

No. 26-1227

**UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

LEE SCHMIDT; CRYSTAL ARRINGTON,

Plaintiffs-Appellants,

v.

CITY OF NORFOLK; MARK TALBOT, in his official capacity as
the Norfolk Chief of Police,

Defendants-Appellees.

On Appeal from the United States District Court for the
Eastern District of Virginia
Case No. 2:24-cv-621-MSD-RJK

RESPONSE BRIEF OF DEFENDANTS-APPELLEES

Adam D. Melita
Karla J. Soloria
CITY OF NORFOLK
DEPARTMENT OF LAW
810 Union Street
Suite 900
Norfolk, VA 23510
(757) 664-4529
adam.melita@norfolk.gov
karla.soloria@norfolk.gov

Counsel for Defendants-Appellees

Donald B. Verrilli, Jr.
Elaine J. Goldenberg
Daniel J. Kane
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW
Suite 500 E
Washington, DC 20001
(202) 220-1100
Donald.Verrilli@mto.com
Elaine.Goldenberg@mto.com
Daniel.Kane@mto.com

*Counsel for Defendant-Appellee
City of Norfolk*

(additional counsel on inside cover)

Justin P. Raphael
MUNGER, TOLLES & OLSON LLP
560 Mission Street
27th Floor
San Francisco, CA, 94105
(415) 512-4000
Justin.Raphael@mto.com

*Counsel for Defendant-Appellee City of
Norfolk*

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS.....	i
INTRODUCTION	1
JURISDICTIONAL STATEMENT	3
STATEMENT OF THE ISSUE.....	3
ADDENDUM OF AUTHORITIES.....	3
STATEMENT OF THE CASE.....	4
I. NPD’s ALPR System	4
A. Flock Cameras and Database	4
B. NPD’s Cameras and Use of Flock Database.....	6
C. Legal Requirements Governing NPD’s ALPRs.....	8
II. This Case	10
SUMMARY OF ARGUMENT	15
STANDARD OF REVIEW	17
ARGUMENT	17
I. Plaintiffs’ Standing Extends Only to the Collection and Storage of Photographs of Their Vehicles and Does Not Include Any Challenge to the Querying of the Database	17
II. Collection and Storage of Photographs of Plaintiffs’ Vehicles on Public Roads Is Not A Fourth Amendment Search.....	25
III. Even Assuming that Plaintiffs Had Standing to Challenge Querying of the Database, That Querying Is Not a Fourth Amendment Search	29
A. Under Governing Precedent, Querying The Database Is Not A Search	30
B. Plaintiffs’ Proposed Three-Factor Test Is Forfeited and Meritless	45
IV. Plaintiffs’ “Original Meaning” Argument Is Waived and Meritless.....	53
CONCLUSION	55
REQUEST FOR ORAL ARGUMENT	57

CERTIFICATE OF COMPLIANCE	58
CERTIFICATE OF SERVICE	59

TABLE OF AUTHORITIES

	Page(s)
FEDERAL CASES	
<i>Alvarado v. Bd. of Tr.</i> , 848 F.2d 457 (4th Cir. 1988)	24
<i>Benham v. Charlotte</i> , 635 F.3d 129 (4th Cir. 2011)	3
<i>Bloosurf v. T-Mobile</i> , 170 F.4th 264 (4th Cir. 2026)	22, 46
<i>Blum v. Yaretsky</i> , 457 U.S. 991 (1982)	19
<i>Byrd v. United States</i> , 584 U.S. 395 (2018)	21
<i>California v. Carney</i> , 471 U.S. 386 (1985)	27, 34
<i>Cardwell v. Lewis</i> , 417 U.S. 583 (1974)	27
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	passim
<i>Cybernet v. David</i> , 954 F.3d 162 (4th Cir. 2020)	17
<i>DaimlerChrysler v. Cuno</i> , 547 U.S. 332 (2006)	3, 19, 24
<i>Est. of Van Emburgh v. United States</i> , 95 F.4th 795 (4th Cir. 2024)	22
<i>FDA v. All. for Hippocratic Med.</i> , 602 U.S. 367 (2024)	18, 19, 20

<i>Florida v. Jardines</i> , 569 U.S. 1 (2013).....	27
<i>Foster v. Univ. of Md.-E. Shore</i> , 787 F.3d 243 (2015).....	21, 22
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	46
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	33, 54
<i>Knibbs v. Momphard</i> , 30 F.4th 200 (4th Cir. 2022)	17
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	23, 53
<i>L.R. Willson & Sons v. Occupational Health & Safety Review Commission</i> , 134 F.3d 1235 (4th Cir. 1998)	27, 28, 43
<i>Leaders of a Beautiful Struggle v. Baltimore Police Department</i> , 2 F.4th 330 (4th Cir. 2021) (en banc)	passim
<i>Lujan v. Defs. of Wildlife</i> , 504 U.S. 555 (1992).....	18
<i>McGinn v. Broadmead</i> , 167 F.4th 667 (4th Cir. 2026)	22
<i>Minnesota v. Carter</i> , 525 U.S. 83 (1998).....	21
<i>New York v. Class</i> , 475 U.S. 106 (1986).....	26, 27, 29
<i>Ohio v. Robinette</i> , 519 U.S. 33 (1996).....	31, 46
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	21

<i>Riley v. California</i> , 573 U.S. 373 (2014).....	36
<i>Rinaldi v. Sylvester</i> , 2025 WL 2682691 (S.D.N.Y.).....	35
<i>Schemel v. City of Marco Island Fla.</i> , 2025 WL 2958798 (M.D. Fla.), <i>appeal docketed</i> , No. 25-13913 (11th Cir.)	35
<i>Scholl v. Ill. State Police</i> , 776 F. Supp. 3d 701 (N.D. Ill. 2025), <i>appeal docketed</i> , No. 25-1847 (7th Cir.)	17, 19, 35, 36
<i>United States v. Acosta</i> , 2025 WL 2427700 (N.D. Okla.).....	35
<i>United States v. Bowers</i> , 2021 WL 4775977 (W.D. Pa.).....	35
<i>United States v. Brown</i> , 2021 WL 4963602 (N.D. Ill.)	35
<i>United States v. Brown</i> , 2025 WL 2444596 (W.D. Okla.)	35
<i>United States v. Chatrie</i> , 136 F.4th 100 (4th Cir. 2025) (en banc), <i>cert. granted</i> , 2026 WL 120676.....	50, 51
<i>United States v. Cooper</i> , 2025 WL 35035 (E.D. La.)	35
<i>United States v. Ellison</i> , 462 F.3d 557 (6th Cir. 2006)	26
<i>United States v. Floyd</i> , 811 F. Supp. 3d 1345 (M.D. Fla. 2025).....	35
<i>United States v. George</i> , 971 F.2d 1113 (4th Cir. 1992)	25, 26, 28, 29

<i>United States v. Graham</i> , 2022 WL 4132488 (D.N.J.)	35
<i>United States v. Gregory</i> , 128 F.4th 1228 (11th Cir. 2025)	49
<i>United States v. Griffin</i> , 2025 WL 1474679 (S.D. Ind.)	35
<i>United States v. Harry</i> , 130 F.4th 342 (2d Cir. 2025)	28
<i>United States v. Hay</i> , 95 F.4th 1304 (10th Cir. 2024)	28
<i>United States v. Houston</i> , 813 F.3d 282 (6th Cir. 2016)	28
<i>United States v. Jackson</i> , 2025 WL 1530574 (D. Kan.)	35, 36, 44
<i>United States v. James</i> , 2023 WL 3370421 (W.D. La.)	35
<i>United States v. Jiles</i> , 2024 WL 891956 (D. Neb.)	35
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	13, 20, 30
<i>United States v. Knotts</i> , 460 U.S. 276 (1983)	passim
<i>United States v. Lawrence</i> , 2026 WL 765307 (D.N.D.)	35
<i>United States v. Martin</i> , 753 F. Supp. 3d 454 (E.D. Va. 2024)	20, 35, 36, 46
<i>United States v. Murillo-Lopez</i> , 151 F.4th 584 (4th Cir. 2025)	42

<i>United States v. Porter</i> , 170 F.4th 381 (5th Cir. 2026)	35
<i>United States v. Porter</i> , 2022 WL 124563 (N.D. Ill.)	35
<i>United States v. Robinson</i> , 744 F.3d 293 (4th Cir. 2014)	53
<i>United States v. Rubin</i> , 556 F. Supp. 3d 1123 (N.D. Cal. 2021).....	35
<i>United States v. Runner</i> , 43 F.4th 417 (4th Cir. 2022)	25
<i>United States v. Salcido-Gonzalez</i> , 2024 WL 2305478 (D. Utah).....	35
<i>United States v. Sturdivant</i> , 786 F. Supp. 3d 1098 (N.D. Ohio 2025), <i>appeal docketed</i> , No. 26-3426 (6th Cir.)	35, 36
<i>United States v. Taylor</i> , 54 F.4th 795 (4th Cir. 2022)	25
<i>United States v. Toombs</i> , 671 F. Supp. 3d 1329 (N.D. Ala. 2023).....	35
<i>United States v. Vankesteren</i> , 553 F.3d 286 (4th Cir. 2009)	27, 29, 34, 49
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	23
<i>Wikimedia Foundation v. NSA</i> , 857 F.3d 193 (4th Cir. 2017)	22, 23
STATE CASES	
<i>Commonwealth v. Church</i> , 2025 WL 2908089 (Va. Ct. App. Oct. 14, 2025)	44, 45, 52

<i>Commonwealth v. Roberson</i> , 113 Va. Cir. 565 (2024).....	8
---	---

<i>Robinson v. Commonwealth</i> , 927 S.E.2d 822 (Va. Ct. App. 2026).....	passim
--	--------

STATUTES

2025 Va. Acts Ch. 720.....	8
----------------------------	---

Va. Code § 2.2-5517	8, 9, 20, 45
---------------------------	--------------

Va. Code § 2.2-5517(E)	5, 8, 38
------------------------------	----------

Va. Code § 2.2-5517(F)	9, 43
------------------------------	-------

Va. Code § 2.2-5517(H).....	9
-----------------------------	---

Va. Code § 46.2-715	26
---------------------------	----

Va. Code § 46.2-1013(B).....	26
------------------------------	----

OTHER AUTHORITIES

Courts of Justice, <i>Virginia Senate</i> , SR A (305), Feb. 10, 2025, available at https://virginia-senate.granicus.com/View Publisher.php?view_id=3	20
---	----

Neera Tanden & Nick Wilson, Center for American Progress, <i>A Plan to Stop Crime in Our Communities</i> (Jan. 29, 2026), available at https://www.americanprogress.org/article/delivering- accountability-a-plan-to-stop-crime-in-our-communities/	8
--	---

Orin Kerr, <i>The Digital Fourth Amendment</i> (2025).....	36
--	----

Orin Kerr, <i>Katz as Originalism</i> , 71 Duke L.J. 1047 (2022).....	53
---	----

INTRODUCTION

This Court should affirm the district court’s summary-judgment ruling that use of automated license plate readers (“ALPRs”) by the Norfolk Police Department (“NPD”) complies with the Fourth Amendment.

The district court correctly held that Plaintiffs have standing to challenge only the photographing and storage of images of their cars on public roads, not any querying of a database of those images. The court correctly ruled that the photographing and storage is not a Fourth Amendment search under binding precedent. The court correctly concluded that even if Plaintiffs could challenge NPD’s querying of the database, that querying is also not a search, as the summary-judgment record confirmed that NPD cannot use the database to reveal the whole—or anything close to the whole—of Plaintiffs’ movements or any intimate details about Plaintiffs’ associations or activities. Indeed, the court emphasized that the evidence demonstrates that Plaintiffs’ broad assertions about supposed “tracking” of their movements are simply incorrect. And the court correctly observed, based on Plaintiffs’ own concession, that Plaintiffs’ “original meaning” theory of the Fourth Amendment is foreclosed by precedent.

The district court thus joined an unbroken line of federal courts, including the Fifth Circuit, that have held that use of ALPRs does not violate the Fourth

Amendment. It also joined the Virginia Court of Appeals, which has twice held the same thing as to NPD's ALPR system—the very system at issue in this case.

Plaintiffs ignore nearly all of that. They omit any discussion of settled law holding that there is no reasonable expectation of privacy in the exterior characteristics of vehicles in public places and approving police use of fixed cameras like the ones at issue here, offering instead various theories of the Fourth Amendment that no court has adopted. They gloss over a lopsided factual record showing that NPD's ALPRs take snapshots on only a tiny percentage of Norfolk roads; that Plaintiffs' cars were rarely photographed by the ALPRs and never subject to a database query; and that there is *no* evidence that NPD learned intimate information about *anyone* through use of ALPRs and the database. They barely cite the Virginia statute that strictly regulates use of ALPRs in the Commonwealth and allows retention of photographs for only a limited time. And they simply disregard the dozens of cases rejecting challenges just like theirs.

