

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

---

STEPHANIE SCHOLL *and* FRANK BEDNARZ,

Plaintiffs,

v.

ILLINOIS STATE POLICE; BRENDAN F. KELLY,  
*in his official capacity as Director of the  
Illinois State Police*; JAY ROBERT PRITZKER,  
*In his official capacity as Governor of the  
State of Illinois*; KWAME RAOUL, *in his  
official capacity as Attorney General of  
Illinois*,

Defendants.

---

Case No. 1:24-cv-4435

Hon. Judge Martha M. Pacold

**Plaintiffs' Memorandum of Law in  
Support of their Motion for Preliminary  
Injunction**

**Introduction**

Plaintiffs, Cook County residents subject to Defendants' mass surveillance system, move the Court to preliminarily enjoin Defendants from accessing the data Defendants are actively collecting, which tracks the movements of Plaintiffs—and anyone else in Cook County who drives a car or truck—everywhere they go, every day, without a warrant, or probable cause, or reasonable suspicion, or any limitation at all: Defendants' policy is to track every innocent citizen and later decide which is a reasonable target for law enforcement.

The Fourth Amendment requires more. Plaintiffs therefore ask this Court to enjoin Defendants such that, for the duration of this litigation, they may only access the collected data after obtaining a warrant. Such an injunction will reasonably balance any legitimate law enforcement interest Defendants claim, while providing the most basic protection for Plaintiffs, who are currently enduring a daily violation of their Fourth Amendment rights.

## Facts

After the 2019 shooting of a postal worker on an I-57 expressway, Illinois passed the Tamera Clayton Expressway Camera Act (the “Act”), 605 ILCS 140/1 et seq., which funded the installation of more than 300 Automated License Plate Reader (“ALPR”) cameras across every expressway in Cook County—I-90 Kennedy, I-290 Eisenhower, I-55 Stevenson, I-94 Dan Ryan, the Bishop Ford, and I-57. Compl. ¶¶ 14–15. An ALPR does roughly what it sounds like: each camera records every car that drives by, identifies the car based on its license plate, and stores the fact that this car drove by the given camera at the given time. *Id.* at ¶ 16. Law enforcement then uses this information in one of two primary ways. First, prospectively for locating a car’s present location—perhaps to find a fleeing suspect or missing person. *Id.* at ¶ 18. Second, and more troublingly, Defendants store the record of every camera a car drives by for 90 days, so that Defendants can reconstruct the past movements of any citizen who draws the attention of law enforcement. *Id.* at ¶ 33.

The ALPRs that the Illinois State Police (“ISP”) has installed for this purpose are made by Vigilant, a subsidiary of Motorola Solutions. *Id.* at ¶ 31. The cameras feed into Vigilant’s Law Enforcement Archival Reporting Network (“LEARN”), a national database that aggregates ALPR data from each law enforcement agency nationwide—state, local, and federal—that uses Vigilant ALPRs. These law enforcement agencies across the country can access each other’s camera information—so other law enforcement agencies that are Vigilant customers can see license plates captured by ISP’s cameras, and ISP can access the billions of datapoints collected by other jurisdiction’s ALPRs around the country. *Id.* at ¶ 32. According to ISP’s publicly available data, ISP’s retention of ALPR records for 90 days means that, at any given time, ISP is in possession of approximately 350 to 450 million “Detections” (when a car is recorded driving

past a camera), augmented by the billions more in the LEARN database. *Id.* at ¶ 33. ISP can access this data at its discretion—the Act provides requirement that it obtain a warrant or make any showing of probable cause or reasonable suspicion before accessing the historical tracking data on any citizen whom it has decided is of interest. *Id.* at ¶ 4. In 2022, Illinois passed an updated version of the Act, which expands the use of ALPRs to 20 additional counties around the state—the installation of which has already begun. *Id.* at ¶ 22.

Plaintiffs are two Cook County residents who regularly drive their own personal vehicles. *Id.* at ¶¶ 5–6. ISP records every time Plaintiffs drive around Cook County, and it stores that information for future criminal investigations of Plaintiffs, without any probable cause or reasonable suspicion—so that, simply by living in the Chicago area and having a car, Plaintiffs are subject to constant, daily tracking of their movement. *Id.* at ¶ 38.

