User Name: James Klahr
Date and Time: Monday, November 24, 2025 11:58 AM EST
Job Number: 268868559

Document (1)

1. *United States v. Jackson*
   Client/Matter: Kirksville
   Search Terms: privacy & flock camera
   Search Type: Terms and Connectors
   Narrowed by:

Content Type	Narrowed by
	-None-

United States v. Jackson

United States District Court for the District of Kansas

May 29, 2025, Decided; May 29, 2025, Filed

Case No. 24-cr-10010-JWB

Reporter
2025 U.S. Dist. LEXIS 101960 *; 2025 LX 158463; 2025 WL 1530574

UNITED STATES OF AMERICA, Plaintiff, v. SIDNEY JAMAR JACKSON, Defendant.

Counsel: [*1] For Sidney Jamar Jackson, Defendant: Ellen Albritton, LEAD ATTORNEY, Office of the Federal Public Defender, Wichita, KS; Ellen Christine Bertels, LEAD ATTORNEY, Federal Public Defenders, District of Kansas, Wichita, KS.

For USA, Plaintiff: Molly M. Gordon, LEAD ATTORNEY, Office of United States Attorney - Wichita, Wichita, KS.

Judges: JOHN W. BROOMES, UNITED STATES DISTRICT JUDGE.

Opinion by: JOHN W. BROOMES

Opinion

MEMORANDUM AND ORDER

This matter came on for hearing on April 16, 2025, on Defendant's motion to suppress evidence obtained from the warrantless use of the Flock Safety, Inc. ("Flock Safety") system of license-plate-reading cameras and search database ("Flock" or "Flock System"). Defendant argues that the warrantless use of the Flock System violates the *Fourth Amendment's* prohibition against unreasonable searches. (Doc. 22.) At the hearing, the court granted Defendant's three motions to take judicial notice of 1) Google Maps of the Wichita, KS area, 2) Flock Safety's internet page, and 3) prior testimony of Captain Casey Slaughter of the Wichita Police Department. (Doc. 43, 44, 45; Def. Ex. H.) The court then heard testimony regarding the use and deployment of the Flock System in and around Wichita, Kansas. The court heard **[*2]** testimony from five witnesses. The court first heard testimony from Defendant Sidney Jackson. It then heard testimony from two officers who participated in the use of the Flock System on January 3, 2024: Jorge Fernandez and Jonathan Marr. Afterwards it heard from Mike Molina, who is an attorney for Flock Safety, and then from Captain Casey Slaughter. After hearing all the testimony, the court took the motion to suppress under advisement. For the reasons set forth herein, Defendant's motion to suppress is denied.

I. Facts

After hearing testimony and receiving exhibits into evidence, the court finds the following facts in accordance with *Rule 12(d) of the Federal Rules of Criminal Procedure* and based on a preponderance of the evidence. *United States v. Shrum, 908 F.3d 1219, 1229 n.7 (10th Cir. 2018)*.

A) Flock System use and deployment

Flock Safety is a technology company based out of Atlanta, Georgia, that provides law enforcement with a system of automatic license plate reading ("ALPR") cameras and an affiliated search database. Flock Safety's flagship product, "LPR" (formerly called "Falcon") cameras, are black, oval shaped cameras which are powered by an attached battery and a solar panel. These cameras can be mounted to dedicated 12- to 14-foot-high Flock poles or attached to other pre-existing utility **[*3]** poles. Like traditional ALPR's, Flock's cameras are stationary and capture high speed pictures of every rear-facing license plate that passes by the camera twenty-four hours a day, seven days a week, so long as the ***Flock camera*** is operational. Flock Safety also creates "deployment plans" for clients to help find optimal placement for ***Flock cameras***.[1]

[1] These Flock Safety deployment plans consider geographic limitations to placing cameras, such as access to sunlight or wireless LTE network coverage to keep the ***Flock cameras***

However, ***Flock cameras*** have an intentionally narrow field of view, with motion detection triggering up to 75 feet away and a field of view around 20 feet wide. Usually, these cameras can cover two to four lanes of traffic. Flock Safety also offers pan tilt zoom video cameras which record video in addition to pictures, and a temporary Falcon Flex camera which is powered by a battery and intended for use at large events or other temporary settings. In total, there are currently close to 100,000 ***Flock cameras*** that have been deployed around the country. Although Flock retains ownership of the hardware, all photos and data are owned by the local agency or Flock customer.

Flock cameras use infrared technology to capture license plate numbers, time and geographic location, and a still image of each passing vehicle. The camera takes numerous highspeed **[*4]** photos of passing cars and then a Flock-created artificial intelligence pulls the best photo to upload to the Flock System. In addition to license plate numbers, ***Flock cameras*** can also identify the make, model, color, resident status, type of license plate, and any damages or alteration of the subject vehicle (such as bumper stickers or a roof rack). Although the Flock photographs are able tell the direction that a vehicle is traveling at the time the photo is taken, the Flock System cannot discern the speed of the vehicle, the identity of any vehicle occupant (apart from some camera angles showing that the vehicle may have multiple occupants), or the end destination to which any vehicle is travelling. ***Flock cameras*** are also able to photograph motorcycles and bicycles, though users cannot initially search for bicycles in the Flock System.