For all of Plaintiffs' rhetoric, this is not a close case. Faced with a one-sided record, the district court held that Norfolk's system of fixed, roadside license-plate readers complies with the Fourth Amendment. That holding is not only dictated by precedent but also eminently sensible, as accepting Plaintiffs' position would throw into question a variety of long-established law-enforcement practices that protect the public. Every federal court to consider the question has rejected Plaintiffs'

arguments, and this Court should not depart from that consensus—least of all in a case like this one, where nobody queried the database for data on Plaintiffs and the factual record overwhelmingly disproves their claim.

JURISDICTIONAL STATEMENT

As the district court correctly ruled, Plaintiffs do not have standing to challenge the querying of a database of photographs taken by ALPRs in Norfolk. *See* pp.17-24, *infra*; *DaimlerChrysler v. Cuno*, 547 U.S. 332, 353 n.5 (2006). This Court therefore lacks jurisdiction of the “merits” of that issue. *Benham v. Charlotte*, 635 F.3d 129, 134 (4th Cir. 2011).

STATEMENT OF THE ISSUE

Whether the district court correctly ruled that NPD did not conduct a Fourth Amendment search when fixed ALPRs photographed Plaintiffs’ vehicles moving on public roads and uploaded the resulting images to a database.

ADDENDUM OF AUTHORITIES

Relevant constitutional, statutory, and regulatory authorities appear in the Addendum.

STATEMENT OF THE CASE

I. NPD's ALPR System

A. Flock Cameras and Database

During the pandemic, Norfolk experienced a surge in vehicle-related crimes, including car thefts and drive-by shootings. JA383-384, JA414-415, JA1494, JA1710-1714.¹ To address that surge, and to promote other vital public-safety functions like locating missing persons, NPD purchased ALPRs from Flock Safety ("Flock"). JA384, JA1494-1496, JA1710-1716.

Flock's ALPRs are fixed, motion-activated cameras, typically mounted on top of poles and installed next to public roadways. JA7, JA433-434. They are designed to photograph the backs of passing vehicles so as to record external vehicle characteristics visible to the naked eye, including license-plate characters. JA433-434, JA437-38, JA465-466, JA2046-2047. The cameras do not pan, tilt, or zoom. JA433-434, JA2277. They do not collect information on where a trip began or ended or where a car came from, stopped, or went. JA386, JA433-434. And they do not target individuals, whether inside or outside vehicles. JA7-8, JA386, JA435, JA440, JA466. Instead, the cameras show only that a particular vehicle passed by a particular camera at a particular time. JA386, JA434, JA2016.

¹ The district court decided this case at summary judgment and explained that the material facts were "largely" not in dispute. JA13 n.8.

After a Flock camera photographs a passing vehicle, the image is uploaded to encrypted servers, where it is stored in a database for a retention period governed by applicable state-law limitations. JA8, JA434, JA440, JA1387-1388, JA2124-2125. In Virginia, a state statute restricts retention of ALPR data to a maximum of 21 days, absent an ongoing criminal investigation or pending court case. *See, e.g.*, Va. Code § 2.2-5517(E). Once an image is uploaded, Flock applies machine learning to identify license-plate numbers and certain other external features. JA434-439, JA1295.

Only authorized users who enter a password can review images in the database. JA187, JA385, JA433, JA1396-1401, JA1945. A user can run queries for full or partial license-plate numbers or a limited set of vehicle characteristics: vehicle make, color, and body type; identifying features like roof racks and toolboxes; and the presence (but not content) of bumper and window stickers. JA433-439, JA1288, JA1299, JA1320, JA1326. Users cannot search the database for people, and Flock does not create or maintain a profile for any particular vehicle. JA386, JA433-435, JA466, JA1409-1410. Thus, the database cannot provide a name, address, or any other information associated with a license-plate number. JA435.

Under limited circumstances, authorized users may receive real-time alerts when a particular vehicle is photographed by a Flock camera to which the user has

access. JA434. Such an alert may be sent when a photograph matches information on certain law-enforcement lists, like those maintained by the National Center for Missing & Exploited Children (which issues “AMBER Alerts”) or the FBI’s National Crime Information Center. JA434. In addition, within certain constraints, authorized users may create custom “hotlists” that generate real-time alerts—for example, to find a stolen car. JA188-189, JA386, JA434-435, JA1713-1714.

B. NPD’s Cameras and Use of Flock Database

NPD operates 176 Flock cameras in Norfolk. JA9, JA384. Because the cameras typically photograph vehicles traveling only in one direction, multiple cameras are placed at a single location—e.g., major four-way intersections have four cameras. NPD’s cameras are clustered in 75 locations in Norfolk, which are mostly busy intersections, roads in commercial areas, and freeway ramps. JA9, JA384-385, JA433-434, JA1728, JA2277.

NPD’s cameras cover only approximately 0.113% of Norfolk’s roadways and 0.0069% of the square mileage within city limits. JA9-10, JA433, JA2278-2279. Consistent with that sparse coverage, the cameras rarely photograph particular vehicles. Over a four-month sample period, the average vehicle was photographed

only once every two days. JA2282. And even the 5% of vehicles that were most photographed were on average photographed no more than once a day. JA2282.²

NPD chose to place ALPRs where there are high rates of violent crime, a large number of high-priority calls requiring immediate police presence, or numerous cars crossing into or out of Norfolk. JA9, JA384-385, JA424, JA1809. The few ALPRs in areas exclusively zoned as residential account for less than 1% of the photographs that the ALPRs take in Norfolk. JA2277-2278, JA2322-2323.

NPD has never purchased any Flock products other than ALPR cameras. JA384, JA1309-1310, JA2046. And NPD has only Flock's basic software package, meaning that—contrary to Plaintiffs' suggestion, Br.5-6—NPD has no access to “Convoy Analysis” and “Real-Time Routing” features. JA384, JA432-433, JA1341-1343, JA1357.³ Moreover, the Flock database that NPD uses does not incorporate data from other systems, and NPD officers cannot query other systems for ALPR data. JA392.

² NPD has access to data from around 40 Flock cameras operated by third parties in Norfolk who have opted to share that data. JA2344-2347. Including those cameras does not materially affect the statistics set forth above. JA2281-2282.

³ NPD has access to a “Vehicle Journey” feature, which notes on a map where an ALPR photographed a particular vehicle within a particular timeframe. JA243-244, JA1366-1367, JA1406-1407. It does not show where a vehicle stopped or started or the path it took. JA1411-1413.

NPD’s use of ALPRs has directly benefited the public in numerous ways. JA9, JA390-391. NPD has used the technology to recover stolen vehicles, reduce the auto-theft rate, locate missing people, and solve violent crimes. JA390-391. For example, NPD’s cameras in Norfolk played a key role in solving the murder of Ali Karim Muhammad, JA390; investigating the fatal shooting of Christopher Armbrister, JA386; *see Commonwealth v. Roberson*, 113 Va. Cir. 565 (2024); stopping a rash of commercial burglaries, *see Robinson v. Commonwealth*, 927 S.E.2d 822 (Va. Ct. App. 2026); and locating a missing woman, JA391. Other jurisdictions in Virginia and elsewhere in this Circuit (and the country) have likewise used ALPRs to protect local communities by solving numerous crimes and missing-persons cases.⁴

C. Legal Requirements Governing NPD’s ALPRs

In May 2025, Virginia enacted a statute imposing some of the Nation’s most restrictive conditions on use of ALPR data, including by NPD. *See* 2025 Va. Acts Ch. 720 (H.B. 2724); Va. Code § 2.2-5517. Those conditions include the following:

- ALPR data must be purged within 21 days, unless the data is part of an “ongoing investigation, prosecution, or civil action.” Va. Code § 2.2-5517(E).

⁴ *See, e.g.*, Dkt.132, at 4-8; Neera Tanden & Nick Wilson, Center for American Progress, *A Plan to Stop Crime in Our Communities* 27 & n.238 (Jan. 29, 2026), available at <https://www.americanprogress.org/article/delivering-accountability-a-plan-to-stop-crime-in-our-communities/>.

- Law-enforcement agencies can access ALPR data only for (1) a criminal investigation; (2) an investigation involving a missing, human-trafficked, or otherwise endangered person; or (3) notifications related to a missing, human-trafficked, or otherwise endangered person, a person with an outstanding warrant, a stolen vehicle, or a stolen license plate. *Id.* § 2.2-5517(D).
- Law-enforcement agencies are generally prohibited from sharing ALPR data with any out-of-state, federal, or private entity. *Id.* § 2.2-5517(F).
- Any ALPR query must have an “audit trail” showing who made the query and what it said, and law-enforcement agencies must audit their use of ALPR databases every 30 days. *Id.* § 2.2-5517(D), (H)(6).

In June 2025, Norfolk promulgated “Operational General Order—493: Flock Safety ALPR System” (“General Order”), which implements Section 2.2-5517 and imposes additional requirements. JA183-194. For example, under the General Order NPD’s Flock cameras may “be positioned” to photograph “only vehicles that are exposed to public view.” JA187. Any authorized user seeking to query the database must first enter a case number, an offense type, and the basis for reasonable suspicion. JA188. NPD must review its audit logs at least once a month. JA190. And to create a custom hotlist, which terminates after 21 days, an authorized user must receive supervisory approval after submitting a form stating the purpose of the alert. JA188-189.

NPD’s policies comply in full with the statute and the General Order. In some respects, NPD takes an even more restrictive approach to use of the ALPR data than those authorities require. JA385-389, JA466-474.

II. This Case

A. In October 2024, Plaintiffs Lee Schmidt and Crystal Arrington filed a Section 1983 complaint alleging that the ALPR cameras allow NPD to “access the whole of [Plaintiffs’] or any other driver’s movements” and therefore violate the Fourth Amendment. JA90; *see* JA58, JA74-97. The complaint alleged that Plaintiffs are ordinary citizens who live in or near Norfolk and simply prefer that the cameras not photograph their vehicles. JA76-77. And the complaint sought a declaratory judgment and a permanent injunction requiring Defendants to obtain a warrant before using the cameras to “collect images” or accessing any data they generate. JA87-96.

Discovery showed that the cameras did not, in fact, reveal the “whole” of Plaintiffs’ movements. Plaintiffs’ vehicles were photographed only sporadically: during an average 21-day retention period, Plaintiffs’ vehicles were photographed by an NPD camera on average between two and three times per day. JA10-11, JA392, JA2281. On days when Plaintiffs’ vehicles were photographed multiple times, the photographs were taken, on average, 45 to 50 minutes apart, with a distance of 2.5 to 3.5 miles separating the photographs. JA10-11, JA2282-2283, JA2326-2329. It was exceedingly rare for Plaintiffs’ vehicles to be photographed more than once in a 30-minute span, and an overwhelming majority of the time their vehicles were not photographed at all. JA2283, JA2326-2329. NPD also never

queried the database for any vehicle registered to either Plaintiff (except as part of discovery in this litigation), and—as Plaintiffs agree—there is no reason to expect that NPD will ever do so. JA11 (Plaintiffs “do not expect that they will be subject to an ALPR query in the future”); *see* JA392.

Plaintiffs did not put forward any expert testimony supporting their assertions that the cameras provide extensive information about their movements and daily lives, even though their experts had access to over four months of Norfolk data and two months of Hampton Roads data. JA2275. One expert did not even look at that data, much less how NPD uses it, and therefore admitted that he offered no opinion on whether “Flock camera data can be used to construct a realistic model of how people travel by car within Norfolk.” JA2938; *see* JA2904-2906, JA2936-2937. His work was limited to simulations of hypothetical routes that cars might travel in the city. The other expert did look at the data, but could not identify any specific places that Plaintiffs visited until after he was *told* what particular locations Plaintiffs frequent. Even then, he claimed to be able to infer only that one Plaintiff shopped at a grocery store and that the other *may* have visited her father. JA2229, JA2236, JA2261-2262, JA2570-2571. Ultimately, neither expert was willing to opine that the cameras tracked the whole of Plaintiffs’ movements or revealed their intimate associations. JA2494-2498, JA2900-2903.

B. The parties filed cross-motions for summary judgment, and the United States filed a Statement of Interest supporting Defendants. Dkt.139. The district court (Davis, J.) granted Defendants’ motion and denied Plaintiffs’ motion. JA1-51.

The district court first ruled that Plaintiffs had standing only to challenge the “taking and storing” of ALPR photographs and lacked standing to challenge any “quer[ies] of the ALPR database.” JA15, JA20-21; *see* JA21 (Plaintiffs “largely concede[d]” that standing point). The court noted that Plaintiffs had disclaimed any argument that Defendants violated the Fourth Amendment by “searching” the database for Plaintiffs’ “license plates”; that NPD had never queried the database for information about Plaintiffs’ vehicles; and that there was no imminent risk of any such query. JA20-21.