### **Standard of Review**

Plaintiffs are entitled to preliminary relief where (1) they will otherwise suffer irreparable harm; (2) traditional legal remedies are inadequate; and (3) there at least some likelihood of success on the merits. *HH-Indianapolis, LLC v. Consol. City of Indianapolis*, 889 F.3d 432, 437 (7th Cir. 2018). If a plaintiff makes such a showing, the court proceeds to a balancing analysis, weighing the harm a denial of the preliminary injunction would cause the plaintiff against the harm of a grant to the defendant. *Mays v. Dart*, 974 F.3d 810, 818 (7th Cir. 2020). This is a sliding scale approach: the more likely the plaintiff is to win on the merits, the less the balance of harms needs to weigh in his favor, and vice versa. *Id.*

### **Argument**

#### **I. Plaintiffs are likely to succeed on the merits.**

Plaintiffs are likely to succeed on the merits of their claim that Defendants' warrantless, suspicionless, probable-cause-free tracking of their movements everywhere they drive in their

car is a Fourth Amendment search that violates their connotational privacy interest in the whole of their physical movements. Illinois is tracking Plaintiffs everywhere they go around Cook County—and in the future, the state hopes to track them elsewhere in Illinois. This comprehensive tracking of every innocent citizen’s movement violates fundamental privacy protections the Supreme Court has recognized.

The Fourth Amendment protects persons from unreasonable searches of their homes and property. *See* U.S. Const. amend IV. A search occurs when the government intrudes on a reasonable expectation of privacy that society is prepared to recognize as legitimate. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Searches conducted without a warrant are “presumptively unreasonable.” *Kentucky v. King*, 563 U.S. 452, 459 (2011) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

“Any Fourth Amendment analysis . . . must be grounded on an accurate understanding of the facts.” *United States v. Curry*, 965 F.3d 313, 316 (4th Cir. 2020). Thus, “when addressing a facial challenge to a statute authorizing warrantless searches, the proper focus of the constitutional inquiry is searches that the law actually authorizes, not those for which it is irrelevant.” *City of Los Angeles v. Patel*, 576 U.S. 409, 419 (2015). “Stated differently, Plaintiffs must show the [law’s] actual applications are unconstitutional.” *Bell v. City of Chi.*, 835 F.3d 736, 739 (7th Cir. 2016).

Twentieth-century Fourth Amendment doctrine provided little protection for things one did in public, including the public movements of one’s car. *See, e.g. United States v. Knotts*, 460 U.S. 276, 281 (1983). But the advent of new technologies has led to the development of a different approach, in the face of decreasing marginal costs of mass surveillance and increasing ubiquity of surveillance technology. *See United States v. Tuggle*, 4 F.4th 505, 509 (7th Cir. 2021)



(“Nonetheless, we are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans.”).

In *United States v. Jones*, 565 U.S. 400 (2012), the government attached a GPS tracking device under the bumper of a suspect’s car, tracking his movements constantly for a month. The defendant’s movements were all public, the sort of thing that an old-fashioned tail could in theory have captured, but there was no longer a resource constraint on the government’s ability to tail someone so comprehensively. Although the majority opinion in *Jones* was content to resolve the case as an illegal trespass (the physical attachment of the tracker to the suspect’s property), five justices expressed concern that “physical intrusion is now unnecessary to many forms of surveillance . . . [so that] the monitoring undertaken in this case [could be done] by enlisting factory—or owner—installed vehicle tracking devices or GPS-enabled smartphones.” *Id.* at 415 (Sotomayor, J., concurring) (emphasis added); *see also id.* at 428 (Alito, J., concurring). There was no majority view as to how long such tracking would have to last to violate the Fourth Amendment, but five justices agreed that “at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” *Id.* at 415 (Sotomayor, J., concurring) (internal quotation marks omitted). Justice Sotomayor went further, arguing that the Court should consider

whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.

*Id.*

In *Carpenter v. United States*, 585 U.S. 296 (2018), the Court answered the question that the majority in *Jones* left open, holding that warrantless tracking of cell phone locations violated the Fourth Amendment. The government in *Carpenter* had obtained records from the phone company of which cell towers the defendant's phone connected to over the course of several months, and unfortunately for Mr. Carpenter the locations matched up with a string of robberies. The majority opinion held that, even though the data in question recorded public movements, “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.” *Id.* at 310. The Court embraced the view taken by the concurrences in *Jones*:

Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken. For that reason, society'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 individual's car for a very long period.

*Id.* (quoting *Jones*, 565 U.S. at 429 (Alito, J., concurring)) (internal quotation marks and citations omitted). The Court stressed that the backward-looking nature of the cell phone records was particularly troubling:

Moreover, 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. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers.

*Id.* at 312. The search therefore “invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.” *Id.* at 313.