After a ***Flock camera*** takes a photo of a passing vehicle, these photos are then uploaded via a wireless data network to Flock Safety's encrypted cloud servers with a latency upload period of a couple of seconds. Upon upload, Flock's proprietary software runs a "vehicle fingerprint" on any vehicle in the photo and uses a machine learning algorithm to **[*5]** look for the vehicle identifiers stated above. After this upload and processing, local law enforcement can access the photographs via an online dashboard and search the resulting photo database by the cataloged vehicle characteristics and by specific license plate numbers. Law enforcement officers can also narrow their search radius by geographic location or by an area search. It should be noted that Flock Safety cannot access this data; rather local users are the only ones who can access the data from their local ***Flock cameras***. These Flock photos are only retained on the cloud for 30 days, and after that time, they are permanently deleted unless they are saved to a local hard drive by a Flock user.[2] And Flock Systems are not limited to only law enforcement. Private companies, homeowners' associations ("HOA"), and neighborhoods can also install and use Flock Systems, and Flock Safety claims on their website to be used by more than 5,000 communities.[3] These non-law enforcement groups can set their systems to identify residents vs. non-residents after the residents register their vehicle license plates with their neighborhood's Flock Safety system. However, the searchable Flock database **[*6]** is limited to authorized law enforcement personnel, and all access to the Flock System is recorded and subject to audit.[4]

Besides the data that is native to an individual municipality or HOA, Flock allows entities to share data with each other to create a broad, searchable network of aggregated data. This network can include other law enforcement agencies in the same state as well as agencies from other states. Any two municipalities can sign a memorandum of understanding (MOU) to share the data captured by each of their local Flock Systems with one another, thereby increasing the geographic reach and volume of data available to any authorized Flock user for that local system. Nevertheless, Flock Safety claims that it complies with state data laws,

functional, but also consider local data about where cameras can be placed for the highest volume of traffic or crime deterrence. Generally, Flock recommends placing cameras on main throughways, at the ingress and egress point of shopping centers, or in high crime areas. However, the goal is not to put a camera on every intersection.

[2] According to testimony at the suppression hearing from Mike Molina, some jurisdictions require retention of historic data longer than 30 days by statute. In these jurisdictions, Flock Safety follows the guidelines set by statute, but in all other jurisdictions, the data is deleted after 30 days.

[3] Mike Molina testified at the suppression hearing that Flock Safety started its business by selling cameras to communities and HOAs for the purpose of providing evidence should a crime be committed within the community. They then expanded their business model to include traditional ALPRs for law enforcement and more recently cameras for commercial customers.

[4] Mike Molina also testified that Flock Safety and Axon had a partnership, where Flock could run its vehicle fingerprint algorithm through Axon cameras and these cameras would also produce searchable images in the Flock database. However, he also testified that this relationship is currently in flux and is scheduled to expire later in 2025.

which sometimes limit the amount of data that can be shared between municipalities or law enforcement agencies. Yet, apart from these various state laws, data sharing decisions are left to the local policies of the individual law enforcement agencies that are Flock Safety clients. For HOAs and private communities with local ***Flock cameras***, they do not have to sign a MOU with local law enforcement to share data. Rather, they can choose to share **[*7]** their data with local law enforcement in the Flock System and can toggle this feature on or off. This characteristic is native to the Flock System network and this community data will be both shared directly to and searchable by local law enforcement if it is toggled on.

In addition to aggregating data, the Flock system also provides real-time alerts for vehicles which are placed on a Flock "Hot List." A Hot List can be locally created by a Flock user to target specific vehicles, and it is automatically sent to a local Flock System when a vehicle is identified from the Federal Bureau of Investigation's National Crime Information Center ("NCIC"). When a vehicle on a Hot List is identified, law enforcement is given real-time notification about the location of that vehicle. This information can be provided on the Flock online dashboard or pushed to a mobile phone. Notifications from a Hot List are pushed to a Flock System user several seconds after a Flock photo is taken and the vehicle algorithmically identified. Since vehicles are moving when they are photographed by ***Flock cameras***, a Flock System Hot List hit could potentially be a stale lead by the time officers arrive at the location. **[*8]** Nevertheless, Hot Lists can be used by law enforcement to narrow a geographic search on the ground and to confirm a general area to try and locate a target vehicle. If a local law enforcement agency has signed a MOU with another agency or municipality, local Hot Lists can also search the wider Flock System network for a target vehicle.

The City of Wichita (the "City" or "Wichita") and the Wichita Police Department ("WPD") have utilized license plate readers since 2014 and have grown the program from using mobile scanning to also deploying Flock stationary cameras. Although the City initially used cameras from a different manufacturer for license plate scanning, it switched to the Flock System at the end of 2020. They initially began with a demo of 66 ***Flock cameras*** deployed around the city, and then increased the ***Flock camera*** count to 110 cameras when the demo was successful. By January 2024 (which is the month of the arrest underlying this motion), the City had increased their camera count to 160 ***Flock cameras***. Since 2024, the City has increased the number of Flock stationary cameras in their network from 160 to 190. This number is driven by budget or other funding concerns, and with **[*9]** more funding the City and WPD hope to deploy even more ***Flock cameras***. Within Wichita, there are roughly 500 lane miles of road,[5] which means that the ***Flock camera*** coverage is roughly one camera per 2.6 lane miles of road.

Given these inherent geographical limitations, the City and WPD used data analytics to strategically place ***Flock cameras*** in high crime areas or on roads with a high volume of traffic. This deployment strategy led the City and the WPD to capture images of over 775,000 vehicles in the month of February 2025 alone. (*See* Def. Ex. A.) Access to the Flock System in Wichita is limited to commissioned law enforcement officers and not generally available to the public under the Kansas Open Records Act. Moreover, any unauthorized use of the Wichita Flock System can lead to termination and criminal prosecution. Within the WPD, authorized users of the Flock System receive several hours of instruction prior to accessing the Flock database. Additionally, the WPD uses Flock daily in a wide variety of investigations, from simple cases of shoplifting to complex cases of homicide and kidnapping. The WPD uses the **[*10]** historical location data from the Flock System to help build timelines and track movements related to criminal investigations. However, the tracking is not continuous. The data is limited to only those locations where a ***Flock camera*** is stationed, and it is possible to evade detection by driving in areas without ***Flock camera*** coverage.