The district court next concluded that, on the undisputed facts, Defendants’ “collection and storage” of photographs of vehicles on public roads does not constitute a Fourth Amendment search. JA31-34. The court explained that, under well-established law, “citizens do not ‘have a reasonable expectation of privacy in the visible exterior parts of an automobile that travels the public roads and highways.’” JA31-32. And the court noted that “a collection of photos taken in public places that [is] never accessed or analyzed reveals *nothing* about a person’s movements from one place to another.” JA33-34.

The district court also ruled that, even assuming a challenge to querying were permissible, the summary-judgment evidence conclusively shows that there is no Fourth Amendment violation. JA34-47. The court explained that “what a person displays in public is definitionally not private—and the calculus only shifts when police surveillance is so intrusive that it crosses the line into cataloging the whole, or nearly the whole, of a person’s movements.” JA36; *see* JA24-30, JA35-42, JA47-50; *see also* JA37-40 (explaining that *Carpenter v. United States*, 585 U.S. 296 (2018), and *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc), involved “*near continuous*” data collection that could “consistently reveal where trips started, where they ended, or where . . . a driver stopped in between,” as well as movements outside of vehicles and in private spaces); JA40-42 (in *United States v. Jones*, 565 U.S. 400 (2012), there was “*continuous*” and lengthy GPS surveillance of a vehicle).

The district court concluded that the record evidence is “insufficient to demonstrate” that the Norfolk ALPR system takes “enough images of Plaintiffs—or other drivers—to reconstruct the whole of their movements” or to “provide an ‘intimate’ window into where citizens drive, park, visit, linger, sleep, or patronize.” JA35, JA43; *see* JA36, JA40-42. The cameras photograph only vehicles and only in certain locations; accordingly, during a “multi-month test period, full matches of Plaintiffs’ plates typically occurred miles apart, with lengthy gaps of time

unaccounted for by Defendants' ALPR system." JA38-39; *see* JA39 ("no data" in "nearly all of the 66 square miles of Norfolk"). "After the system identifies a car, it quickly loses the trail, and thus does not 'follow' or 'surveil' that same car unless it happens past another fixed ALPR camera," which can "occur hours or even days later" and "several miles away." JA41 (emphasis omitted). And although having multiple photographs of a car enables drawing a "rudimentary" line between "Point A and Point B," the informational holes are "pronounced," and there is no way of "knowing . . . even roughly where[] a vehicle starts a trip, drives, parks, lingers, or overnights." JA41-42; *see* JA45-46 (Virginia statute indicates that ALPR use "within [statutory] parameters" comports with public's "reasonable expectation of privacy").

The district court rejected the argument that it matters for constitutional purposes whether camera data can be combined with other information or "assumptions" to "*assist* in reconstructing a [driver's] route." JA42. The court explained that a Fourth Amendment search occurs only if the technology at issue *itself* reveals "all, or virtually all, of a person's movements" and thus enables deductions about an individual "*from*" those movements. JA48-49 (quoting *Beautiful Struggle*, 2 F.4th at 345); *see* JA42-43. The court further concluded that the record evidence is "insufficient to demonstrate that the ALPR images collected

by Defendants,” even “*when supplemented by ‘other’ investigative techniques,* reveals the whole of [drivers’] movements.” JA35.

SUMMARY OF ARGUMENT

I. As the district court correctly concluded, Plaintiffs have standing to challenge only the collection and storage of photographs of their vehicles. Plaintiffs ask this Court to consider what NPD *might* have done with the photographs had it queried the database for information about Plaintiffs’ vehicles. But Plaintiffs lack standing to raise such a claim: no such query has occurred, Plaintiffs admit there is no likelihood that one will ever occur, and Plaintiffs therefore have no actual or imminent injury from database querying. This Court should not permit Plaintiffs to assert others’ Fourth Amendment rights or to press their general policy preferences through the medium of this lawsuit.

II. The only question properly before this Court is whether NPD conducts a Fourth Amendment search when fixed ALPRs photograph vehicles traveling on public roads. As decades of precedent make clear, the answer is no. There is no reasonable expectation of privacy in the visible exterior parts of a vehicle traveling on public roads. And the government does not violate any such reasonable expectation when it photographs what anyone on the street could already see. Indeed, both the Supreme Court and this Court have recently made clear that use of security cameras in public places raises no constitutional problem.

III. Even if Plaintiffs did have standing to challenge querying of the database, those queries would not constitute a Fourth Amendment search, as the district court correctly held. Under settled precedent, the Fourth Amendment inquiry is whether the data “enables police” to analyze “the whole of individuals’ movements.” *Beautiful Struggle*, 2 F.4th at 333, 343-48. But the data here does not come close to doing so. That is true of ALPRs in general, as the Fifth Circuit and numerous other courts have held, and of the specific ALPRs in this case, as the Virginia appellate court has twice held. The record here clearly demonstrates that the cameras are in static locations covering well under 1% of Norfolk’s roads; that Plaintiffs’ vehicles were photographed very infrequently, with enormous gaps in geography and time; that camera data is purged after 21 days; and that even with access to months of data collected for this lawsuit, Plaintiffs’ experts were totally unable to use that data to determine where Plaintiffs traveled, let alone to open an intimate window into their private associations. That is very different from the scope and amount of data collected in *Carpenter* and *Beautiful Struggle*.

In the face of that fatal problem, Plaintiffs try to construct a new Fourth Amendment test from out-of-context snippets of those decisions—but that argument is forfeited and meritless. Among other issues, Plaintiffs simply elide from their newly invented test the central consideration in *Carpenter*, which they cannot satisfy: whether the data at issue is truly comprehensive.

IV. Plaintiffs’ final fallback argument, based on the purported original meaning of the Fourth Amendment, is waived, foreclosed by binding precedent, and wrong on its own terms. This Court should reject it out of hand.

STANDARD OF REVIEW

This Court reviews a grant of summary judgment de novo, *see Cybernet v. David*, 954 F.3d 162, 167 (4th Cir. 2020), and may affirm on any basis apparent in the record, *see Knibbs v. Momphard*, 30 F.4th 200, 230 (4th Cir. 2022).

ARGUMENT

I. Plaintiffs’ Standing Extends Only to the Collection and Storage of Photographs of Their Vehicles and Does Not Include Any Challenge to the Querying of the Database

Plaintiffs’ claim fails at the outset because they lack standing to challenge the primary conduct that forms the basis of their Fourth Amendment claim. The district court ruled that Plaintiffs have standing to challenge only the collection and storage of photographs of their vehicles—not the querying of the database where those photographs are stored. JA14-21 (citing *Scholl v. Ill. State Police*, 776 F. Supp. 3d 701, 719 (N.D. Ill. 2025), *appeal docketed*, No. 25-1847 (7th Cir.), reaching the same conclusions in a similar case). Plaintiffs have forfeited any challenge to the district court’s standing ruling, and in any event the ruling is straightforwardly correct.

A. 1. To establish Article III standing, plaintiffs must show an “injury in fact”—that is, a “particularized” injury that “affected” them “in a personal and individual way.” *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 381 (2024). That requirement screens out plaintiffs who have a “general legal, moral, ideological, or policy objection” rather than a “personal stake.” *Id.* at 379, 381.

Here, as the district court explained, NPD’s use of ALPRs proceeds in two steps. JA14-15. The first step is automatic: vehicles are photographed as they pass cameras, and the images are uploaded to a database. JA15. Typically, the images remain unseen for 21 days, at which point they are automatically deleted pursuant to Virginia law. JA191, JA440. But if an “NPD investigation calls for it” before deletion occurs, an authorized user can proceed to the second step: querying the database to see if a particular license plate or vehicle was photographed. JA15.

Plaintiffs have standing to challenge only the first step. Although Plaintiffs’ vehicles were photographed, and those images were uploaded to the database, NPD never queried the database for data on Plaintiffs’ vehicles (except to comply with Plaintiffs’ discovery requests in this action). JA11, JA20, JA392. Moreover, Plaintiffs have conceded that they “do not expect that they will be subject to an ALPR query in the future,” JA11—which means that they face no imminent risk of any future querying of the database for information about their vehicles, JA11, JA20 (citing Dkt.140, at 11), JA392; *see Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560

(1992) (Article III injury-in-fact must be “actual or imminent, not conjectural or hypothetical”). The district court therefore “easily conclude[d]” that Plaintiffs lack standing to press a claim that querying the database amounts to a constitutional violation. JA20.

That conclusion is self-evidently correct. Given that querying has never affected Plaintiffs and is not likely ever to do so, their complaints about querying necessarily concern only what happened (or could happen) to others. But Plaintiffs cannot rest their claim on government conduct that affects only other people. *See Hippocratic Med.*, 602 U.S. at 393 n.5. Plaintiffs also cannot leverage an alleged injury (here, the fact that their vehicles were photographed) to attack conduct that did not cause that injury. “[S]tanding is not dispensed in gross,” and a plaintiff cannot, “by virtue of his standing to challenge one government action, challenge other governmental actions that did not injure him.” *DaimlerChrysler v. Cuno*, 547 U.S. 332, 353 & n.5 (2006); *see Blum v. Yaretsky*, 457 U.S. 991, 999 (1982); *see also, e.g., Scholl*, 776 F. Supp. 3d at 719.

This case illustrates why those standing limitations matter. The injury-in-fact requirement prevents plaintiffs from using the federal courts to litigate generalized policy disagreements properly “resolved by the political branches.” *Hippocratic Med.*, 602 U.S. at 379-80. Such restraint is especially warranted in the Fourth Amendment context, where legislatures are uniquely “well situated” to “balance

privacy and public safety.” *Jones*, 565 U.S. at 429-30 (Alito, J., concurring). Here, the Virginia General Assembly recently passed a statute that authorizes the use of ALPRs and ALPR data subject to carefully calibrated constraints. *See* Va. Code § 2.2-5517.⁵ Individuals like plaintiffs who are not injured by conduct that the law addresses cannot use the courts to side-step that enactment.

The injury-in-fact requirement also ensures that “legal questions” will “be resolved, not in the rarified atmosphere of a debating society, but in a concrete factual context.” *Hippocratic Med.*, 602 U.S. at 379. Federal courts thus routinely address (and reject) Fourth Amendment challenges to ALPR technology in criminal cases, where suppression hearings create factual records that establish how law enforcement uses ALPR data as to particular criminal defendants. *See, e.g., United States v. Martin*, 753 F. Supp. 3d 454 (E.D. Va. 2024). But here, because NPD never queried the database for Plaintiffs’ vehicles or license plates, there is no concrete factual context for deciding a Fourth Amendment question about querying.

The abstractness of Plaintiffs’ claim is especially apparent when considering the “analysis” that Plaintiffs’ experts offered in this case. One expert offered a purely hypothetical “simulation” analysis that did not rely on the actual ALPR data or database—much less on any actual facts about how NPD officers use the database.

⁵ Plaintiffs’ counsel advocated against that law before the General Assembly. *See* Courts of Justice, *Virginia Senate*, SR A (305), Feb. 10, 2025 (video at 2:25:20), *available at* https://virginia-senate.granicus.com/ViewPublisher.php?view_id=3.

JA2906-2910, JA2955. That expert conceded that he had “no knowledge of how [NPD] is actually using” the database and could not assess whether “Flock camera data could be used to construct a realistic model of how people travel by car within Norfolk.” JA2904, JA2398. Plaintiffs’ other expert reviewed the ALPR data, but he conducted a wholly artificial analysis in which he was simply *told* locations that Plaintiffs actually frequent and then used that information to try to determine where they might have gone. JA2486-2487, JA2570-2571. That exercise bears little resemblance to the information that a query of the database might yield.

2. Although the district court did not reach the issue, Plaintiffs lack Fourth Amendment standing (a non-jurisdictional requirement) for all the same reasons. To invoke the Fourth Amendment, a person must show that “his own Fourth Amendment rights” were “infringed by” the conduct he seeks to challenge, *Byrd v. United States*, 584 U.S. 395, 403 (2018), and Plaintiffs cannot make that showing. Asserting a violation of “someone else’s[] Fourth Amendment rights” is not sufficient. *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *see Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978); *Dow Chem. v. United States*, 476 U.S. 227, 238 n.5 (1986).

B. 1. Plaintiffs have forfeited several times over any challenge to the district court’s lengthy standing analysis. First, Plaintiffs address standing in only a single footnote in their brief in this Court. Br.41 n.16. But arguments raised solely in an “isolated footnote” are not preserved on appeal. *See Foster v. Univ. of Md.-E. Shore*,

787 F.3d 243, 250 n.8 (2015). And Plaintiffs’ lone footnote—which asserts only that they have standing to challenge the “collection, and maintenance in a government database, of records relating to” them, Br.41 n.16—does not even contest the district court’s holding that they lack standing to challenge any querying of the database. JA34.

Second, as the district court explained, Plaintiffs “largely concede[d]” below that they lacked standing “to challenge the query stage of Defendants’ ALPR system.” JA21; *see* JA20 (relying on “Plaintiff[s]’ own admissions”). Plaintiffs’ forfeiture below bars them from asserting on appeal that they have standing to challenge querying, especially as “any argument against forfeiture is forfeited too” by Plaintiffs’ failure to raise it in their opening brief. *Bloosurf v. T-Mobile*, 170 F.4th 264, 272-73 (4th Cir. 2026).⁶

2. Forfeiture aside, Plaintiffs have not come close to establishing that they have standing to challenge querying of the database.