Like the cell-phone location data in *Carpenter*, ALPR data is generated involuntarily; like carrying a cell phone, traveling in a car on highways is an indispensable feature of contemporary life; like the phone data, ALPR data is historical and searchable, allowing authorities to simply

track everyone and later decide whom among the population to investigate; and, like cell phones. the license plates and cars are specifically associated with the owner of the property being tracked. Indeed, the government’s collection of ALPR data is in many ways *more* concerning than its use of cell-phone data in *Carpenter*, in that all the ALPR data is in the hands of the State in the first instance—in *Carpenter*, the data was in possession of the phone companies, and the government had to specifically request the records of the specific suspect.

Defendants will likely point out that the ALPR data only captures the movement of the car, and not Plaintiffs’ movements after they get out of the car. But the cell phone in *Carpenter* likewise only provided a limited set of data points: each cell tower Mr. Carpenter’s phone connected to on the relevant days. Individual ALPR detections are in fact more precise, taking a photo of a car at a specific location, whereas the cell-site location information was only accurate to the range of a given cell tower. And even relatively “low resolution” data, when aggregated together, can tell the government a great deal about our lives. As the Fourth Circuit explained in striking down Baltimore’s arial surveillance program under *Carpenter*:

We do not suggest that the AIR program allows perfect tracking of all individuals it captures across all the time it covers. Though data is collected in 12-hour increments, the tracks are often shorter snippets of several hours or less. Still, the program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield “a wealth of detail,” greater than the sum of the individual trips.

*Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 2 F.4th 330, 342 (4th Cir. 2021). Such data “enables deductions about what a person does repeatedly, what he does not do, and what he does ensemble, which reveals more about a person than does any individual trip viewed in isolation.” *Id.* (quoting *United States v. Maynard*, 615 F.3d 544, 562–63 (D.C. Cir. 2010) (cleaned up).

Defendants record every time a citizen goes to the hospital, or the family planning clinic, or the

NRA convention, or BlackLivesMatter rally; when they go out to dinner with friends, or visit a romantic partner—any one datapoint may be of limited use, but the aggregation allows Defendants to deduce the intimate details of each of our lives. “*Carpenter* held those deductions go to the privacies of life, the epitome of information expected to be beyond the warrantless reach of the government. And here, as there, the government can deduce such information only because it recorded everyone’s movements.” *Leaders of a Beautiful Struggle*, 2 F.4th at 342 (internal citations omitted).

Nor is it an answer to suggest that citizens concerned about privacy simply rely on public transportation. The entire point of *Carpenter*—and *Jones*—is that citizens do not forfeit their expectation of privacy simply by living in the modern world. *See also Kyllo v. United States*, 533 U.S. 27 (2001) (extending fourth amendment to thermal imaging technology). As the Fifth Circuit recently held, even ostensibly voluntary opt-in features such as location tracking don’t necessarily vacate any expectation of privacy. *United States v. Smith*, No. 23-60321, 2024 U.S. App. LEXIS 20149, at \*37 (5th Cir. Aug. 9, 2024) (“These requests typically innocuously promise app optimization, rather than reveal the fact that users’ locations will be comprehensively stored in a ‘Sensorvault,’ providing Google the means to access this data and share it with the government.”).

Like cell phones, cars are a ubiquitous feature of modern life, and the Supreme Court has consistently found that Fourth Amendment doctrine must accommodate itself to the technological needs of our day. Which is why, for instance, the Court rejected searching cell phones incident to arrest, finding that a person’s cell phone now contains far more personal information than the purses and wallets of prior Fourth Amendment cases. *Riley v. California*,

573 U.S. 373, 393 (2014); *see also* *Kyllo*, 533 U.S. at 34 (thermal imaging camera required a warrant).

The Seventh Circuit’s cases applying *Carpenter* confirm as much. The Seventh Circuit has noted that *Carpenter* was concerned with the ability to aggregate historical location data and recognized that “the warrantless acquisition of that type of data implicates unique privacy interests,” because such data “provides a detailed record of a person’s past movements, which is made possible so long as he carries a cell phone.” *United States v. Soybel*, 13 F.4th 584, 587 (7th Cir. 2021). As both the Supreme Court and the Seventh Circuit have recognized,

the privacy concern is magnified by the data's retrospective quality because historical CSLI gives police access to a category of information otherwise unknowable. Obtaining historical CSLI without a warrant would allow the government to effectively travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers.

*Id.* at 592 (quoting *Carpenter*) (cleaned up). The result is a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years . . . [that] implicates privacy concerns far beyond those considered” by more traditional Fourth Amendment doctrine.