Testimony from Capt. Slaughter confirmed that his WPD property crimes task force alone uses Flock on an hourly basis to assist in ongoing investigations or detect wanted vehicles for intervention and interception. On the day of the hearing, the Flock transparency page for the WPD showed that the WPD had run 2,705 Flock searches and had 37,113 Hot List hits in the 30 days prior to April 16, 2025 (though the majority of the Hot List hits were automatically created by Flock from the

---

[5] A lane mile is the number of miles of pavement going in one direction on a road within a single lane. Miles of roadway multiplied by the number of lanes results in the total lane miles for a given road. *See* Road Terms and Definitions, MICH. DEP'T OF TRANSP., https://www.michigan.gov/mdot/About/mdot-road-terms-and-definitions (last visited May 28, 2025). *See also* Bryant Walker Smith, *Managing Autonomous Transportation Demand*, 52 Santa Clara L. Rev. 1401, 1422 n.12 & n.13 (2012).

NCIC according to Capt. Slaughter). However, according to WPD policy, searching the Flock System or receiving an alert from the Flock System does not give probable cause or reasonable suspicion to stop a target vehicle. The City has MOUs with approximately 150 other jurisdictions across the country, but nearly all the other jurisdictions with which Wichita shares data are in Kansas, **[*11]** Missouri, Oklahoma, and Texas. Additionally, local HOAs and national businesses, such as Lowe's, share data with the Wichita Flock System. However, this shared data is only available to the Wichita Flock System and cannot be shared with other law enforcement agencies with which Wichita has signed an MOU. According to Capt. Slaughter, all local HOAs that have a Flock System currently share data with the WPD.

B) Events of January 3, 2024

To help meet its mission and mandate, the United States Drug Enforcement Administration ("DEA") creates local domestic task forces, which are cooperative efforts between the DEA and local law enforcement agencies, to maximize resource usage and access local knowledge. One such taskforce is based out of Wichita and Jorge Fernandez is a DEA Agent and Task Force Officer ("TFO") working out of this Wichita DEA office. Around 12:30 p.m. on January 3, 2024, TFO Fernandez received a phone call from Special Agent Colin Strickland in the Omaha, Nebraska, DEA office. On this phone call, Agent Strickland informed TFO Fernandez that a white, four-door sedan with Nebraska plates and registered to Adam Safar was in Wichita to pick up five pounds of methamphetamine. **[*12]** Agent Strickland also said that Adam and a person named "Sid" were going to be driving the vehicle, and that two females were also likely to be present.[6]

Since TFO Fernandez did not have authorized access to any local Flock System, he passed this vehicle information to Officer Jonathan Marr, who was a member of the Haysville Police Department and assigned to the DEA taskforce. As part of his employment with the Haysville Police Department, Officer Marr had access to the Haysville Flock System.[7] Since only members of local law enforcement are allowed to access their Flock Systems, the DEA taskforce must rely on local officers assigned to the taskforce to use any functionality of a Flock System when they want to search for a vehicle.

When Officer Marr initially ran a Flock search on the very generic vehicle descriptions of a white sedan with Nebraska plates, the Wichita Flock System returned numerous results, and the taskforce began to run individual plates to see if any were registered to Adam Safar. Agent Strickland then called TFO Fernandez a second time and provided him with a list of specific vehicles registered to Adam Safar. Using this knowledge, the taskforce was able to refine their **[*13]** Flock search query by the known license plate numbers for vehicles registered to Adam Safar and the Wichita Flock System returned a positive hit on a white, four-door Chevy Cruz which had been driving in Wichita that day. However, the officers did not know the specifics of who was in the vehicle nor what the vehicle contained; instead, they only knew that the vehicle itself was in Wichita.

Once the officers confirmed that a vehicle matching the description from Agent Strickland was in Wichita, four DEA agents in separate cars and three WPD community resource team members deployed onto the city streets to locate the vehicle. Officer Marr then set up a Flock Hot List for this target Chevy Cruz in the Wichita Flock System, and anytime the Wichita Flock System got a hit on this vehicle, he relayed the approximate location and direction of travel to all the officers on patrol. After approximately nine Flock System hits and four hours of searching (*see* Def. Ex. S), the taskforce finally found the target vehicle around 4:30 p.m. parked at a smoke shop on the southwest corner of 13th and Oliver streets in Wichita. The officers then followed the vehicle and surveilled it for several hours, until **[*14]** officers observed the target vehicle run a red light. At this point, officers initiated a traffic stop on the target vehicle, whereupon they discovered Defendant Sidney Jamar Jackson sitting in the front passenger seat. During the stop, a drug dog alerted to the presence of narcotics in the car and the officers searched the vehicle. This search led them to find approximately 2.38 kilograms of methamphetamine inside a bag in the trunk. Defendant was then arrested along with the three other occupants of the car.

---

[6] Defendant does not challenge the sufficiency of this tip from Agent Strickland as a basis for officers to try and locate the target vehicle; instead, Defendant's challenge is limited to only the taskforce's use of the Flock System.

[7] At the time of Officer Marr's use of the Haysville Flock System, Wichita and City of Haysville had signed a MOU that allowed Haysville officers to access data from Wichita's Flock System and vice versa.

On January 23, 2024, a federal grand jury returned a one-count indictment against Defendant for possession with intent to distribute 50 grams or more of methamphetamine in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A). (Doc. 7.) Defendant then filed the present motion, arguing that the warrantless use of the Flock System violates the Fourth Amendment's prohibition against unreasonable searches. (Doc. 22.) The government contends that Defendant had no reasonable expectation of ***privacy*** in his movements on public roads and that the officers' limited use of the Flock database did not impinge on the totality of Defendant's movements. (Doc. 26.)