As noted above, Plaintiffs’ footnote asserts only that they have standing to challenge the “collection, and maintenance in a government database, of records relating to” them, citing *Wikimedia Foundation v. NSA*, 857 F.3d 193, 210 (4th Cir.

⁶ Plaintiffs may not raise new standing arguments on reply. *See McGinn v. Broadmead*, 167 F.4th 667, 674-75 (4th Cir. 2026). Although *lack* of subject-matter jurisdiction may be raised at any time, arguments that this Court *possesses* jurisdiction are forfeitable. *See, e.g., Est. of Van Emburgh v. United States*, 95 F.4th 795, 800 (4th Cir. 2024).

2017). But the relevant question is whether Plaintiffs *also* have standing to challenge NPD’s querying of the database—and *Wikimedia* confirms that they do not. There, this Court held that the plaintiffs lacked standing to press one of two theories of liability because they had failed to plausibly allege an injury under that theory. 857 F.3d at 209-16. Much the same is true here: even if Plaintiffs have standing to challenge the collection and storage of photographs, they lack standing to challenge other conduct that caused them no injury. *See Warth v. Seldin*, 422 U.S. 490, 500 (1975).

Plaintiffs assert that “*collection* of raw data” is necessarily a search “even if the data only reveal intimate details through later ‘analysis,’” since “[a] bathtub is a less private area when the plumber is present even if his back is turned.” Br.42 n.16 (quoting *Kyllo v. United States*, 533 U.S. 27, 36, 39 (2001)). But Plaintiffs confuse standing and the merits. In some cases, courts have concluded on the merits that *collection* of data is a search because the data being collected *is itself private*, like data about what is happening in the interior of someone’s home. *See Kyllo*, 533 U.S. at 34. As discussed below, Plaintiffs have not even tried to make a similar showing here—doubtless because the only data collected is data about vehicle locations on public roadways. *See pp.25-29, infra*. But that has nothing to do with standing—and Plaintiffs are just wrong that they can parlay one form of standing (to challenge data collection) into another form of standing (to challenge subsequent use of the

data), as such “dispens[ation]” of standing “in gross” is forbidden. *DaimlerChrysler*, 547 U.S. at 353 & n.5.

Finally, Plaintiffs appear to rely on a standing discussion in the panel decision in *Beautiful Struggle*, see Br.42 n.16 (citing 979 F.3d 219, 225 (4th Cir. 2020)), but to no avail. That decision has been vacated and lacks any precedential force. See *Alvarado v. Bd. of Tr.*, 848 F.2d 457, 459 (4th Cir. 1988). And the subsequent en banc decision, which does not address standing, makes clear that the *Beautiful Struggle* plaintiffs faced a significant risk that their images had been or would be accessed and analyzed, not simply collected and stored away. In that case, an aerial surveillance program took a photograph every second of a massive swath of Baltimore; law enforcement reviewed that data to “track individuals and vehicles from a crime scene”; the plaintiffs did work that “necessarily involve[d] . . . being present outdoors in areas with high rates of violent crime,” including “visit[ing] scenes . . . as soon as possible after a crime”; and the plaintiffs were therefore particularly likely to appear in images that law enforcement actively reviewed. 2 F.4th at 334-35, 337. Plaintiffs’ situation could not be more different, as law enforcement has never even queried a database for Plaintiffs’ cars, let alone actively reviewed data about Plaintiffs. Accordingly, nothing about *Beautiful Struggle* comes close to suggesting that Plaintiffs have standing to challenge database querying.

II. Collection and Storage of Photographs of Plaintiffs' Vehicles on Public Roads Is Not A Fourth Amendment Search

Because the only possible injury Plaintiffs can claim is the taking and storing of photographs of their vehicles, the only argument Plaintiffs can raise is that taking and storing photographs of vehicles on public roads is a Fourth Amendment search that requires a warrant. But that argument is wrong, as confirmed by binding precedent that Plaintiffs ignore. “A ‘search’ occurs for purposes of the Fourth Amendment where the government violates a person’s ‘reasonable expectation of privacy,’” *United States v. Taylor*, 54 F.4th 795, 803 (4th Cir. 2022), and no such reasonable expectation can exist as to taking and storing the photographs here.

A. The Supreme Court and this Court have long held that “one does not have a reasonable expectation of privacy in the visible exterior parts of an automobile that travels the public roads and highways.” *United States v. George*, 971 F.2d 1113, 1120 (4th Cir. 1992).

That is so for a host of independent, mutually reinforcing reasons. First, driving a car on a public road necessarily exposes the car to the public. Indeed, a car “has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.” *United States v. Knotts*, 460 U.S. 276, 281 (1983). And viewing something “already in plain view does not involve an invasion of privacy.” *United States v. Runner*, 43 F.4th 417, 421 (4th Cir. 2022).

That logic applies with particular force to the “visible exterior parts of an automobile,” *George*, 971 F.2d at 1120, including its license plate. After all, the “exterior of a car” inevitably is “thrust into the public eye,” such that “to examine it does not constitute a ‘search.’” *New York v. Class*, 475 U.S. 106, 114 (1986). And the public understands that license plates are “required by law to be located in a place ordinarily in plain view from the exterior of the automobile.” *Id.*; see Va. Code §§ 46.2-715, 46.2-1013(B) (requiring that license plates be displayed and illuminated); see also *United States v. Ellison*, 462 F.3d 557, 561-63 (6th Cir. 2006).

Second, drivers on public roads *choose* to expose vehicles and their movements to public view. A driver “voluntarily convey[s] to anyone who want[s] to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.” *Knotts*, 460 U.S. at 281-82. Thus, in *George*, a driver “lacked a reasonable expectation of privacy in his tires” because, “[h]aving chosen to drive and park his truck in public, [he] had no ‘effective[.]’ way to ‘bar the public from viewing’” them. 971 F.2d at 1120-21.

Third, vehicles are commonly subject to close scrutiny by law enforcement under “pervasive and continuing governmental regulation and controls.” *Class*, 475 U.S. at 113. “As an everyday occurrence, police stop and examine vehicles when license plates or inspection stickers have expired, or if other violations” are “noted,”

id., and as a result “[t]he public is fully aware that it is accorded less privacy in its automobiles,” *California v. Carney*, 471 U.S. 386, 392 (1985).

Finally, there is a “lesser expectation of privacy” associated with a vehicle because it is a form of “transportation” that “seldom serves as one’s residence or as the repository of personal effects.” *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality op.); *see Class*, 475 U.S. at 112. Vehicles are fundamentally different from the home, where “intimate activities” take place, *Dow*, 476 U.S. at 236, and “privacy expectations are most heightened,” *Florida v. Jardines*, 569 U.S. 1, 7 (2013).

B. It is equally well established that law enforcement does not violate any reasonable expectation of privacy by photographing things that are otherwise open to public view. Thus, use of the fixed cameras at issue in this case cannot create a reasonable expectation of privacy where none would otherwise exist.

This Court has so held multiple times. In *United States v. Vankesteren*, 553 F.3d 286, 291 (4th Cir. 2009), for example, this Court upheld the use of a motion-activated pole camera in an open field, reasoning that so long as the defendant “had no legitimate expectation of privacy” in the field, officers “were free, as on public land, to use video surveillance to capture what any passerby would have been able to observe.” *Id.* at 291. Similarly, in *L.R. Willson & Sons v. Occupational Health & Safety Review Commission*, 134 F.3d 1235 (4th Cir. 1998), this Court held that

“use of a telephoto camera lens” did not render unreasonable otherwise reasonable police observation. *Id.* at 1238-39. Accordingly, this Court recognized in *Beautiful Struggle* that “[p]eople understand that they may be filmed by security cameras on city streets.” 2 F.4th at 345; *see id.* at 345-46.⁷

The Supreme Court also has recently refused to “call into question conventional surveillance techniques and tools, such as security cameras.” *Carpenter*, 585 U.S. at 316. But that is exactly what treating photographs of public behavior as a search would do—thereby upending long-settled law-enforcement practices.

C. Together, those two principles resolve this case: Plaintiffs have no reasonable expectation of privacy in the exteriors of their vehicles as they travel public roads, so taking and storing photographs of those vehicles on those roads is not a Fourth Amendment search. It is undisputed that NPD’s ALPRs act in a “physically nonintrusive manner,” *George*, 971 F.2d at 1120, to “photograph external vehicle characteristics that are visible to the naked eye,” and that they do so “on the public roadways,” JA7-8; *see* JA187. The cameras thus collect information

⁷ *Accord, e.g., United States v. Harry*, 130 F.4th 342, 350 (2d Cir. 2025) (“collection of footage of activities in public view” at business); *United States v. Houston*, 813 F.3d 282, 287-88 (6th Cir. 2016) (“video footage recorded by a camera” on “top of a public utility pole” that “captured the same views enjoyed by passersby on public roads”); *United States v. Hay*, 95 F.4th 1304, 1316 (10th Cir. 2024) (“camera surveillance of a home visible to passersby”).

that Plaintiffs already made public (and, with respect to license plates, *had to* make public). And absent government action to “access[] or analyze[]” a “collection of photos taken in public places,” which never occurred with respect to Plaintiffs and which Plaintiffs do not have standing to challenge, *see* pp.17-24, *supra*, those photographs reveal nothing at all about Plaintiffs’ movements, JA34.

Plaintiffs close their eyes to all of that. In a case about vehicles, Plaintiffs do not cite *Knotts*, *Class*, or *George*, even though the district court relied on each of them. JA3, JA24, JA32-33. And in a case about photographs, Plaintiffs do not cite *Vankesteren* or the discussions in *Carpenter* and *Beautiful Struggle* acknowledging the constitutionality of security cameras, even though, again, the district court cited each of them. JA32. Yet those on-point authorities dictate affirmance here, and this Court need go no further to resolve this appeal in Defendants’ favor.

III. Even Assuming that Plaintiffs Had Standing to Challenge Querying of the Database, That Querying Is Not a Fourth Amendment Search

As the district court correctly concluded, even assuming that Plaintiffs had standing to challenge querying of the database, that challenge fails on the merits. JA34-50. Plaintiffs inexplicably fault the district court for “fail[ing] to consider” the “*capabilities*” of NPD’s system. Br.30, 45. But the court *did* consider those capabilities—including in a 13-page section of its decision titled “Capability Focus,” JA34-47—and correctly held that querying the database and considering the resulting data is not a Fourth Amendment search.

A. Under Governing Precedent, Querying The Database Is Not A Search

1. No Search Exists Absent Invasion of a Reasonable Expectation of Privacy in the Whole of Plaintiffs' Movements

In determining whether police access to data about people's physical movements constitutes a Fourth Amendment search, the Supreme Court and this Court have held that the pertinent question is whether the data "enables police" to analyze "the whole of individuals' movements." *Beautiful Struggle*, 2 F.4th at 333, 343-46, 348; *accord Carpenter*, 585 U.S. at 313.⁸

That is a high bar—and rightly so. Many of the places that people go are fully open to public observation, and there is generally no reasonable expectation of privacy in things that a person does in public. *See pp.25-29, supra*. Thus, it is only when data about a person's public movements is highly detailed—so as to reveal "intimate" information about individuals' private "associations and activities"—that police access to that data invades an individual's privacy for Fourth Amendment purposes. *Beautiful Struggle*, 2 F.4th at 342.

⁸ *United States v. Jones*, 565 U.S. 400 (2012), found a Fourth Amendment violation based on "physical[] occup[ation]" of "private property" through placing a GPS tracking device on a car. *Id.* at 404. No such occupation is at issue here. The GPS device in *Jones* also tracked *all* of a car's movements over time, *see id.* at 402-03, which NPD's cameras do not do.

Only near-comprehensive data satisfies that test. To be sure, access to data about someone’s movements may violate a reasonable expectation of privacy even if the data does not reveal *every single place* that a person goes. *See Beautiful Struggle*, 2 F.4th at 343; *see also Ohio v. Robinette*, 519 U.S. 33, 39 (1996). Nevertheless, precedent makes clear that data about someone’s movements does not violate a reasonable expectation of privacy absent “detailed, encyclopedic” records. *Beautiful Struggle*, 2 F.4th at 341 (quoting *Carpenter*, 585 U.S. at 309).

In *Carpenter*, for example, the Supreme Court found a Fourth Amendment search only where cell-site location information (“CSLI”) allowed the government to “achieve[] near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” 585 U.S. at 312. The CSLI tracked people carrying cell phones not only in public places but on private land and inside private buildings—for instance, a work site or a doctor’s office to which the general public has no access—and even inside their homes. *See id.* at 311. And it did so almost continuously. For instance, the data about the criminal defendant in *Carpenter* yielded “12,898 location points cataloging [his] movements—an average of 101 data points per day” for over four months. *Id.* at 302. That type of data, the Court concluded, provided “an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.” *Id.* at 311.