*Id.* As with cell phone data, the historical location data collection that Plaintiffs challenge allows the government to simply track every citizen, and “travel back in time” whenever authorities decide they’d like to retrace any of our whereabouts. This happens effectively every day, when Plaintiffs go to work, or to the grocery store, or the doctor’s office. And while ISP’s policy choice is to only retain the data for 90 days—not much less than the 127 days of data the government collected in *Carpenter*—nothing prevents Defendants from changing that policy to 120 days, or 365, or a decade.

Even when Seventh Circuit has rejected *Carpenter*-based claims, it has done so on grounds that drive home just how much more like *Carpenter* this case is. For instance, the court

concluded that it is not a violation of the Fourth Amendment under *Carpenter* to set up three cameras in a single public location, even if those cameras record that single location continually for months. *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021). Plaintiffs here are not challenging three cameras in one place; they’re challenging hundreds of cameras all over Cook County. A power company’s recording of home electricity use, for purposes of billing customers, didn’t violate the Fourth Amendment because it was done by the utility company and not for a law enforcement purpose. *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2018) (“Critically, Naperville conducts the search with no prosecutorial intent.”). Here, the express purpose of this tracking is for later investigation of crimes.

As this technology is new, there is little case law directly addressing ALPRs and the Fourth Amendment. But a state trial court in Virginia recently granted a motion to suppress APLR data on the same *Carpenter*-based theory Plaintiffs advance here. *Commonwealth v. Bell*, Circuit Court of The City of Norfolk, Case No. CR23001500-00; 01; 02, 2024 Va. Cir. LEXIS 77 (May 10, 2024) (attached as Exhibit A). Other authorities involving ALPRs have generally not reached the *Carpenter* question, or not found it applicable to the facts before them. In *Commonwealth v. McCarthy*, 484 Mass. 493, 508, 142 N.E.3d 1090, 1105–06 (2020), the Massachusetts Supreme Court agreed that a citizen has “a constitutionally protected expectation of privacy in the whole of his public movements,” and that interest “potentially could be implicated by the widespread use of ALPRs.” The defendant had been identified by ALPRs covering two bridges on the way to and from Cape Cod. “With enough cameras in enough locations,” the Court said, “the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes,” and Massachusetts’ policy of retaining the data for one year “certainly [was] long enough to warrant constitutional protection.”

*Id.* at 506. The Court erred, however, in limiting its analysis to a very narrow understanding of the facts before it, treating only the four cameras on the two bridges as relevant to the case before it, and ruling that the recording by those cameras alone was insufficient to offend the Fourth Amendment. *Id.* at 509.

Other courts confronting this question have similarly held the ALPR data used to convict the given defendant was not pervasive enough to trigger *Carpenter*. See *United States v. Yang*, 958 F.3d 851, 863 (9th Cir. 2020) (Bea, J., concurring) (“Despite its 5 billion total records, the LEARN database contained a single entry for the Yukon that Yang had rented”); *United States v. Rubin*, 556 F. Supp. 3d 1123, 1129–30 (N.D. Cal. 2021) (“although this ALPR database contained more information about Rubin than the single entry at issue in Yang, and the precise volume of information is unknown, it is clear that the information was not remotely comparable to the ‘detailed, encyclopedic’ information at issue in *Carpenter*”); *United States v. Bowers*, No. 2:18-CR-00292-DWA, 2021 U.S. Dist. LEXIS 196899, at \*10 (W.D. Pa. Oct. 11, 2021) (“This limited data collection does not even begin to approach the same degree of information as that gathered in *Carpenter*”); *Commonwealth v. Watkins*, 2021 Pa. Dist. & Cnty. Dec. LEXIS 2485 (Dec. 15, 2021) (“While this Court finds the practice of reading and compiling license plate information troubling, it determined that the facts in this case are insufficient to establish the use of an LPR as the equivalent of physically placing a GPS device on a car”); *United States v. Graham*, No. 21-645 (WJM), 2022 U.S. Dist. LEXIS 163818, at \*14 (D.N.J. Sep. 12, 2022) (“In this case, law enforcement’s use of ALPR database limited to a single occurrence on a single day did not reveal private details of Defendant’s life.”).

Plaintiffs are not here challenging a single camera, or handful of cameras, that might have picked them up once or twice. Rather, the facts pled here establish precisely what *Carpenter*

requires: a pervasive system of hundreds of cameras that follow them all around the Chicago area—and soon will follow them all around the State of Illinois—and store that data for months without a warrant, probable cause, reasonable suspicion, or any other standard. That is an unreasonable search under the Fourth Amendment.

**II. Without a preliminary injunction, Plaintiffs will suffer irreparable harm and do not have an adequate remedy at law.**

Unless enjoined, Defendants’ mass surveillance system will cause irreparable harm to Plaintiffs. First and foremost, Defendants’ tracking of Plaintiffs violates Plaintiffs’ constitutional rights, which alone constitutes manifest, irreparable harm. *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (“It has long been established that the loss of constitutional freedoms, ‘for even minimal periods of time, unquestionably constitutes irreparable injury.’” (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976))). And even if further demonstration of irreparable harm were required, such a requirement is surely met by evidence that Defendants’ mass surveillance will burden Plaintiffs’ and others’ associational and expressive activity: Plaintiffs will be tracked wherever they go and will have to consider that and limit their activities to the extent they don’t want them to be known to the government. This chilling effect on their associational freedoms and right to travel cannot be recompensed by a damages award at the end of this case.

Nor do plaintiffs have any adequate remedies at law. The damage suffered by the violation to Plaintiffs’ privacy is not quantifiable and therefore damages are inadequate. *ACLU v. Alvarez*, 679 F.3d 583, 589 (7th Cir. 2012) (“the quantification of injury is difficult and damages are therefore not an adequate remedy”) (quotation and citation omitted).



**III. The balance of equities and public interest favor a preliminary injunction.**

The public interest always favors the protection of constitutional rights—and the balance of equities here clearly favors injunctive relief. Plaintiffs’ requested injunction is narrow: they ask that this Court order that Defendants be enjoined from accessing ALPR data unless they first obtain a warrant. There is no request at this stage that Defendants deactivate or remove the cameras—Plaintiffs simply ask that, as this case is litigated, Defendants observe the most basic requirements of constitutional process: conduct reasonable searches subject to a warrant. Government officials are not harmed by the issuance of a preliminary injunction which prevents the state from implementing a likely unconstitutional practice. *See Joelner v. Vill. of Wash. Park*, 378 F.3d 615, 620 (7th Cir. 2004) (government could suffer “no irreparable harm” from being “prevented from enforcing an unconstitutional statute”); *see also Centro Tepeyac v. Montgomery Cty.*, 722 F.3d 184, 191 (4th Cir. 2013) (“[A] state is in no way harmed by issuance of a preliminary injunction which prevents [it] from enforcing restrictions likely to be found unconstitutional.”); *Rodriguez v. Robbins*, 715 F.3d 1127, 1145 (9th Cir. 2013) (government “cannot suffer harm from an injunction that merely ends an unlawful practice”). Such a warrant requirement will not burden defendants—by definition, any criminal activity they have probable cause to investigate will allow them to use the data as this case goes forward. The only thing they will be prevented from doing is tracking innocent citizens like Plaintiffs—and if for whatever reason they have valid reason to investigate Plaintiffs, they can get a warrant.

**Conclusion**

For the foregoing reasons, Plaintiffs respectfully request that this Court enter a preliminary injunction providing that Defendants may only access the collected data after obtaining a warrant.

Dated: August 20, 2024

Respectfully submitted,

Stephanie Scholl and Frank Bednarz

By: Reilly Stephens  
One of their Attorneys

Reilly Stephens  
Jeffrey Schwab  
Liberty Justice Center  
7500 Rialto Blvd.  
Suite 1-250  
Austin, Texas 78735  
(512) 481-4400  
rstephens@ljc.org  
jschwab@ljc.org

# Exhibit A



JAMILAH D. LECRUISE  
JUDGE

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

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*,

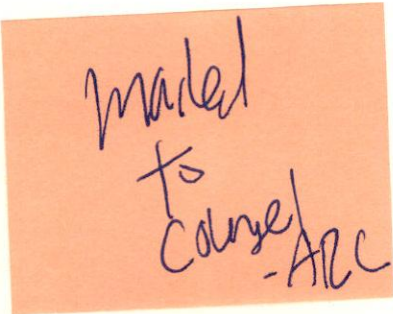
267 Va. 532, 536, 593 S.E.2d 204 (2004). Here, the Court is unconvinced that the Norfolk Police Department would have discovered the Defendant in the suspect vehicle in a way to immediately arrest him before obtaining an incriminatory statement from him without the FLOCK system.

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 blue ink, appearing to read "J.D. LeCruise", written over a horizontal line.

Jamilah D. LeCruise, Judge

An orange rectangular sticky note with handwritten text in black ink. The text reads "mailed to counsel - ABC".

mailed  
to  
counsel  
- ABC