II. Analysis

The Fourth Amendment provides that the "right of the people to be secure in their persons, **[*15]** houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. When a defendant challenges a search as violative of his Fourth Amendment rights, the court must consider two primary factors: 1) whether the defendant manifested a subjective expectation of ***privacy*** in the area searched and 2) whether society is prepared to recognize that expectation as objectively reasonable. United States v. Erwin, 875 F.2d 268, 270 (10th Cir. 1989). Given that Fourth Amendment rights are personal rights, every defendant who seeks to suppress evidence in a criminal matter must show that he has standing to challenge the illegality of any search or seizure. Rakas v. Illinois, 439 U.S. 128, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978). In this case, Defendant was not the owner of the target vehicle, nor was he the driver. However, "[d]rivers and passengers have similar interests in seeing that their persons remain free from unreasonable seizure." Erwin, 875 F.2d at 270; *see also* Brendlin v. California, 551 U.S. 249, 251, 127 S. Ct. 2400, 168 L. Ed. 2d 132 (2007) ("We hold that a passenger is seized [when a traffic stop occurs] and so may challenge the constitutionality of the stop."). Although the Tenth Circuit has held that a passenger needs a possessory interest, or a property interest, in a vehicle to challenge any evidence obtained from it, *see* United States v. DeLuca, 269 F.3d 1128, 1132 (10th Cir. 2001), the challenge raised by Defendant here involves a fundamental question of "permeating police **[*16]** surveillance," which is at the core of what the Fourth Amendment was intended to protect against. United States v. Di Re, 332 U.S. 581, 595, 68 S. Ct. 222, 92 L. Ed. 210 (1948). Accordingly, the court concludes that Defendant has standing to challenge the use of the Flock System to track his movements.

A) Defendant does not have a reasonable expectation of ***privacy*** with regards to the use of an Automated License Plate Reader under the *Katz* Test

To assess whether a "reasonable expectation of ***privacy***" exists, the Supreme Court has applied Justice Harlan's two-fold approach as explained in his concurrence in Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).[8] To claim a ***privacy*** interest under the Fourth Amendment, a defendant first must "have exhibited an actual (subjective) expectation of ***privacy***," and second, that expectation must "be one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361 (Harlan, J., concurring). *See also* United States v. Jacobsen, 466 U.S. 109, 113, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) (noting that unreasonable searches occur "when an expectation of ***privacy*** that society is prepared to consider reasonable is infringed"). This reasoning embodies the practical application of the Court's oft used phrase, "the Fourth Amendment protects people, not places." Katz, 389 U.S. at 351.

In this case, Defendant testified at the hearing that he did not know about the Flock System, its capabilities, or its deployment in Wichita, Kansas. **[*17]** However, he did testify that he believed that law enforcement could not track him without a warrant. This testimony by Defendant may satisfy the first requirement for a reasonable expectant of ***privacy***; namely, that the Defendant has a subjective expectation of ***privacy*** in his movements. However, the Katz test requires more than subjective belief; it requires that a defendant have a subjective expectation of ***privacy*** "that society is prepared to recognize as reasonable." Carpenter v. United States, 585 U.S. 296, 304, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018).

With regard to this second part of the Katz test,

---

[8] The court notes that Defendant's motion relies largely on Carpenter v. United States, 585 U.S. 296, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018), and the reasonable expectation of ***privacy*** derived from *Katz*. *See* id. at 304. Conversely, Defendant does not rely on propertybased theories of Fourth Amendment protection; thus, the court focuses its attention on the theories presented in this case. *See* id. at 406 (Gorsuch, J., dissenting).

Supreme Court jurisprudence has long held that a person travelling in an automobile on public thoroughfares has no reasonable expectation of ***privacy*** in his movements from one place to another. *United States v. Knotts, 460 U.S. 276, 281, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983)*. Visual surveillance of vehicles in plain view does not constitute an unreasonable search for *Fourth Amendment* purposes. *See, e.g., New York v. Class, 475 U.S. 106, 114, 106 S. Ct. 960, 89 L. Ed. 2d 81 (1986)* (involving inspection of vehicle identification number ordinarily visible from outside vehicle, but which was obscured from plain view by papers). This is true even if the surveillance is aided by technology which augments an officer's sensory faculties. *See United States v. Knotts, 460 U.S. at 282* (involving use of radio transmitter on container which was under visual surveillance to help track transport). "One **[*18]** 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." *Cardwell v. Lewis, 417 U.S. 583, 590, 94 S. Ct. 2464, 41 L. Ed. 2d 325 (1974)* (plurality opinion).

In line with this reasoning, the Tenth Circuit has held that license plates are "in plain view on the outside of the car" and as a result "no expectation of ***privacy*** was infringed" when police observe and run license plates on vehicles. *United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980)*. *See also United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989)* ("Because they are in plain view, no ***privacy*** interest exists in license plates"); *Becerra v. City of Albuquerque, No. 23-2053, 2023 U.S. App. LEXIS 29608, 2023 WL 7321633, at *2 (10th Cir. Nov. 7, 2023)* (holding that since a defendant "had no expectation of ***privacy*** in his license plate information, the officers did not conduct a *Fourth Amendment* 'search' by examining it"). As the Seventh Circuit opines, "observing and recording the registration number [is] not a search within the meaning of the *Fourth Amendment*." *United States v. Miranda-Sotolongo, 827 F.3d 663, 668 (7th Cir. 2016)*. Additionally, the police use of a license plate tag reader to scan a license plate is not violative of the *Fourth Amendment*. *United States v. Wilcox, 415 F. App'x 990, 992 (11th Cir. 2011)*. Indeed, the very purpose of having a license plate is to communicate identifying information to officers and state officials. **[*19]** *United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006)*. "The reasoning . . . of the Supreme Court . . . leads us to agree that a motorist has no reasonable expectation of ***privacy*** in the information contained on his license plate under the *Fourth Amendment*." *Id.*