Beautiful Struggle relied on similarly comprehensive surveillance in concluding that a Fourth Amendment search took place. The aerial surveillance in that case was extraordinarily thorough, with planes almost continuously taking photographs covering virtually the entire city while the sun was up. As this Court explained, those planes flew “at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day” and taking images that “capture[d] roughly 32 square miles per image per second.” 2 F.4th at 334. The resulting data “‘track[ed] every movement’ of every person outside in Baltimore” during most daytime hours, including movements that were not on public roads or in other public spaces—for instance, in an enclosed private backyard. 2 F.4th at 341 (quoting *Carpenter*, 585 U.S. at 307). On those facts, this Court ruled that—as in *Carpenter*—the data gave police an “‘intimate window’ into a person’s associations and activities.” *Id.* at 342 (quoting *Carpenter*, 585 U.S. at 311).

2. There Is No Such Invasion of a Reasonable Expectation of Privacy Here

Under that analysis, querying a database to access data from the NPD cameras does not constitute a Fourth Amendment search. As courts across the country have uniformly ruled, data from ALPRs does not provide information about the whole of an individual’s movements or an intimate window into that person’s associations and activities. And, as the extensive evidentiary record in this case demonstrates, data from the ALPRs used by NPD most certainly does not provide that kind of

information—or anything remotely close to it. That is exactly why the Virginia Court of Appeals has twice rebuffed Fourth Amendment challenges to NPD’s use of ALPRs.

a. *ALPRs generally.* ALPRs take photographs of vehicles operated on public roads, but cannot track the whole of any individual’s movements, or anything approaching that whole. JA7-8, JA35, JA1309; *see* pp.10-11, *supra*. ALPRs do not photograph an individual’s vehicle everywhere it goes in public, because they are fixed in only some locations. JA41-42 (ALPRs photograph “*locations*, not *individuals*”); *see Katz v. United States*, 389 U.S. 347, 351 (1967) (Fourth Amendment “protects people, not places”); *Knotts*, 460 U.S. at 281-82. And “unlike a cell phone or ankle monitor, [ALPRs] do not ‘follow’ individuals inside buildings, homes, or anywhere else.” JA7. Because they cannot “faithfully follow[]” individuals “beyond public thoroughfares and into private residences” and “other potentially revealing locales,” *Carpenter*, 585 U.S. at 311, they are incapable of revealing any intimate conduct that may occur in those locations.

Carpenter and *Beautiful Struggle* confirm that data from cameras like ALPRs does not give rise to any Fourth Amendment problem. The Supreme Court specifically declined in *Carpenter* to “call into question conventional surveillance techniques and tools, such as security cameras” or devices that would record only “a person’s movement at a particular time.” 585 U.S. at 315-16. And this Court in

Beautiful Struggle similarly distinguished “pole cameras” and “security cameras,” which are “fixed in place,” from the aerial-surveillance technology that recorded nearly all the daytime outdoor movements of everyone in Baltimore, even in a private outdoor space. 2 F.4th at 345; *accord, e.g., Vankesteren*, 553 F.3d at 291 (upholding use of pole camera).

Indeed, although ALPRs share all of those qualities of security cameras and pole cameras, in many ways ALPRs are *more* protective of privacy than those types of cameras. Unlike those cameras, ALPRs do not pan, tilt, or zoom, so they cannot follow any object, even in their proximity. JA433-434. And, importantly, ALPRs by their nature take pictures of *vehicles* on public roads. JA7-9, JA433-434, JA2047. That fact is critical, because, as discussed above, a driver “travelling in an automobile on public thoroughfares” has no reasonable expectation of privacy either in the exterior of his vehicle or in his “movements from one place to another.” *Knotts*, 460 U.S. at 281; *see pp.25-29, supra*. Thus, although a pole camera may record individuals “engag[ing] in any number of intimate activities” “under the belief that they are not being observed,” *Vankesteren*, 553 F.3d at 291, ALPRs photograph only an inherently public activity, and only in locations where individuals are “fully aware” that they may be observed, *Carney*, 471 U.S. at 392.

It should come as no surprise, then, that every federal court to address the constitutionality of ALPR systems has held that they do not violate a reasonable

expectation of privacy.⁹ In so holding, those courts have repeatedly distinguished *Carpenter* and *Beautiful Struggle*. See, e.g., *Martin*, 753 F. Supp. 3d at 472; *Jackson*, 2025 WL 1530574, at *8; *Bowers*, 2021 WL 4775977, at *5. The Fifth Circuit’s recent decision in *Porter* exemplifies that consensus. *Porter* holds that because a motorist “has no reasonable expectation of privacy in his movements from one place to another,” and because ALPRs provide only “periodic information about a vehicle’s location on public streets and highways,” an ALPR system could not “track[] the whole of an individual’s movements, much less for a very long period,” and thus did not invade any reasonable expectation of privacy. 170 F.4th at 386-87.

⁹ See, e.g., *United States v. Porter*, 170 F.4th 381, 386-87 (5th Cir. 2026); *United States v. Lawrence*, 2026 WL 765307, at *1 (D.N.D.); *United States v. Floyd*, 811 F. Supp. 3d 1345, 1345-50 (M.D. Fla. 2025); *Schemel v. City of Marco Island Fla.*, 2025 WL 2958798, at *2 (M.D. Fla.), *appeal docketed*, No. 25-13913 (11th Cir.); *Rinaldi v. Sylvester*, 2025 WL 2682691, at *16-18 (S.D.N.Y.); *United States v. Brown*, 2025 WL 2444596, at *3-5 (W.D. Okla.); *United States v. Acosta*, 2025 WL 2427700, at *4-6 (N.D. Okla.); *United States v. Sturdivant*, 786 F. Supp. 3d 1098, 1107-14 (N.D. Ohio 2025), *appeal docketed*, No. 26-3426 (6th Cir.); *United States v. Jackson*, 2025 WL 1530574, at *5-10 (D. Kan.); *United States v. Griffin*, 2025 WL 1474679, at *8-9 (S.D. Ind.); *Scholl*, 776 F. Supp. 3d at 713-21; *United States v. Cooper*, 2025 WL 35035, at *4-7 (E.D. La.); *Martin*, 753 F. Supp. 3d at 468-76; *United States v. Salcido-Gonzalez*, 2024 WL 2305478, at *11-12 (D. Utah); *United States v. Jiles*, 2024 WL 891956, *16-19 (D. Neb.); *United States v. Toombs*, 671 F. Supp. 3d 1329, 1339-42 (N.D. Ala. 2023); *United States v. James*, 2023 WL 3370421, at *4-6 (W.D. La.); *United States v. Graham*, 2022 WL 4132488, at *4-5 (D.N.J.); *United States v. Porter*, 2022 WL 124563, at *2-3 (N.D. Ill.); *United States v. Brown*, 2021 WL 4963602, at *1-4 (N.D. Ill.); *United States v. Bowers*, 2021 WL 4775977, at *2-5 (W.D. Pa.); *United States v. Rubin*, 556 F. Supp. 3d 1123, 1127-30 (N.D. Cal. 2021).

Those decisions also illustrate that the exact number of ALPRs that a city chooses to install is relevant only to the extent that it bears on whether the cameras can be used to reveal intimate details. Some courts that have rejected Fourth Amendment challenges to ALPR systems have done so in cases involving greater numbers of cameras than the 176 ALPRs in 75 clusters at issue here. *See, e.g., Sturdivant*, 786 F. Supp. 3d at 1103 (1,636 ALPRs in Cuyahoga County, Ohio); *Griffin*, 2025 WL 1530574, at *9 (as many as 600 ALPRs in Marion County, Indiana); *Scholl*, 776 F. Supp. 3d at 707 (344 ALPRs in Cook County, Illinois); *Martin*, 753 F. Supp. 3d at 468 (188 ALPRs in and around Richmond, Virginia). And any approach that depends on a specific number of cameras would “launch courts” on an impossible “line-drawing expedition.” *Riley v. California*, 573 U.S. 373, 401 (2014); *see* Orin Kerr, *The Digital Fourth Amendment* 174-77 (2025) (arguing against test that forces courts to “announc[e] bizarre and arbitrary lines”).

b. NPD’s ALPRs. This Court need not opine on the constitutionality of ALPRs generally to resolve this case, as it is plain that querying a database for data from NPD’s ALPRs in particular does not invade any reasonable expectation of privacy. The district court reviewed an extensive summary-judgment record, assessed “what [NPD’s] ALPR system is *capable of revealing* if queried,” and determined on undisputed facts that the system came nowhere close to allowing NPD to “reconstruct the whole of [Plaintiffs’] movements”—or anyone else’s—or

providing an intimate window into any driver's life. JA34-50. That analysis was correct, and it accords with two recent decisions of the Virginia Court of Appeals upholding the constitutionality of the very same NPD system at issue here.

i. To start, it bears repeating that NPD's ALPRs take photographs of only vehicles on public roads at fixed locations and do not collect information about individuals outside of cars. *See* pp.25-29, *supra*; JA7-8, JA35, JA40, JA386. Those facts alone distinguish this case from *Carpenter* and *Beautiful Struggle*, where the relevant technology effectively allowed police to "attach[] an ankle monitor" to individuals and follow them into private places. *Beautiful Struggle*, 2 F.4th at 341 (quoting *Carpenter*, 585 U.S. at 312).

NPD's ALPRs also do not collect anything like the kind of comprehensive data at issue in *Carpenter* and *Beautiful Struggle*, whether in terms of sheer scope of coverage or the number of data points gathered. The CSLI data in *Carpenter* revealed "an average of 101 data points per day," resulting in "near perfect" and near-continuous surveillance, 585 U.S. at 302, 312, and the aerial surveillance in *Beautiful Struggle* tracked "every movement of every person outside in Baltimore" in daylight via 32-square-mile-wide photographs taken every second, 2 F.4th at 341.

The data from NPD's ALPRs do nothing of the sort. Those cameras are "fixed in 75 clusters across the many miles of Norfolk roadways," covering only 0.113% of Norfolk's roadways and 0.0069% of the square mileage within city limits, JA9-

10, JA433, JA2278-2279, and they do not collect *any* data on any part of Norfolk’s 66 square miles save for those 75 “static locations,” JA36, JA39. The cameras can locate a vehicle only “for the brief time” it is “in one of” those “75 designated areas”; because the cameras are fixed in place and cannot tilt or pan, they cannot “‘follow’ or ‘surveil’” anyone. JA38, JA41. It might be “days” between one photograph of a particular vehicle and the next photograph. JA41. And any data the cameras collect is purged 21 days after the photograph is taken, absent an ongoing investigation or case. JA387-388, JA440; Va. Code § 2.2-5517(E).

The record evidence regarding Plaintiffs’ vehicles demonstrates concretely how little data NPD’s ALPRs collect about any individual’s movements in the city. Although Plaintiffs originally alleged that the cameras could closely track their movements and identify intimate details about their lives, JA85-89, the actual facts tell a very different story. Plaintiffs received in discovery all NPD ALPR data collected over a period of roughly four months (and additional data from surrounding areas). JA2275.¹⁰ That data showed that Plaintiffs’ vehicles were rarely photographed—on average only two or three times per day. JA10; *see* JA2281-2282 (95% of cars photographed were photographed even less). And those photographs of Plaintiffs’ vehicles were taken, on average, roughly three miles apart. JA10-11,

¹⁰ The data was retained for more than 21 days only because of Plaintiffs’ decision to sue.

JA2283. That left vast gaps in information about the location of Plaintiffs' vehicles, in both temporal and geographical terms. JA38 ("miles apart" with "lengthy gaps of time"). Accordingly, as the district court concluded, the data cannot identify "where, or even roughly where, a vehicle starts a trip, drives, parks, lingers, or overnights." JA41; *see* JA39 (data "does not consistently reveal where trips started, where they ended, or where (or even in which specific 'quadrant') a driver stopped in between"); JA386; *see also* JA2283, JA2326-2329 ("overwhelming majority" of "time" in Plaintiffs' days did not include any ALPR photographs).

Unsurprisingly, Plaintiffs' own experts could draw virtually no conclusions from the data about Plaintiffs' activities, let alone open an intimate window into Plaintiffs' private lives. The single Plaintiffs' expert who actually examined the data admitted that he could not "necessarily identify the specific location or address a person visited based on ALPR captures alone." JA2259. With months of data at his fingertips, that expert opined only that one Plaintiff shopped at one grocery store—but only after counsel told the expert that Plaintiff shopped there, allowing the expert to rule out the many other nearby stores. JA2261-2262; *see* JA2229, JA2286-2289, JA2570-2571. Use of ALPR data to "discover" something the expert already knew is hardly an invasion of anyone's privacy. Otherwise, the expert was unable to use the ALPR data to offer *any* opinion about Plaintiffs' activities, associates, or affiliations. Plaintiffs incorrectly assert (Br.38) that the expert also deduced that one

Plaintiff visited her father; in fact, the expert opined only that the Plaintiff likely visited a residential neighborhood where he had been told (but could not determine from the data) the Plaintiff's father lived. JA2236, JA2293; *see* JA2542-2543 (the expert admitting he could tell only that Plaintiff was in "general area" likely containing many houses and businesses).

Plaintiffs' other expert, who *did not review any* of NPD's ALPR data, disclaimed any view on whether "Flock camera data can be used to construct a realistic model of how people travel by car within Norfolk." JA2938; *see* pp.10-11, *supra*. He engaged in only a "simulation" analysis, and he conceded that he would not be able to use ALPR data to reconstruct even a small percentage of most of his simulated routes. JA2955, JA2978-2979; *see* JA2300-2303. And even if NPD's ALPR data *could* "reconstruct one route," or "link a vehicle to one church or to one business due to the fortuitous placement of one or more ALPR cameras," *id.*, this case still would not resemble *Carpenter* and *Beautiful Struggle*. The Fourth Amendment violations there arose not from "reconstructing *one route*, but tracking *all* (or nearly all) of a citizen's movements." JA44.

For those reasons, the only possible conclusion the evidentiary record supports is the one the district court drew: NPD's ALPRs neither "'track' the whole of a person's movements" nor "provide an 'intimate' window into where citizens drive, park, visit, linger, sleep or patronize." JA43; *see* JA36-41, JA386. Rather,

NPD’s system “has many thousands more blind spots than it has ‘unblinking eyes.’”

JA38. Plaintiffs are therefore incorrect in their unsupported assertion that NPD’s ALPRs can “capture enough information to enable police to reconstruct many people’s habitual routes,” Br.32—which would in any event not be the same thing as tracking the whole of any person’s movements. Under *Carpenter* and *Beautiful Struggle*, there is no Fourth Amendment search and therefore no Fourth Amendment violation.

ii. Having failed to put forward evidence sufficient to raise a genuine issue of fact as to the existence of a search under a correct understanding of the law, Plaintiffs fall back to several arguments that distort the legal standard.

First, Plaintiffs assert that it is enough that ALPRs allow NPD to “deduce, in combination with other information, where a person likely went.” Br.36.¹¹ That is irrelevant here. As the district court correctly concluded, the record evidence is “insufficient to demonstrate that the ALPR images collected by Defendants,” even “*when supplemented by ‘other’ investigative techniques, reveal[] the whole of [drivers’] movements*” or anything close to the whole. JA35; *see* JA47-50.

¹¹ Plaintiffs no longer appear to argue, as they did below, that use of technology constitutes a search if it merely “*contributes*” to an “ability to ‘track’ an individual’s movements,” JA48—and for good reason, as virtually any technology would meet that test. But Plaintiffs do seem to suggest (Br.40) that use of technology qualifies as a search if it provides a piece of information *necessary* to locate a suspect.

In any event, as the district court also recognized, Plaintiffs’ “combination” argument is legally incorrect. JA47-50. That word appears in the case law, *see Carpenter*, 585 U.S. at 312, but Plaintiffs wrest it out of context and twist its meaning. The only relevant question, as this Court has stated, is whether the technology at issue *itself* reveals “the whole of individuals’ movements.” *Beautiful Struggle*, 2 F.4th at 345; *see id.* (explaining that in *Carpenter* the Court held that a search “took place when the government accessed the CSLI” because the CSLI itself “enabled the deductions” from the whole of individuals’ movements (citing *Carpenter*, 585 U.S. at 312)); JA49 (“collection and analysis of 2 or 3 (or even several more) scattered ALPR data points, sometimes miles and hours apart,” does not “constitute[] a ‘search’ simply because this data contributes one or more pieces to a larger investigative jigsaw puzzle”). Plaintiffs’ very different approach would transform into a search requiring a warrant all manner of routine police investigative techniques—like witness interviews and physical surveillance—that are necessary to deducing where someone went, thereby severely hampering law enforcement and harming the public. *See, e.g., United States v. Murillo-Lopez*, 151 F.4th 584, 589 (4th Cir. 2025) (physical surveillance used to locate suspect).¹²

¹² Plaintiffs’ amici contend that even if one form of technology does not enable deductions from the whole of individuals’ movements, data collected using that technology might do so if combined with other forms of data from other sources. *See Policing.Project.Br.11-17*. But NPD’s ALPR system does not incorporate information from other systems, and officers cannot query other systems for ALPR

Second, Plaintiffs assert that *Beautiful Struggle* held that *any* “habits and patterns are inherently intimate,” Br.33, such that any police activity that discovers them is a Fourth Amendment search. But *Beautiful Struggle* says no such thing; it repeatedly emphasizes that the question is whether there is an invasion of a reasonable expectation of privacy in “the whole of [someone’s] movements.” *E.g.*, 2 F.4th at 333, 341-46. And, again, Plaintiffs’ newly invented rule would require a warrant for a vast array of commonplace police activities, such as parking outside someone’s workplace to observe his comings and goings. That is not the law. *See L.R. Willson*, 134 F.3d at 1238-39 (rejecting argument that officer conducted a search by viewing plaintiff at workplace from across the street).

iii. Plaintiffs’ failure to engage with pertinent Virginia law is also striking. In rejecting Plaintiffs’ arguments about NPD’s use of ALPRs, the district court aligned itself with the Virginia Court of Appeals, which has *twice* decided that NPD’s use of *its specific system* does not constitute a Fourth Amendment search—and rejected arguments just like Plaintiffs’. *See Robinson v. Commonwealth*, 927 S.E.2d 822

data. JA392. Similarly, although Plaintiffs and amici raise concerns about data-sharing, *see* Br.8; Cato.Br.12-13; EFF.Br.12-19, Virginia law bars most sharing unless a narrow exception applies, *see* Va. Code § 2.2-5517(F); JA388. NPD thus “does *not* share data” with “any private parties, law enforcement agencies outside of Virginia, or federal law enforcement agencies.” JA389.

(Va. Ct. App. 2026); *Commonwealth v. Church*, 2025 WL 2908089 (Va. Ct. App. Oct. 14, 2025). Plaintiffs do not cite or attempt to address either of those decisions.

In both decisions, the Virginia appellate court distinguished *Carpenter* and *Beautiful Struggle* on exactly the grounds discussed above. The court explained that ALPRs are comparatively unintrusive because they take photographs “of vehicles, not persons”; the “only information collected” is “already publicly viewable to anyone who sees the vehicle on the street”; and the data is retained for only a limited period. *Church*, 2025 WL 2908089, at *2-3; *see Robinson*, 927 S.E.2d at 828. In both cases, the court zeroed in on NPD’s specific system, explaining that NPD’s ALPRs provide only “short-term monitoring” and do not “create an ‘intimate window’” into individuals’ “overall movements and associations.” *Church*, 2025 WL 2908089, at *3; *see Robinson*, 927 S.E.2d at 828. In both cases, the court declined to “speculat[e] about hypothetical, potential misuse” of the ALPRs, focusing instead on the “specific facts” before it. *Church*, 2025 WL 2908089, at *4; *see Robinson*, 927 S.E.2d at 828.

Plaintiffs also hardly mention Virginia’s ALPR statute, even though the statute “offers at least some indication that the use of ALPR systems within [the statute’s] parameters promotes public safety without transgressing the public’s reasonable expectation of privacy.” JA46; *see Jackson*, 2025 WL 1530574, at *10 (“legislative process” is “far better equipped to regulate” ALPRs than “blunt

instrument” of judicial decision-making). It is true that *Robinson* and *Church* do not bind this Court and that compliance with Section 2.2-5517 does not “insulate” NPD from “judicial scrutiny.” JA46. But the fact that Virginia’s courts and legislature *both* consider NPD’s conduct reasonable weighs powerfully against a contrary ruling here.

B. Plaintiffs’ Proposed Three-Factor Test Is Forfeited and Meritless

Faced with precedent and a factual record that foreclose their claim, Plaintiffs try to move the goalposts, urging this Court to adopt a three-factor test of their own invention to determine when use of technology contravenes a reasonable expectation of privacy. Br.24-47. That argument is both forfeited and meritless.

1. Plaintiffs never mentioned their three-factor test below. Indeed, they did not mention any “factors” at all. Instead, Plaintiffs proposed the same analysis that the district court applied: whether the technology at issue “enables inferences or deductions from the whole of people’s past movements.” Dkt.108, at 16. Yet now, on appeal, Plaintiffs lead with an argument that “*Carpenter* requires courts to consider several factors,” and they fault the district court for failing to “reach[]” every factor, even though they never asked the district court to do so. Br.24, 30. That argument is forfeited—and “any argument against forfeiture is forfeited too,” as Plaintiffs do not try to show exceptional circumstances sufficient to overcome

forfeiture. *Bloosurf*, 170 F.4th at 272-73; *see id.* (arguments that court “used the wrong test” are forfeited where party never disputed the “which test” question).

2. Plaintiffs were right the first time, because the three-factor test on which they rely does not exist. In arguing otherwise now, Plaintiffs must seriously distort the Supreme Court’s decision in *Carpenter*. Among other things, they elide the most important consideration in deciding whether photographing Plaintiffs’ vehicles on public roads invades a reasonable expectation of privacy: whether the resulting data is “comprehensive.” *Carpenter*, 585 U.S. at 315, 320.

Plaintiffs claim that their three-factor test is found in *Carpenter*, Br.30, 42-44—but *Carpenter* does not set out any multi-factor test. *See, e.g., Martin*, 753 F. Supp. 3d at 471 (rejecting argument that *Carpenter* “adopted a new” multi-factor “balancing test”). It would be surprising if *Carpenter* did so, as the Supreme Court has consistently rejected the use of multi-factor tests in Fourth Amendment cases. *See, e.g., Robinette*, 519 U.S. at 39; *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983) (rejecting “two-pronged test” in favor of “totality-of-the-circumstances analysis” to “better achieve” Fourth Amendment’s goals). *Carpenter* simply considers the particular case-specific circumstances relevant to the Court’s determination that CSLI was comprehensive data that violated the defendant’s “expectation of privacy in the whole of his physical movements,” 585 U.S. at 311-13, without ever

suggesting that—in a different case with different facts—different circumstances could not be relevant to the analysis.

Even assuming that the circumstances discussed in *Carpenter* did amount to “factors” in a test, Plaintiffs misuse *Carpenter* in two ways. First, they ignore the parts of *Carpenter* that they do not find helpful to their position. According to Plaintiffs, *Carpenter* asks whether the technology at issue (a) has “the capacity to enable deductions about intimate habits and patterns”; (b) is “easy, cheap, and efficient”; and (c) “enable[s] police to reconstruct people’s past movements.” Br.30-44. But the Court considered much more—for instance, whether the technology tracks people into non-public places, whether exposure of the relevant information is “voluntary,” and whether the data collected is “comprehensive.” 585 U.S. at 315, 320; *see id.* at 340 (Kennedy, J., dissenting).

Especially striking is Plaintiffs’ complete omission from their test of *Carpenter*’s consideration of the data’s “comprehensiveness.” That consideration was central to the result in *Carpenter*, as it bears closely on whether there has been interference with a reasonable expectation of privacy in the “whole of” a person’s “movements.” 585 U.S. at 311-13. The Court reached a different result in *Carpenter* than it had in *Knotts*, where the Court held that bugging and tracking of a container carried in a car did not violate the Fourth Amendment, precisely because the data in *Carpenter* was so much more comprehensive: an “all-encompassing record” of an

individual's whereabouts over "127 days." *Id.* at 311. Plaintiffs' failure to say anything about comprehensiveness is no doubt explained by the clear non-comprehensiveness of the ALPR data in this case, which is extremely sparse as to any individual vehicle and must almost always be discarded within a few weeks.

Second, even where Plaintiffs do address the considerations mentioned in *Carpenter*, Plaintiffs do not fairly portray those considerations, instead seeking to broaden or narrow them as is most beneficial to Plaintiffs' preferred outcome. The first factor in Plaintiffs' proposed test, which is whether data "enable[s] police to deduce habits and patterns," Br.41, is emblematic of that problem. In Plaintiffs' telling, that factor comes from *Carpenter* and indicates that a search requiring a warrant has occurred. But what *Carpenter* *actually* says is much narrower: that the use of comprehensive data that provides "an intimate window into a person's life" is important in the analysis. *Carpenter*, 585 U.S. at 311. And Plaintiffs' broader view makes no sense as a way to determine whether a search has occurred. All kinds of data enable police to make deductions about habits and patterns—for instance, an officer's glimpse through binoculars of a pedestrian's employee badge, or a photograph taken by a security camera pointed at a public road of a person leaving a roadside church on a Sunday morning. But the law does not require a warrant before the police can gather that data and make those deductions. Rather, as *Carpenter* states, the question is whether comprehensive data enables deductions

from “the whole of [individuals’] physical movements.” *Carpenter*, 585 U.S. at 313; *see* JA49-50.

Plaintiffs’ second purported *Carpenter* factor—whether technology is “easy, cheap, and efficient,” Br.42—is likewise broader than any consideration that drove the decision in *Carpenter* (or in *Beautiful Struggle*). *Carpenter* does note that “cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools.” 585 U.S. at 311. But as explained above, *see* pp.33-34, *supra*, in *Carpenter* the Court declined to “call into question” operation of traditional tools like “security cameras,” *id.* at 316, and this Court in *Beautiful Struggle* declined to cast any doubt on pole or security cameras, 2 F.4th at 345. Similarly, the Supreme Court has held that photographs do not constitute a search just because “human vision is enhanced somewhat,” *Dow*, 476 U.S. at 238, and this Court has rejected the argument that officers’ use of a “resource-efficient surveillance method” alters the “Fourth Amendment analysis,” *Vankesteren*, 553 F.3d at 291; *see also United States v. Gregory*, 128 F.4th 1228, 1235 (11th Cir. 2025) (government may “us[e] technology to conduct lawful investigations more efficiently”). Plaintiffs therefore cannot plausibly argue that *Carpenter*’s one-sentence observation about the efficiency of cell-phone tracking suggests that ease or efficiency has enough force in the Fourth Amendment analysis to overcome the absence of comprehensive data.

In the end, Plaintiffs cannot cite a *single decision* of any court that has adopted their three-factor test. Although Plaintiffs look for support in this Court’s decisions, there is none to be found. The analysis in *Beautiful Struggle* does not resemble Plaintiffs’ test; rather, following *Carpenter*, that decision addresses an array of case-specific considerations bearing on whether the technology at issue “enable[d] deductions from the whole of individuals’ movements” so as to open “an intimate window” into their “associations and activities.” 2 F.4th at 341-46; *see* JA49-50 (discussing *Beautiful Struggle*). And this Court’s one-sentence decision in *United States v. Chatrue*, 136 F.4th 100 (4th Cir. 2025) (en banc), *cert. granted*, 2026 WL 120676 (No. 25-112), does not engage in an analysis like Plaintiffs’ either. Plaintiffs cite a concurrence in *Chatrue* stating that *Carpenter* “laid the foundation for a new, multifactor test.” *Id.* at 119 (Wynn, J., concurring). But that concurrence does not set out the test that Plaintiffs propose, and (like *Carpenter*) it emphasizes the comprehensiveness of the data—a factor that Plaintiffs elide because the data here is so far from comprehensive. *Compare id.* at 120-25 & n.4 (considering “comprehensiveness,” “retrospective quality,” invasiveness, and cost and efficiency), *with* Br.30-44; *see also* 136 F.4th at 148 (Berner, J., concurring) (assessing a different set of factors: “(1) how revealing th[e] data is, and (2) whether the information was, in practical terms, given to the third party voluntarily”).

3. Even if *Carpenter* had set out factors that courts *must* consider, including in a case like this one involving traditional surveillance tools, the relevant factors here would compel the conclusion that NPD’s use of its ALPR system comports with the Fourth Amendment. The same would be true under the factors discussed in the *Chatrie* concurrences, and even under Plaintiffs’ misguided test.

First, the data here is not remotely comprehensive. As explained, Plaintiffs’ vehicles were photographed only sporadically due to the NPD ALPRs’ very limited scope of coverage, and the amount of data that those ALPRs collect is similarly limited—all of which is a far cry from the data in *Carpenter* and *Beautiful Struggle*. See pp.37-41, *supra*. In other words, “it simply cannot be said that the City of Norfolk’s system of Flock cameras amount[s] to ‘near perfect surveillance.’” *Robinson*, 927 S.E.2d at 827-28 (quoting *Carpenter*, 585 U.S. at 312); see *id.* at 828 (explaining that “cameras interspersed along public roads throughout the City of Norfolk are hardly analogous to the 127 days of [CSLI] at issue in *Carpenter*” or the “aerial surveillance of every movement of virtually every resident of Baltimore for twelve hours a day” in *Beautiful Struggle*).

Second, NPD’s system does not reveal intimate details. Again, NPD’s ALPRs photograph cars, not people, and only on public roads. See pp.25-29, *supra*. That photography yields only information that drivers “voluntarily conveyed to anyone who wanted to look.” *Knotts*, 460 U.S. at 281; accord *Robinson*, 927 S.E.2d at 828

(NPD ALPRs “did not create an ‘intimate window’” into defendant’s “overall movements and associations”); *Church*, 2025 WL 2908089, at *3 (same). *Carpenter* and *Beautiful Struggle*, by contrast, both involved data about *non-public* places people went—whether inside buildings, as in *Carpenter*, or in private yards or other private spaces open to the sky, as in *Beautiful Struggle*. See pp.31-32, *supra*. And contrary to Plaintiffs’ assertion, despite being given full access to months and months of NPD ALPR data, Plaintiffs utterly failed to “show[] how Norfolk could use its Flock Cameras to deduce intimate details,” Br.33—as exemplified by the fact that Plaintiffs’ own expert could not use the data to identify places they visited without first being directly told what and where those places were. See pp.39-40, *supra*.

Finally, NPD’s system does not “enable police” to meaningfully “reconstruct people’s past movements.” Br.44. Given the paucity of ALPRs in Norfolk and the statutory 21-day limit on data retention, NPD’s system cannot come close to reconstructing the whole of anyone’s movements. JA35; see *Robinson*, 927 S.E.2d at 828 (holding that NPD’s ALPRs cannot create a “comprehensive chronicle” of individuals’ movements and declining to speculate whether that might change in the future). Plaintiffs’ experts did not show otherwise. See pp.39-40, *supra*. And to the extent that Plaintiffs argue that this factor weighs in their favor solely because ALPR data is “retrospective,” Br.45, that argument likewise proves too much, as security-

camera and pole-camera footage is also retrospective (as well as cheap and efficient), and those long-used tools are constitutionally sound. *See* pp.33-34, *supra*.

IV. Plaintiffs’ “Original Meaning” Argument Is Waived and Meritless

Plaintiffs contend that the Fourth Amendment’s “original meaning” governs here and dictates that *any* investigative activity, including the use of ALPRs, constitutes a search permissible only with a warrant. Br.47-55. This Court should reject that contention for multiple reasons.

First, Plaintiffs have affirmatively waived it. They candidly told the district court that Supreme Court precedent “foreclosed” an original-meaning argument and that there was no “need” to “reach” it, Dkt.108, at 29, and the district court rejected it on that basis, JA51. That renders the argument unreviewable, “even for plain error.” *United States v. Robinson*, 744 F.3d 293, 298 (4th Cir. 2014).

Second, the argument is meritless under decades of binding precedent requiring a privacy-based analysis. *See Carpenter*, 585 U.S. at 343-61 (Thomas, J., dissenting). As that precedent establishes, looking to a reasonable expectation of privacy *reflects* the original public meaning of the Fourth Amendment. *See, e.g., Kyllo*, 533 U.S. at 34 (“assur[ing] preservation” of “privacy against government that existed when the Fourth Amendment was adopted”); *see also* Orin Kerr, *Katz as Originalism*, 71 Duke L.J. 1047 (2022).

Finally, Plaintiffs’ proposed “original meaning” test makes no sense. Plaintiffs claim that “ordinary citizens in the founding generation” would have defined a “search” as “purposeful investigative conduct”—that is, anything police might do to assess whether a crime has occurred and, if so, who committed it. Br.48. Plaintiffs also assert that a search is unreasonable when “a law-abiding person would feel less secure if the government” can “conduct a particular type of search without judicial oversight,”—even though people presumably always feel more secure with judicial oversight in place, and such “feel[ings],” *id.*, are impossible to ascertain. On Plaintiffs’ view, therefore, any investigative act, including simply observing the appearance and demeanor of a police-station visitor, would require a warrant. That is patently untenable. Police officers cannot operate under such constraints, and they did not do so when the Fourth Amendment was adopted. *See Katz*, 389 U.S. at 352-53 (before 1967, only physical trespass could constitute a Fourth Amendment search). And modern officers, who must make quick decisions without the benefit of hindsight, cannot reliably discern whether “[o]rdinary citizens at the Founding” would have “condemned” their conduct. Br.49.

Like Plaintiffs’ other arguments, then, Plaintiffs’ “original meaning” argument is untethered from governing law. Plaintiffs dislike the fact that a camera occasionally photographs their cars driving down public streets, and they seek to parlay that preference into a Fourth Amendment rule that would severely hamper

use of a non-intrusive tool that has allowed police to solve murders, kidnappings, missing-persons cases, human-trafficking offenses, vehicle thefts, and numerous other crimes that harm the public. *See* p.8, *supra*. But Plaintiffs' position would give rise to nonsensical results. It cannot be reconciled with Virginia's statute. And, most importantly, it runs headlong into well-established Fourth Amendment jurisprudence—which is why the Fifth Circuit, the Virginia appellate court, and dozens of other courts across the country have unanimously held that use of ALPRs does not constitute a search. This Court should reach the same conclusion.

CONCLUSION

The judgment should be affirmed.

DATED: June 11, 2026

/s/ Adam D. Melita

Adam D. Melita

Karla J. Soloria

CITY OF NORFOLK

DEPARTMENT OF LAW

810 Union Street

Suite 900

Norfolk, VA 23510

(757) 664-4529

adam.melita@norfolk.gov

karla.soloria@norfolk.gov

Counsel for Defendants-Appellees

Respectfully submitted,

/s/ Elaine J. Goldenberg

Donald B. Verrilli, Jr.

Elaine J. Goldenberg

Daniel J. Kane

MUNGER, TOLLES & OLSON LLP

601 Massachusetts Avenue NW

Suite 500 E

Washington, DC 20001

(202) 220-1100

Donald.Verrilli@mto.com

Elaine.Goldenberg@mto.com

Daniel.Kane@mto.com

Justin P. Raphael

MUNGER, TOLLES & OLSON LLP

560 Mission Street

27th Floor

San Francisco, CA, 94105

(415) 512-4000

Justin.Raphael@mto.com

Counsel for Defendant-Appellee

City of Norfolk

REQUEST FOR ORAL ARGUMENT

Pursuant to Fourth Circuit Rule 34(a), Defendants request oral argument because the legal issues are important and this case is of serious consequence to Defendants. Counsel believe that argument will significantly assist the Court.

DATED: June 11, 2026

MUNGER, TOLLES & OLSON LLP

By: /s/ Elaine J. Goldenberg

Elaine J. Goldenberg
Counsel for Defendant-Appellee
City of Norfolk

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 12,993 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). I further certify that this brief complies with the typeface and type style requirements of Fed. R. App. P. 32(a)(5)-(6) because it has been prepared in proportionally spaced 14-point Times New Roman font using Microsoft Word.

DATED: June 11, 2026

MUNGER, TOLLES & OLSON LLP

By: /s/ Elaine J. Goldenberg

Elaine J. Goldenberg

Counsel for Defendant-Appellee

City of Norfolk

CERTIFICATE OF SERVICE

I hereby certify that on June 11, 2026, I electronically filed the foregoing with the Clerk of the United States Court of Appeals for the Fourth Circuit using the CM/ECF system, which sent notification of such filing to all registered CM/ECF users.

DATED: June 11, 2026

MUNGER, TOLLES & OLSON LLP

By: /s/ Elaine J. Goldenberg

Elaine J. Goldenberg
Counsel for Defendant-Appellee
City of Norfolk

ADDENDUM OF CONSTITUTIONAL AND STATUTORY AUTHORITIES

INDEX TO ADDENDUM

U.S. Const. amend. IV	ADD-1
VA. CODE ANN. § 2.2-5517 (West 2025)	ADD-1
General Order OPR-493: Flock Safety ALPR System	ADD-8

United States Constitution Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Virginia Code § 2.2-5517

Use of automatic license plate recognition systems by law-enforcement agencies

A. For purposes of this section:

“Audit trail” means all records of queries and responses in an automatic license plate recognition system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the (i) date and time of access; (ii) license plate number or other data elements used to query the system; (iii) specific purpose, as set forth in subsection D, for accessing or querying the system, including the offense type for any criminal investigation; (iv) associated call for service or case number; and (v) username of the person or persons who accessed or queried the system.

“Audit trail data” means all forms of data collected or generated by an automatic license plate recognition system for purposes of producing an audit trail.

“Automatic license plate recognition system” or “system” means a system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data.

“Division” means the Division of Purchases and Supply of the Department of General Services.

“Law-enforcement agency” means any agency or entity that employs law-enforcement officers as defined in § 9.1-101.

“Missing or endangered person” means a person who has been identified as missing or endangered based on information provided by the National Criminal Information Center, the National Center for Missing and Exploited Children, or the Missing Children Information Clearinghouse (§ 52-31 et seq.) or pursuant to a Virginia Amber Alert (§ 52-34.1 et seq.), a Virginia Critical Operation for a Disappeared Child Initiative Alert (§ 52-34.3:1 et seq.), a Virginia Senior Alert (§ 52-34.4 et seq.), a Virginia Blue Alert (§ 52-34.7 et seq.), a Virginia Critically Missing Adult Alert (§ 52-34.10 et seq.), a Virginia Missing Person with Autism Alert (§ 52-34.13 et seq.), or any substantially similar alert under the laws of another state or territory of the United States, the District of Columbia, or the United States.

“Notification” means an alert from an automatic license plate recognition system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the automatic license plate recognition system for comparison purposes.

“Person associated with human trafficking” means a person who is either a suspected victim or an alleged perpetrator of either commercial sex trafficking or labor trafficking.

“Publicly post” means to post on a website that is maintained by the agency or on any other website on which the agency generally posts information and that is available to the public or that clearly describes how the public may access such information.

“Query” means a search of automatic license plate recognition system data based on information entered by the user, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the automatic license plate recognition system.

“System data” means all forms of data collected or generated by an automatic license plate recognition system, including images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted.

“Vendor” means a business, company, corporation, or other nongovernmental entity that contracts with a law-enforcement agency for the installation, use, or maintenance of an automatic license plate recognition system.

B. Pursuant to § 2.2-1112, the Division of Purchases and Supply shall determine the automatic license plate recognition systems for use in the Commonwealth in accordance with this section. An automatic license plate recognition system shall not be approved by the Division for use by a law-enforcement agency unless:

1. The vendor certifies that it will not sell or share any system data or audit trail data gathered in the Commonwealth, except upon request of the contracting law-enforcement agency for a purpose set forth in subsection F, and will only access system data or audit trail data upon request of the contracting law-enforcement agency for maintenance and quality assurance purposes;
2. The vendor certifies that its system is capable of purging system data collected or generated in the Commonwealth after 21 days of the date of its capture, or earlier if requested by the contracting law-enforcement agency, in such a manner that the system data is destroyed and not recoverable by either the vendor or the contracting law-enforcement agency;
3. The vendor certifies that its system is capable of producing an audit trail and purging audit trail data collected or generated in the Commonwealth after two years of the date of its capture in such a manner that the audit trail data is destroyed and not recoverable by either the vendor or the contracting law-enforcement agency;

4. The databases used by the system to provide notifications as set forth in subsection D are updated at least every 24 hours, or as soon as practicable after such updates become available; and

5. The system meets information security standards as established by the Virginia Information Technologies Agency.

C. (Effective July 1, 2026) A law-enforcement agency may enter into a contract with a vendor for the installation, use, or maintenance of a system approved by the Division. The contract shall specify that system data and audit trail data will be the property of the law-enforcement agency and that the system meets the requirements set forth in subsection B. The contract shall further specify that the vendor will immediately notify the law-enforcement agency upon receipt of any subpoena duces tecum, execution of any search warrant, or any other request from a third party for such system data or audit trail data, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

D. A law-enforcement agency may use a system only (i) as part of a criminal investigation into an alleged violation of the Code of Virginia or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed; (ii) as part of an active investigation related to a missing or endangered person, including whether to issue an alert for such person, or a person associated with human trafficking; or (iii) to receive notifications related to a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate. All information necessary for the creation of an audit trail shall be entered in order to query system data. A law-enforcement agency shall not query or download system data unless such data is related to at least one of these purposes. A law-enforcement agency may download audit trail data for purposes of generating audit reports. A stop of a motor vehicle based on a notification from the system shall be consistent with subsection M.

E. System data shall be purged after 21 days of the date of its capture in such a manner that such data is destroyed and not recoverable by either the vendor or the law-enforcement agency. Audit trail data shall be purged after two years of the date of its capture in such a manner that such data is destroyed and not recoverable by either the vendor or the law-enforcement agency. However, if the system data or the audit trail data is part of an ongoing investigation, prosecution, or civil action, such data shall be retained by the law-enforcement agency until (i) the investigation concludes without any criminal charges or (ii) the final disposition of any criminal or civil matter related to the data, including any direct appeals and any writs of habeas corpus pursuant to Article 3 (§ 8.01-654 et seq.) of Chapter 25 of Title 8.01 or federal law, in accordance with applicable records retention law and policy.

F. System data and audit trail data shall not be subject to disclosure under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). A law-enforcement agency shall not sell

any system data or audit trail data. A law-enforcement agency shall not share system data or audit trail data with, or disseminate such data to, any database of any other state, federal, private, or commercial entity. A law-enforcement agency may share system data or audit trail data for the following purposes:

1. With another law-enforcement agency for purposes set forth in subsection D, which may include allowing another law-enforcement agency to query system data, provided that the agency receiving such data shall comply with all of the provisions of this section;
2. With the attorney for the Commonwealth for purposes set forth in subsection D or for complying with discovery or a court order in a criminal proceeding;
3. With a defendant or his counsel for purposes of complying with discovery or a court order in a criminal proceeding;
4. Pursuant to a court order or a court-issued subpoena duces tecum in any criminal or civil proceeding;
5. With the vendor for maintenance or quality assurance purposes; or
6. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding warrant.

In addition, the Department of State Police shall share system data obtained from any system installed, maintained, and operated on any limited access highway or any bridge, tunnel, or special structure under the jurisdiction of the Commonwealth Transportation Board or the Department of Transportation with any law-enforcement agency in the locality where such system is installed, maintained, or operated, and such law-enforcement agency may share such system data for the purposes set forth in this subsection.

G. A law-enforcement agency that uses a system shall maintain records sufficient to facilitate public reporting as required by this section, the production of an audit trail, and discovery in criminal and civil proceedings, appeals, and post-conviction proceedings.

H. A law-enforcement agency that uses a system shall establish a policy governing such use that is consistent with this section that includes:

1. Training requirements for individuals who will use or access the system;
2. The purposes for which the system can be used or accessed;
3. Procedures to ensure that the databases used by the system to provide notifications as set forth in subsection D are updated at least every 24 hours, or as soon as practicable after such updates become available;
4. Procedures to confirm the accuracy of any notifications made by the system before stopping a vehicle that are consistent with subsection M;

5. A prohibition against downloading system data that is not related to at least one of the purposes set forth in subsection D, except for downloads of audit trail data for purposes of generating audit reports;
6. An internal auditing procedure that occurs at least once every 30 days;
7. Procedures for the retention and destruction of system data and audit trail data that are consistent with subsection E;
8. A prohibition on the sale of system data and audit trail data and restrictions on the sharing of system data and audit trail data that are consistent with subsection F; and
9. Security procedures to protect the system, system data, and audit trail data from unauthorized access, destruction, use, modification, or disclosure.

I. A law-enforcement agency that uses a system shall report to the Department of State Police by April 1 of each year, in a format to be determined by the Department of State Police, on its use of the system during the preceding calendar year, which shall include the following data:

1. The total number of cameras owned or leased by an agency as part of a system at the conclusion of each calendar year, including the number of such cameras designed to be affixed inside or on a motor vehicle, permanently affixed adjacent to a highway, or temporarily affixed or placed adjacent to a highway for purposes of capturing system data;
2. A list of all state and federal databases with which the system data was compared, unless the existence of any such database itself is not public;
3. The total number of times the system was queried, including the specific purposes of the queries, as set forth in subsection D, and the offense types for any criminal investigation;
4. The race, ethnicity, age, and gender of any individual identified as a suspect and charged with a criminal offense as a result of a query of the system as part of a criminal investigation;
5. The number of motor vehicles stopped based on notifications from the system, including the specific reasons for the notifications as set forth in subsection D;
6. The race, ethnicity, age, and gender of the driver of any motor vehicle stopped based on a notification from the system;
7. Whether the agency allows any other law-enforcement agencies to access its system data, and if so, which other agencies have been granted such access;
8. The number of identified instances of unauthorized use of or access to the system, including the nature and circumstances of such instances; and

9. The number of subpoena duces tecum, search warrants, and any other requests received from a third party for system data or audit trail data, including the identity of the entity that requested the issuance of such subpoena duces tecum, executed such search warrant, or requested such data, and whether any data was provided to such entity, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

J. The Department of State Police shall aggregate the data provided pursuant to subsection I and report it to the Governor, the General Assembly, and the Virginia State Crime Commission by July 1 of each year.

K. A law-enforcement agency that uses a system shall publicly post the policy set forth in subsection H and the report set forth in subsection I. Data shall not be publicly posted if it contains personal or case identifying information. If any data (i) contains an articulable concern for any person's safety, (ii) is otherwise prohibited from public disclosure by federal or state statute, or (iii) may compromise sensitive criminal justice information if disclosed, such data may be excluded from being publicly posted.

L. A law-enforcement agency shall not use a system for the purpose of interfering with individuals engaged in lawful activities or tracking individuals on the basis of the content of lawfully protected speech.

M. A notification by a system for purposes set forth in subsection D does not, by itself, constitute reasonable suspicion as grounds for law enforcement to stop a vehicle. Prior to stopping a vehicle based on a notification, a law-enforcement officer shall:

1. Develop independent reasonable suspicion for the stop; or
2. Confirm that the license plate or identifying characteristics of a vehicle match the information contained in the database used to generate the notification.

N. Any person who willfully and intentionally queries, accesses, or uses a system for a purpose other than set forth in subsection D, or who willfully and intentionally sells, shares, or disseminates system data or audit trail data in violation of subsection F, is guilty of a Class 1 misdemeanor.

O. Any evidence obtained as the result of a violation of subsection D, F, L, or M is not admissible by the Commonwealth in any criminal or civil proceeding, but such evidence may be admitted by a defendant in a criminal proceeding or a litigant, other than the Commonwealth, in a civil proceeding.

P. This section does not apply to systems used:

1. For the enforcement of traffic laws, which includes parking regulations, speed limits, tolling requirements, high-occupancy vehicle requirements, or on-road emissions monitoring;

2. By the Department of Motor Vehicles at permanent weighing stations and in mobile weighing operations; or

3. By any state or local agency or any private entity for non-criminal justice purposes.

Q. A vendor shall immediately notify the contracting law-enforcement agency under subsection C upon receipt of a subpoena duces tecum, execution of a search warrant, or any other request from a third party for any system data or audit trail data, unless disclosure of such subpoena duces tecum, search warrant, or request is otherwise prohibited by law.

R. Prior to or coincident with the implementation of an automatic license plate recognition system, a local law-enforcement agency shall take measures to promote public awareness on the use of such system.



THE CITY OF NORFOLK

POLICE DEPARTMENT

MEMORANDUM

TO: All Commands

FROM: Chief of Police

COPIES TO: _____

SUBJECT: Memo 25-097: General Order OPR-493: Flock Safety ALPR System

DATE: June 30, 2025

Operational General Order 493: Flock Safety ALPR System has now been issued superseding Special Order 23-002: Flock Safety. Personnel will acquaint themselves with the new order (attached). The current issue of the order is located at R:Reference\Orders & Memos\General Orders.

All personnel will log into PowerDMS and electronically sign, acknowledging receipt and understanding of the general order.

Commanding officers are to ensure compliance.

This memo self-cancels when superseded by notification.

A handwritten signature in blue ink, appearing to read "Mark Talbot", with a circled "DA" or similar initials to the right.

Mark Talbot
Chief of Police

MET/ps/ats
(Attachment)

The information contained is restricted for official Departmental use only. Any further disclosure outside of the Norfolk Police Department is strictly prohibited.

 THE CITY OF NORFOLK POLICE DEPARTMENT		Operational General Order - 493: Flock Safety ALPR System	
		Office of Preparation: Personnel and Accreditation Division CALEA: none	
LEGAL REVIEW DATE:	6/30/2025 12:22 PM EDT	RECORDED DATE:	6/30/2025 9:41 AM PDT
City Attorney:	Signed by: <i>Karla Soloris</i> 2839D1E644DB432	City Manager/Director of Public Safety:	DocuSigned by: <i>Pat O'Rourke</i> E88E1B3EDF5842D...
APPROVED BY THE AUTHORITY OF THE CHIEF OF POLICE:		<i>Mark Talbot</i> 34D2533294444E8...	

Purpose:

The purpose of this general order is to provide Norfolk Police Department personnel with requirements, guidelines, and principles for the use, response, collection, access, dissemination, retention and purging of Flock Safety data to ensure that information is used for legitimate law enforcement purposes only and in accordance with applicable law.

Policy:

It is the policy of the Norfolk Police Department to further support law enforcement capabilities by utilizing the latest technologies for crime prevention and apprehension of criminal suspects. Flock Safety utilizes Automatic License Plate Readers (ALPRs) to scan, detect and identify license plate numbers and vehicle characteristics. Officers will receive the appropriate training before being authorized to use these devices for law enforcement purposes. The Flock Safety ALPR system and the ALPR cameras associated with the system will be used and maintained by manufacturer recommendations and this policy.

Order Contents:

- I. Definitions
- II. Responsibilities
- III. Permitted Uses and System Access
- IV. