 1, 2019\)](#)

Disposition: Reversed and final judgment.

Counsel: For NEAL, HARRISON, Appellant (191127): ROSENTHAL, EDWARD SCOTT, (ESQ.), MANITTA, LANA MARIE, (ESQ.), ROHRBACH, DAVID CARL, (ESQ.), HEILMAN, EDEN BROOKE, (ESQ.), SAFSTROM, JENNIFER MARIE, (ESQ.), COLLIER, DANIEL CHRISTOPHER, (ESQ.), Appellee Parties.

For FAIRFAX COUNTY POLICE DEPARTMENT, ROESSLER, EDWIN C., JR., (CHIEF OF POLICE COLONEL), Appellee (191127): TEARE, ELIZABETH DOYLE, (ESQ.), GIBBONS, KAREN LEE, (ESQ.), BAUCOM, KIMBERLY PACE, (ESQ.), RAPHAEL, STUART ALAN, (ESQ.), COX, TREVOR STEPHEN, (ESQ.), MCGUIRE, MATTHEW ROBERT, (ESQ.).

For FAIRFAX COUNTY POLICE DEPARTMENT, ROESSLER, EDWIN C., JR., (COLONEL, CHIEF OF POLICE), Appellant (191129): TEARE, ELIZABETH DOYLE, (ESQ.), GIBBONS, KAREN LEE, (ESQ.), BAUCOM, KIMBERLY PACE, (ESQ.), RAPHAEL, STUART ALAN, (ESQ.), COX, TREVOR STEPHEN, (ESQ.), MCGUIRE, MATTHEW ROBERT, (ESQ.), Appellee Parties.

For NEAL, HARRISON, Appellee (191129): ROSENTHAL, EDWARD SCOTT, (ESQ.), MANITTA, LANA MARIE, (ESQ.), ROHRBACH, DAVID CARL, (ESQ.), HEILMAN, EDEN BROOKE, (ESQ.), SAFSTROM, JENNIFER MARIE, (ESQ.), COLLIER, DANIEL CHRISTOPHER, (ESQ.).

Judges: PRESENT: Lemons, C.J., Mims, [***2] Powell,

Kelsey, McCullough, and Chafin, JJ., and Millette, S.J.
OPINION BY JUSTICE STEPHEN R. McCULLOUGH.

Opinion by: STEPHEN R. McCULLOUGH

Opinion

[**124] [*258] OPINION BY JUSTICE STEPHEN R. McCULLOUGH

The Fairfax County Police Department ("Police Department") appeals from an injunction that prohibits it from passively collecting, storing, and using license plate and related data through its Automated License Plate Recognition ("ALPR") system. Among other things, the Police Department contends that the circuit court erred in concluding that the ALPR system satisfies the definition of an "information system" under the [Government Data Collection and Dissemination Practices Act, Code §§ 2.2-3800 through -3809](#) [**125] ("Data Act"). Neal separately appeals the circuit court's award of attorney's fees, contending the circuit court erred in reducing the fees sought by his attorneys. App. 2089. We agree with the Police Department that the ALPR system does not constitute an "information system" within the intentment of the Data Act and we, therefore, reverse the decision below.

BACKGROUND

I. THE ALPR SYSTEM.

The Police Department's ALPR system uses cameras that capture images of passing vehicles' license plates. The cameras can be stationary or mounted [***3] on a police vehicle. Once the camera captures a license plate image it converts that image into an alpha-numeric combination. In order to access that alpha-numeric combination and associated data, an officer of the Police Department must specifically log on to the ALPR software program. Logging on to the ALPR software program requires a unique log-in credential and password. Only officers who have completed the

required training can gain access to the software. The Police Department employs the ALPR system for "active" and "passive" uses.

"Active" use involves checking the license plates that are scanned against a "hot list." The Virginia State Police publishes this "hot list" twice daily. The list consists of all active stolen [*259] license plates and vehicles from two databases, the National Crime Information Center ("NCIC") and Virginia Criminal Information Network ("VCIN"). The hot list also contains license plates associated with suspected criminal activity, such as abductions. The hot list is available to authorized law enforcement personnel who can access it through a secure website. The hot list can be imported into the ALPR system either automatically through a server or manually [***4] by the end user. The end user may also manually enter a license plate into the ALPR system along with a notation regarding the reason for the entry, for example a stolen vehicle.