This is not to say that a defendant never has any expectation of ***privacy*** in a vehicle. Indeed, "[a]n individual operating or traveling in an automobile does not lose all reasonable expectation of ***privacy*** simply because the automobile and its use are subject to government regulation." *Delaware v. Prouse, 440 U.S. 648, 662, 99 S. Ct. 1391, 59 L. Ed. 2d 660 (1979)*. Private conversations within the car are likely protected in the same way that the private conversations in the phone booth at issue in *Katz* were. However, because "[t]he exterior of a car . . . is thrust into the public eye, . . . to examine it does not constitute a 'search.'" *Class, 475 U.S. at 114*. Thus, under current guidance from the Supreme Court, Defendant does not have a reasonable expectation of ***privacy*** in his license plate or in his movements on roads which would make the actions of the police in using the Flock System to capture pictures of his license plate violative of the *Fourth Amendment*.

B) Law enforcement's limited use of the Flock System to track Defendant in one day is not violative of the *Fourth Amendment* under *Carpenter*

Although Defendant does not have **[*20]** a reasonable expectation of ***privacy*** in his movements in a vehicle, he contends that the Flock System, which captured the Chevy Cruz's movements on nine different occasions around Wichita on January 3rd, violated his expectation of ***privacy*** in the totality of his movements under the Supreme Court's 2018 decision of *Carpenter v. United States. 585 U.S. at 310*. In *Carpenter*, police used historical cell-site location information ("CSLI") obtained from a cell phone service provider to track the movements of a defendant over the course of 127 days. This data included 12,898 individual location points which "catalog[ed] [the defendant's] movements—an average of 101 data points per day." *Id. at 302*. This CSLI data was not only "detailed, encyclopedic, and effortlessly compiled" but also "continuously reveal[ed] [an individual's] location." *Id. at 309*. The Supreme Court held that although law enforcement may be able to track an individual's location for a short period of time, they could not "secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id. at 310* (citing *United States v. Jones, 565 U.S. 400, 430, 132 S. Ct. 945, 181 L. Ed. 2d 911* (ALITO, J.,

concurring in judgment)).[9] The Court held that individuals have a reasonable expectation of ***privacy*** "in the whole of their physical movements." **[*21]** *Id. at 310*. Defendant here argues that a search for a license plate number in the Flock System was akin to a search of historical cell-site location information, which the Supreme Court held in *Carpenter* required a search warrant. Defendant contends that the Flock System is comparable to the CSLI in *Carpenter* since (1) Flock provides highly detailed data of a sensitive nature to law enforcement, (2) Flock produces and stores huge quantities of data, (3) Flock's surveillance is widespread and indiscriminate, and (4) Flock's database allows law enforcement automatic and retrospective access to this data. Although there are certainly ***privacy*** concerns when any law enforcement agency possesses aggregated data for its use in surveillance, the court is not convinced that *Carpenter* applies to this case.

First, there is a distinct difference in the quantity and quality of the photos at issue in this case as opposed to the data at issue in *Carpenter*. In reaching its decision that law enforcement's use of CSLI data required a warrant, the Supreme Court considered *Fourth Amendment* precedent regarding GPS tracking. In particular, the Court paid special attention to the distinction between the cases of *Knotts* and *Jones*. In deciding **[*22]** that *Carpenter* fit within the GPS tracking framework of *Jones*, the Court held that the volume of data "provide[d] an intimate window into a person's life" such that the aggregation would provide law enforcement access to otherwise unknowable information. *Carpenter, 585 U.S. at 311*. This included access to private places and gave law enforcement a volume of information "as if [the government] had attached an ankle monitor to the phone's user." *Id. at 312*.

The Flock System at issue here lacks the wide and continuous tracking of a defendant which the Supreme Court has stated is constitutionally suspect. In this case, there were only nine distinct points where the Flock System captured the Chevy Cruz on camera, and these photographs occurred over the course of just one day. The photos did not show the identity of anyone inside the car, nor did the photos provide any insight into any intimate details of their personal lives. At best, the photos show that the car is occupied by multiple individuals, but there is no way for police to use this information to discern private details that would otherwise be covered by a reasonable expectation of ***privacy***. The police in this case did not even know the identity of Defendant until **[*23]** after the target vehicle was pulled over for a traffic stop. This stands in stark contrast to the thousands of datapoints and over one hundred days of surveillance in *Carpenter*, and the 2,000 pages of data over a 4—week period which the Supreme Court construed as a dragnet style of search in *United States v. Jones. 565 U.S. at 409 n.6*. "Ultimately, resolution of this issue focuses on 'the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance' from the ALPR.'" *United States v. Cooper, No. CR 23-131, 2025 U.S. Dist. LEXIS 1466, 2025 WL 35035, at *5 (E.D. La. Jan. 6, 2025)* (citing *Commonwealth v. McCarthy, 484 Mass. 493, 142 N.E.3d 1090, 1104 (2020)*). Thus, given the limited amount of information available to law enforcement, the court is not convinced that the amount of data derived from the Flock System is constitutionally suspect. And this court is not alone in reaching this conclusion. In evaluating similar questions on the extent of data obtained by ALPR systems, numerous courts have held that the use of ALPR systems is not violative of *Fourth Amendment* rights when faced with questions nearly identical to the ones raised by Defendant here.[10]

---

[9] In *U.S. v Jones, 565 U.S. 400, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)*, police placed a GPS-tracking device on a vehicle belonging to a suspected narcotics trafficker and then used that device to track the defendant's movements. *Id. at 402, 404*. The police recorded Jones' vehicle's movements over a four-week period, with the GPS providing over 2,000 pages of data on the vehicle's location with an accuracy of 50-100 feet. *Id. at 403*. The Court avoided the question of 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, the Supreme Court held that a search had occurred in violation of the *Fourth Amendment* because placing the GPS on Jones' car constituted a physical intrusion on a constitutionally protected area which necessitated a warrant. *Id. at 406-07*.

[10] *See United States v. Martin, 753 F. Supp. 3d 454, 456 (E.D. Va. 2024)*; *United States v. Cooper, No. CR 23-131, 2025 U.S. Dist. LEXIS 1466, 2025 WL 35035, at *6 (E.D. La. Jan. 6, 2025)* which deal specifically with the Flock System.

Other cases deal with ALPR systems generally and hold that their use does not violate a reasonable expectation of ***privacy***: *USA v. Rubin, 556 F. Supp. 3d 1123 (N.D. Cal. 2021)*; *United States v. Bowers, No. 2:18-CR-00292-DWA, 2021 U.S. Dist. LEXIS 196899, 2021 WL 4775977 (W.D. Pa. Oct. 11, 2021)*; *United States v. Brown, No. 19 CR 949, 2021 U.S. Dist. LEXIS 206153, 2021 WL 4963602 (N.D. Ill. Oct. 26, 2021)*; *United States v. Porter, No. 21-CR-00087, 2022 U.S. Dist. LEXIS 6755, 2022 WL 124563 (N.D. Ill. Jan. 13, 2022)*; *United States*

It is also instructive to look at cases where courts have found law enforcement surveillance violates the Fourth Amendment. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit faced a challenge **[*24]** to the city of Baltimore's Aerial Investigation Research program which used aerial photography to track movement across 90% of the city. 2 F.4th 330, 334 (4th Cir. 2021). This program used cameras that could capture 32 square miles per image per second and obtained 12 hours of coverage per day. *Id.* The Fourth Circuit ruled that this program of mass surveillance was a search under the Fourth Amendment and *Carpenter* and enjoined the program from continuing. Id. at 347-48. Similarly, the Fifth Circuit recently addressed the question of whether the use of Google's geofencing data constituted a search under the Fourth Amendment which required a warrant. United States v. Smith, 110 F.4th 817, 830 (5th Cir. 2024). Google maintains an extensive location history database by tracking a Google account user's location on average every two seconds, and Google stores this data for at least eighteen months. Id. at 823. Law enforcement began accessing this data to identify all Google users who were in a geographic area during a given time frame. Id. at 824-25. Using the *Carpenter* framework, the court found that the quantity and quality of data used to establish a user's location constituted a general warrant and was unconstitutional under the Fourth Amendment. Id. at 840.

Contrast these two clear examples of widespread mass surveillance with the limited surveillance of the Flock **[*25]** System in this case. It is true that the Flock System captures photographs of any car that passes a camera; however, the limited number of cameras means that the amount of data collected is incomplete and does not track the totality of an individual's movements. As persuasively noted by Judge Ambrose in the Western District of Pennsylvania, "[u]nlike the all-pervasive cell-site location data collection in *Carpenter*, and its 'all-encompassing' and 'near-perfect surveillance' of a cell phone user's comings and goings, the ALPR technology at issue captures only the public movements of vehicles that happen to pass by locations on a public street in view of an ALPR camera . . . Even in the aggregate, the ALPR cameras [sic] 'capability to capture multiple shots of a single vehicle and/or store historical data does not approach the near-constant surveillance of cell-phone users' public and private moves that so concerned the Court in *Carpenter*." United States v. Bowers, No. 2:18-CR-00292-DWA, 2021 U.S. Dist. LEXIS 196899, 2021 WL 4775977, at *3 (W.D. Pa. Oct. 11, 2021). Judge Milazzo in the Eastern District of Louisiana agreed, noting, "the data collected by the ALPR system is far more limited than CSLI. A person must actively pass by one of the cameras for any data to be collected and even then, only a small amount **[*26]** of information is collected and retained. Individual snapshots in certain locations at specific times 'hardly rise to the level of persistent, unceasing public surveillance that the courts found troublesome in *Carpenter*.'" United States v. Cooper, No. CR 23-131, 2025 U.S. Dist. LEXIS 1466, 2025 WL 35035, at *6 (E.D. La. Jan. 6, 2025) (citing United States v. Martin, 753 F. Supp. 3d 454, 473 (E.D. Va. 2024)). The above reasoning convinces the court that the amount of information currently obtained by the Flock System in Wichita is not the pervasive and continuous gathering of information with which the Supreme Court was concerned in Carpenter and Jones, but rather is the limited sort of information that augments law enforcement's natural abilities in Knotts. Ultimately, "the Constitution does not forbid the government from using technology to conduct lawful investigations more efficiently." United States v. Gregory, 128 F.4th 1228, 1235 (11th Cir. 2025).

Second, ***Flock cameras*** do not capture images of people, but rather the Flock System is limited to capturing only pictures of vehicles. As a result, data obtained from ***Flock cameras*** is very different from data obtained from cell phones. At the hearing, Mike Molina testified that the Flock System may be able to gain some information about the passengers in a vehicle if they are sticking their hands out the window at the time

---

v. Graham, No. CR 21-645 (WJM), 2022 U.S. Dist. LEXIS 163818, 2022 WL 4132488 (D.N.J. Sept. 12, 2022), *aff'd*, No. 23-3197, 2025 U.S. App. LEXIS 2110, 2025 WL 342190 (3d Cir. Jan. 30, 2025); *United States v. Toombs, 671 F. Supp. 3d 1329 (N.D. Ala. 2023)*; United States v. Jiles, No. 8:23-CR-98, 2024 U.S. Dist. LEXIS 34957, 2024 WL 891956 (D. Neb. Feb. 29, 2024).

But cf. Schmidt v. City of Norfolk, No. 2:24CV621, 2025 U.S. Dist. LEXIS 21096, 2025 WL 410080, at *7 (E.D. Va. Feb. 5, 2025) (holding in a federal civil case against the use of Flock Systems in Norfolk, Virginia, that the plaintiff survived a motion under Fed. R. Civ. Proc. 12(b)(6) since "well-pled facts plausibly allege a violation of an objectively reasonable expectation of ***privacy***"); Commonwealth v. Bell, 113 Va. Cir. 316 (2024) ("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"). However, these two cases appear to be outliers within the broader movement of the judiciary.

a photograph is taken by a ***Flock camera***. However, the **[*27]** Flock System cannot identify any biographical or biological information which would allow law enforcement to track individuals instead of just their vehicles. Ultimately, the ***Flock cameras*** "exposed no details about where [Defendant] traveled, what businesses he frequented, with whom he interacted in public, or whose homes he visited, among many other intimate details of his life." *United States v. Brown, No. 19 CR 949, 2021 U.S. Dist. LEXIS 206153, 2021 WL 4963602, at *3 (N.D. Ill. Oct. 26, 2021)*. Instead, a search of the Flock System "only reveals when, where, and in which direction a certain vehicle was driving—information of limited value, and data from which it is difficult to discern an individual's familial, political, professional, religious, and sexual associations." *United States v. Jiles, No. 8:23-CR-98, 2024 U.S. Dist. LEXIS 34957, 2024 WL 891956, at *19 (D. Neb. Feb. 29, 2024)*. Given that the Flock System does not capture any biographical details of any individuals apart from incidental details to driving on a public road, using the Flock System to track a vehicle is not the same kind of personal search that the Supreme Court critiqued in *Carpenter*.

Moreover, it is instructive to observe the fundamental differences between the nature of the surveillance in cases like *Carpenter* and *Jones* versus the surveillance at issue in this case. In *Carpenter*, the use of CSLI data allowed the government to continuously **[*28]** monitor the movements of essentially everyone. As shown by the facts in that case, once suspicion focused on Carpenter, the government was able to retrospectively glean information about the totality of Carpenter's movements over a wide span of time. Similarly, the GPS tracker in *Jones* allowed the government to track Jones' movements all the time, at least so long as he was travelling in the target vehicle. By contrast, the Flock System, as employed in this case, allows the government to monitor the movements of all the vehicles in Wichita at limited points in time. The data gathered is limited to the locations of particular vehicles at specific points in time, with no real indication of who is in those vehicles. When armed with that information in the present case, law enforcement obtained only nine data points on the Chevy Cruz over the four-hour period that it took them to find the target vehicle and commence on-the-ground surveillance. Given the facts of this case, the intrusiveness of the surveillance facilitated by the Flock System is far less than (and fundamentally different from) the pervasive surveillance found to violate the *Fourth Amendment* in *Carpenter* and *Jones*.

As for the Fourth Circuit's **[*29]** decision in *Leaders of a Beautiful Struggle*, the court noted that once word spread about the Baltimore Police Department's aerial surveillance pilot program, "[i]n the face of public outcry, the program was discontinued." *2 F.4th at 333*. While it is does not appear that the Fourth Circuit attached legal significance to that information, such a reaction by the public would seem to have at least some bearing on the inquiry as to whether "an expectation of ***privacy*** that society is prepared to consider reasonable is infringed." *Jacobsen, 466 U.S. at 113*. In this case, no evidence was presented that such a public response to use of the Flock System by law enforcement has occurred.

To be sure, the court is concerned that the aggregation and searchability of the photos taken on the Flock System could rise to the level where "the retrospective quality of the data ... gives police access to a category of information otherwise unknowable." *Carpenter, 585 U.S. at 312*. However, the limited nature of the photographs taken in this case and the 30-day limitation on retention of photographs assuages the court's concerns at this time.[11]

Therefore, Defendant has not shown that his *Fourth Amendment* rights were violated by the Government's warrantless use of the Flock System to search **[*30]** for a specific license plate number and to create a Hot List to track that specific license plate number.

Nevertheless, the fact that the Flock System does not presently violate an expectation of ***privacy*** does not foreclose the potential for Flock to one day rise to the level of dragnet search with which the Supreme Court has voiced concern. Indeed, the court can easily see how the more widespread and pervasive deployment of ***Flock cameras*** (or cameras connected to the Flock System) could eventually rise to the level of systemic and continuous tracking with which the Supreme Court took issue in *Carpenter*. As was noted by Judge Carlos Bea of the Ninth Circuit, "I understand that ALPRs *may* in time present many of the same issues the Supreme Court highlighted in *Carpenter*. ALPRs can effortlessly, and automatically, create voluminous databases of

---

[11] It also should be noted that any photographs can be downloaded from the Flock System and saved locally by individual clients. In this case, the evidence is that the WPD downloads photographs only when there is a police purpose, otherwise the photographs are deleted. However, the testimony from Captain Slaughter exemplifies how important the role of local law enforcement evidence retention policies can be in preventing the violation of *Fourth Amendment* rights.

vehicle location information . . . In retrospective searches, detailed and potentially private information may be exposed." *United States v. Yang, 958 F.3d 851, 863 (9th Cir. 2020)* (Bea, J., concurring). Undeniably, the use of automatic license-plate readers to generate a pretext for stopping drivers is something which is not new. *See United States v. Ellison, 462 F.3d 557, 564 (6th Cir. 2006)* (Moore, J., dissenting) (noting that an officer running a license plate **[*31]** number through a computer database search without any heightened suspicion could raise *Fourth Amendment* concerns); *see also United States v. Lurry, 483 F. App'x 252, 255 (6th Cir. 2012)* (Moore, J., dissenting). However, the court is not convinced that the use of the Flock System in Wichita has yet risen to an insidious level such as would warrant the drastic and remedial action of invoking the exclusionary rule in this case.[12] "This Court must rule on the facts as they are and may not speculate about what the future may hold for Flock's capabilities." *United States v. Martin, 753 F. Supp. 3d 454, 476 (E.D. Va. 2024)*.

With the rise of new technologies, courts are left to apply aging *Fourth Amendment* doctrines in an era of increasing government surveillance. Increased computing power, when combined with artificial intelligence, allows the government to process vast amounts of data on nearly all its citizens. We live in a constitutional republic, not a burgeoning authoritarian society. Many *Fourth Amendment* carveouts and doctrines were crafted in an era where there was no capacity to replace human surveillance with computer surveillance. This presents unique challenges, since aggregated data on actions and movements can now be cross referenced to create individual profiles once suspicion has become centered on an individual. As the Supreme **[*32]** Court in *Carpenter* noted with regard to CSLI information, "the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection . . . this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when." *Carpenter, 585 U.S. at 312*. As of now, "[n]o specific federal legislative framework exists that governs federal law enforcement use of ALPRs.[13] KRISTIN FINKLEA, CONG. RSCH. SERV., R48160, LAW ENFORCEMENT AND TECHNOLOGY: USE OF AUTOMATED LICENSE PLATE READERS 6 (2024). Perhaps a solution to this dilemma between oversight and ***privacy*** would be to establish statutory guidelines akin to how the Electronic Communications ***Privacy*** Act of 1986 set new guidelines on the use of wiretaps in a digital era.[14] However, this is something that is better left to the purview of the legislative branch, rather than courts.

Indeed, the *Fourth Amendment* is a rather crude tool to fashion rules on such a rapidly evolving realm of technology. By the time hundreds of trial court judges apply their own **[*33]** individual notions of what the Constitution requires on this subject and the appellate process has run its full course, the creative application of newer technology may have rendered those rules obsolete or otherwise inadequate to curb the abuses of an ever-growing surveillance state. For this reason, it seems incumbent on legislative bodies to address those concerns. Those institutions are far better equipped to regulate the use of surveillance systems like the Flock System through the legislative process of hearings and investigations. This legislative process, subject to the public accountability of the ballot box, can craft detailed requirements suited to the current state of technology and revise those requirements as the capabilities of

---

[12] As Judge Bea later noted in his *Yang* concurrence, "It's clear to me that the database search did not reveal the whole, or even any, of Yang's physical movements. It would be folly to hold that searches of ALPR databases require a warrant without identifying even one case where the 'whole of [one's] physical movements' was implicated in an ALPR database search . . . If the technology evolves in the way that *amici* hypothesize, then perhaps in the future a warrant may be required for the government to access the LEARN [license plate] database, but this should only be the case if the database evolves to provide comparable location information to the records at issue in *Carpenter*." *United States v. Yang, 958 F.3d 851, 864 (9th Cir. 2020)* (Bea, J., concurring).

[13] Although there is no federal legislative framework for governing use of ALPRs, some states have enacted guidelines for the use of ALPRs. *See, e.g.*, *2025 Va. Acts ch. 720* (establishing regulations for the use of ALPRs in *Title 2.2, Chapter 55.6, section 2.2-5517* Code of Virginia).

[14] This is not to suggest that accessing ALPR databases deserves all the layers of oversight and authorization required for the far more intrusive surveillance of a wiretap under the Electronic Communications ***Privacy*** Act; but, rather, the court simply references that act as a well-known example of how a legislative body crafted detailed requirements for a form of electronic surveillance that would have been essentially impossible for courts to devise through interpretation of the *Fourth Amendment*.

those systems, and how they are deployed, inevitably change. By contrast, the *Fourth Amendment* is a blunt instrument wielded by judges who are limited by the record compiled before them. These judges oftentimes lack the authority and the information necessary to effectively and timely craft rules with the exacting detail that these types of surveillance systems require to lawfully promote public safety while preserving the ever-shrinking sphere of ***privacy*** to **[*34]** which citizens are entitled. But, if legislatures refuse to meet that challenge, it is likely only a matter of time before the courts will be compelled to intervene.

Given the current status and configuration of the Flock System in the Wichita area, the court finds that, in this particular case, there is no violation of an expectation of ***privacy*** that society would see as reasonable.

III. Conclusion

Defendant's motion to suppress (Doc. 22) is DENIED. The court notes that there are only six days remaining for trial under the Speedy Trial Act. This would not allow the parties much time to prepare for trial, nor would it allow sufficient time to summon a jury. The court finds it is in the interests of justice to continue the trial on its own motion to allow the parties additional time to prepare and so that a jury may be scheduled in due course. *See* *18 U.S.C. § 3161(h)(7)(A)*. The ends of justice are served by granting this continuance and excluding, for Speedy Trial purposes, the time from the entry of this order to the new trial date. The case is set for status conference Friday, May 30, 2025, at 10:30 A.M. in chambers, and the trial is set to begin on June 9, 2025.

IT IS SO ORDERED. Dated this 29th day of May 2025.

/s/ John Broomes **[*35]**

JOHN W. BROOMES

UNITED STATES DISTRICT JUDGE