While scanning license plates, the ALPR software alerts the operator when it detects a potential stolen vehicle or license plate. According to a Standard Operating Procedure ("SOP") developed by the Police Department, "[a]n alarm is NOT conclusive confirmation that a license plate or vehicle is wanted, but an indicator that additional investigation is warranted." If the ALPR system alerts, the officer is instructed to visually verify the license plate, to make sure it is from the correct state and displays the same characters as the ones on the screen. The SOP then instructs the officer to make sure the hot list is still active by checking the NCIC/VCIN databases, either by running the information in a search on the computer in the car or by a voice request. The SOP further states that "[s]tolen vehicle or license plate responses from NCIC/VCIN shall be confirmed by Teletype in accordance with established procedures as soon as practical." Additionally, if an officer makes contact with a suspect, the contact [***5] must be "documented as appropriate in the I/Leads Records Management System" or by "using the COMMENT button from the event screen in I/MOBILE." The I/Leads system documents arrests or a contact between an officer and a suspect. There is no connection between the ALPR program and the I/Leads police report system. The two are separate systems.

The ALPR database does not contain the name or other identifying information about the owner of the vehicle. To obtain this information, the officer must log off of the ALPR database and log on to a separate database, such as the VCIN, NCIC, or Department of Motor

Vehicles ("DMV") databases, that are maintained by other agencies. There is no computerized link between the ALPR database and these other databases.

[*260] Beyond "active use," the Police Department also engages in what the parties refer to as "passive use." The Police Department maintains a database that stores the images that are captured, as well as the GPS coordinates of the locations where those images were captured. This data is stored for 364 days, after which time the information is purged. The database can be searched only by license plate number. Only police officers who are trained [***6] and certified as ALPR system users can query the database. The Police [**126] Department's passive use of the ALPR system data is what is at issue in this case.

II. INITIAL PROCEEDINGS.

Harrison Neal filed a complaint seeking "an injunction and/or writ of mandamus" pursuant to the Data Act. He asked the circuit court to prohibit the Police Department from continuing to collect and store license plate data without suspicion of any criminal activity, i.e., the Police Department's passive use of the technology. Neal contended that the ALPR database is an "information system" that gathers personal information during its passive use and that this practice contravenes the Data Act. Neal filed his complaint after he submitted a Freedom of Information Act request to the Police Department asking for its ALPR records regarding his vehicle. He received two sheets of paper in response. Each sheet contained a picture of his vehicle and his license plate, and listed the time and date the photo was taken.

The circuit court entered summary judgment in favor of the Police Department, concluding the data at issue did not qualify as "personal information" under the Data Act. We reversed that judgment of the circuit [***7] court in [Neal v. Fairfax County Police Department, 295 Va. 334, 812 S.E.2d 444 \(2018\)](#) ("Neal I"). We examined to what extent the data gathered by the ALPR system constituted "personal information" as defined in the Data Act. [Neal I, 295 Va. at. 345-47.](#)

"Personal information" means all information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, [*261] and his education, financial transactions, medical history, ancestry,

religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.

[Code § 2.2-3801.](#)

We concluded that "a license plate number stored in the ALPR database [***8] would not be personal information because it does not describe, locate or index anything about an individual." [Neal I, 295 Va. at 346](#). That, however, did not end the inquiry. We further held that "pictures and data associated with each license plate number constitute 'personal information' under [Code § 2.2-3801](#). *Id.* That is because "[t]he images of the vehicle, its license plate, and the vehicle's immediate surroundings, along with the GPS location, time, and date when the image was captured 'afford a basis for inferring personal characteristics, such as . . . things done by or to' the individual who owns the vehicle, as well as a basis for inferring the presence of the individual who owns the vehicle in a certain location at a certain time." [Id. at 346-47](#) (quoting [Code § 2.2-3801](#)).

The Data Act imposes certain strictures that are keyed to an "information system." For example, [Code § 2.2-3803](#) restricts an agency's collection, use and dissemination of personal information if the agency maintains an "information system." The Data Act also affords certain rights to data subjects when an agency maintains personal information in an information system. See [Code § 2.2-3803\(A\)\(5\)](#). Agencies maintaining information systems also must make a report of the existence of the system that includes [***9] "a description of the nature of the data in the system and the purpose for which it is used." [Code § 2.2-3807](#). In short, an agency is subject to certain legal obligations if it maintains an "information system." [*262] If an agency does not maintain an information system as defined by the Data Act, those strictures do not apply.

In *Neal I*, we held that "an agency's 'record-keeping process' is an 'information system' [**127] if it contains both 'personal information and the name, personal

number, or other identifying particulars' of an individual." [Id. at 347](#). We determined that "a license plate number may be an 'identifying particular' because it has the potential to identify the individual to whom the plate number is registered in the same way a 'name' or 'personal number' identifies the individual to which it is assigned." [Id. at 348](#). Based on the record before us, which came to us on summary judgment, we lacked a sufficient record to determine "whether a sufficient link can be drawn to qualify a license plate number as an 'identifying particular.'" *Id.* Consequently, we remanded the case to the circuit court to determine "whether the total components and operations of the ALPR record-keeping process provide a means through which [***10] a link between a license plate number and the vehicle's owner may be readily made." *Id.*

III. PROCEEDINGS ON REMAND.

On remand, the circuit court heard evidence concerning the Police Department's ALPR record-keeping process. The evidence established that the same computer in a police vehicle that hosts ALPR software also contains software programs that are capable of accessing DMV registration data, VCIN criminal information, and NCIC criminal information about motor vehicles and their owners and operators. The DMV database is maintained by the Virginia Department of Motor Vehicles, VCIN is maintained by the Virginia State Police, and the Federal Bureau of Investigation maintains the NCIC database. ALPR operators who obtain a license plate number can readily access information from these separate databases from the same computer that allows them to access the ALPR system.

The circuit court issued a letter opinion in which it concluded that the ALPR record-keeping process constituted an "information system" under [Code § 2.2-3801](#). The circuit court found that "the ALPR record-keeping process does not *itself* gather or directly connect to 'identifying particulars' of a vehicle owner." "[W]hile an officer [***11] can access all [of those] databases from the same computer, human intervention is required to match personal, [*263] identifying information from one database with the license plate number in the ALPR database." "If an officer acquires a license plate number from the ALPR software on the [laptop]" and wants to search that information in the NCIC, VCIN, or DMV databases, the officer must take several additional steps. The officer must first "clos[e] out of the ALPR software." Then, the "officer must log into a separate software program called I/MOBILE with a unique state-issued user ID, which is separate from

the Fairfax County user ID." Once an officer has logged into I/MOBILE, "[t]here is a tab [he or she] would click on that would bring up" those databases. The circuit court found that "no less than two computer programs and three passwords" are required before an officer can take information maintained in the ALPR system and use that information to find "the name, personal number, or other identifying particulars of a data subject." Nevertheless, finding that the ALPR system provides a means through which a link to the identity of a vehicle's owner can be readily made, the circuit court [***12] concluded that the ALPR record-keeping process is subject to the Data Act when in passive use.

The circuit court entered an order that "permanently enjoined [the Police Department] from the passive collection, storage and use of [ALPR] data." The court awarded Neal's attorneys \$75,000, out of a fee submission requesting \$642,569.75 in fees.

The Police Department appeals, asking us to overturn the circuit court's conclusion that its retention of license plate data qualifies as an "information system" as defined in the Data Act. For his part, Neal appeals from the circuit court's fee award, which greatly reduced the fees sought by his attorneys. We awarded both parties an appeal.

ANALYSIS

Modern technology enables governments to acquire information on the population on an unprecedented scale. National, state, and local governments can use that information for a variety of administrative purposes and to help apprehend dangerous criminals. But knowledge is power, and power can be [**128] abused. "Well managed, responsible data systems are as essential to the orderly and efficient operation of modern business, industry and government as uncontrolled, unrestricted gathering of total information [*264] dossiers [***13] about total populations are antithetical to a free society." Va. Advisory Legislative Council, Computer Privacy and Security, Va. S. Doc. No. 27 at 11 (1976). Mindful of the risk of abuse, however, the General Assembly enacted the Data Act to impose certain obligations and restrictions on Virginia governmental agencies with respect to the information they gather and to confer certain rights on Virginians. In the words of the Data Act, "[i]n order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals." [Code § 2.2-3800\(B\)\(4\)](#).

In resolving this case, our task is not to reach the right public policy balance by weighing competing demands for efficiency and security against considerations of privacy. Our duty is more modest: we must determine from the text and structure of the Data Act where the legislature has drawn the line.

I. THE ALPR SYSTEM DOES NOT SATISFY THE STATUTORY DEFINITION OF AN "INFORMATION SYSTEM" BECAUSE IT DOES NOT CONTAIN "THE NAME, PERSONAL NUMBER, OR OTHER IDENTIFYING PARTICULARS OF A DATA SUBJECT."

Under well-established principles, an issue of statutory interpretation [***14] is a pure question of law which we review de novo. [Conyers v. Martial Arts World of Richmond, 273 Va. 96, 104, 639 S.E.2d 174 \(2007\)](#). The operative facts are not in dispute. We must resolve a question of law: does the ALPR system qualify as an "information system" because it contains "the name, personal number, or other identifying particulars of a data subject."

[Code § 2.2-3801](#) defines an "information system" as follows:

"[i]nformation system" means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

There is no dispute that the ALPR system captures license-plate numbers and records images of the vehicle, along with [*265] the date, time, and GPS location where the information was recorded. We concluded in *Neal I* that a license plate alone is not "personal information" under the Data Act; however, we concluded that the images of the vehicle, its license plate, and the vehicle's immediate surroundings, along with the GPS location, time, and date when the image was captured did constitute "personal information." [Neal I, 295 Va. at 346-47](#). On remand, the circuit court [***15] found that "the ALPR record-keeping process does not *itself* gather or directly connect to 'identifying particulars' of a vehicle owner" Identifying particulars can be gleaned only from other databases, maintained by other agencies, that an officer has to access separately from the ALPR system. In *Neal I*, we said the agency's record-keeping process must contain "both 'personal information' and the 'name, personal number, or other identifying particulars' of an individual" in order to constitute an "information system."

Neal I, 295 Va. at 347 (quoting Code § 2.2-3801) (emphasis added). The facts as found by the circuit court make it clear that the ALPR database itself does not contain the name, personal number, or other identifying particulars of an individual. Therefore, the ALPR system *itself* does not include the things that would bring it under the strictures of the Data Act. Based on these facts, we conclude that the Police Department's passive use of the ALPR system to capture license plates, photographs of the vehicles, and the date, time, and GPS location of the vehicles do not run afoul of the Data Act.

Neal does not dispute the fact that the ALPR system does not contain the personal details specified in [***16] the Data Act. Instead, he contends that the "record-keeping process" under the Data Act includes information gleaned by an officer after the officer logs off of the ALPR system and separately logs on to other databases maintained by [**129] other agencies to learn additional information. We do not agree. The text of the statute covers "a record-keeping" process. Code § 2.2-3801. "Keeping" is "the act of one that keeps." Webster's Third New International Dictionary 1236 (2002). Since we are dealing with records, to "keep" as intended by the Data Act is to "preserve, maintain" or to "maintain a record." *Id.* at 1235; see also Black's Law Dictionary 1039 (11th ed. 2019) (a "keeper" is "[s]omeone who has the care, custody, or management of something and who [usually] is legally responsible [*266] for it."). There is no evidence that upon searching for information in separate databases, the Police Department is "keeping" any of this information within the ALPR system. The ability to query data in a variety of databases does not offend the Data Act if none of that data is kept in the ALPR system. Having access to data is not the same as "keeping" it. Other provisions of the Data Act support this reading. For example, Code § 2.2-3800(C) addresses [***17] obligations of "[r]ecordkeeping agencies of the Commonwealth." Code § 2.2-3800(C)(8) requires "[a]ny agency holding personal information [to] assure its reliability and take precautions to prevent its misuse." (emphasis added). The strictures of the Data Act contemplate accountability and responsibility by an agency for the data it keeps — not data it can query from other sources. Code §§ 2.2-3800, 3803.

Furthermore, the Data Act defines an "information system" as "the total components and operations of a record-keeping process" — singular. Code § 2.2-3801 (emphasis added). Of course, record-keeping may involve multiple inputs from multiple sources, such as

direct downloads from the State Police, and possibly from other sources, as well as manual inputs from an operator. Nevertheless, "a record-keeping process," singular, cannot plausibly consist of a combination of multiple separately generated and maintained systems. In *Neal I*, we referred on multiple occasions to the Police Department's "ALPR record-keeping process." Neal I, 295 Va. at 348-50. But "a record-keeping" process for ALPR does not include logging off of the ALPR system and separately logging on to other databases to query their contents. Thus, a plain language reading of the words "a record-keeping [***18] process" does not support Neal's expansive reading.

Moreover, the facts are undisputed that these databases, such as the VCIN, NCIC, or DMV databases, are maintained by other agencies. The Data Act defines and regulates the actions of an "agency." See Code § 2.2-3801 (defining "agency"). The Data Act imposes obligations on an agency with respect to the data it collects and maintains. Code § 2.2-3803 (imposing duties on "[a]ny agency maintaining an information system that includes personal information"). As the Police Department points out, interpreting "record-keeping process" and "information system" in a way that includes databases maintained by *other agencies* cannot be squared with the [*267] structure and requirements of the Data Act. For example, the Data Act requires an agency to (1) "[m]aintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to ensure fairness in determinations relating to a data subject," Code § 2.2-3803(A)(4); (2) "[m]aintain a list of all persons or organizations having regular access to personal information in the information system," Code § 2.2-3803(A)(6); (3) "[m]aintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete [***19] and accurate record, including identity and purpose, of every access to any personal information in a system," Code § 2.2-3803(A)(7); and (4) "[e]stablish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security," Code § 2.2-3803(A)(9). In order to fulfill these obligations, the Data Act necessarily presupposes that the agency controls the components and operations of the record-keeping process. See Code § 2.2-3806(A)(5)(a) (referencing "[t]he agency maintaining the information system"); *id.* § 2.2-3806(A)(5)(e) (same). The Data Act imposes restrictions and obligations on "an agency." Code § 2.2-3803. It does not contemplate holding an agency accountable

for the information systems of other agencies.*

[130]** To resist this construction of the Data Act, Neal points to the fact that the definition of "information system" encompasses "information collected or managed by means of computer networks and the Internet." [Code § 2.2-3801](#). However, the statutory text is clear that not all information that is "collected or managed by means of computer networks and the Internet" is swept into an "information system." The information that counts, for purposes of the Data Act, is information, from whatever source, that is part of an agency's "record-keeping process." Information **[***20]** from a separate database that is queried but not stored by a particular record-keeping process is not part of a record-keeping process under the act. The same is true of the phrase "the total components and operations" of a "record-keeping process." [Code § 2.2-3801](#). Under the statutory definition, "the total components and operations" that are relevant are those of "a record-keeping process." The definition of "information system" does not sweep in all components and **[*268]** operations that an agency has access to, or components and operations that in some way support a particular crime-fighting or public protection task.

Neal also contends that the word "manual" in the definition of "information system" includes the actions of an officer. Under this suggested interpretation, an information system includes situations when an officer obtains a license plate through ALPR, and then signs on to a separate database to glean information about the potential driver of a car, or even makes a telephone call to find out more information. This broad reading of the term "manual" is counterintuitive. The word "manual," under the statutory text, refers to the manual inputting of data within a specific record-keeping process, **[***21]** not the ability of an operator to log on to a separate system to learn additional information. See [Code § 2.2-](#)

* Neal argues that the Police Department failed to argue for below, or offer evidence in support of, a finding that the Data Act would be unworkable if interagency databases like the NCIC/VCIN/DMV databases were included within the total components and operations of the ALPR because they are not controlled locally by the Police Department. Therefore, he maintains, this argument was waived. We disagree. This is a statutory construction point, not an evidentiary issue. The text of the Data Act holds an agency accountable for its own information systems, not those of others. The fact that an agency may or may not be able to cooperate with another agency is beside the point when determining whether the Data Act applies to a specific information system.

[3801](#).

Neal advances a number of other contentions. He points to the fact that the ALPR system downloads a hot list from the State Police's VCIN database. If the hot list contained the type of information covered by the Data Act, Neal would have a point. The hot list, however, consists of full or partial license plate numbers. It contains no name, personal number, or other identifying particular of a data subject that would trigger the application of the Data Act to the ALPR system.

Neal also contends that the Police Department's SOP establishes that the ALPR system is an "information system" under the Data Act. That is so, he argues, because the SOP shows that the Police Department obtains information from other databases and directs the users of the ALPR system to use those resources to verify the correctness of the license plate information in the ALPR system. The SOP lends no support to the contention that the separate databases, such as VCIN or NCIC, are part of "a," singular, ALPR "record-keeping process." These separate databases certainly facilitate the investigative process by confirming **[***22]** the accuracy of a hit generated by the ALPR system, but they are not part of the ALPR system and do not form part of its record-keeping process. Neal's argument conflates the ultimate goal of the ALPR system — accurately locating suspects or stolen vehicles — with the ALPR system itself.

[*269] Finally, Neal asserts that the Data Act is a remedial statute, and, therefore, we should construe it broadly. However, we are not at liberty to stretch the meaning of a statute in a manner that would contravene the legislature's intent. See, e.g., [Faulkner v. Town of South Boston, 141 Va. 517, 524, 127 S.E. 380 \(1925\)](#) (observing that "[c]ourts cannot read into a statute something that is not within the manifest intention of the legislature, as gathered from the [language of the] statute itself" and that "[t]o depart from the **[**131]** meaning expressed by the words [in a statute] is to alter the statute[:] to legislate and not to interpret"); [Low Splint Coal Co. v. Bolling, 224 Va. 400, 404, 297 S.E.2d 665 \(1982\)](#) ("Liberal construction" of a statute "may not be used to amend a statute by changing the meaning of the statutory language."). That intent is manifested by the text and structure of the statute which, as explained above, does not apply to the ALPR system as currently configured.

We remanded this case to determine "whether the total components **[***23]** and operations of *the ALPR record-*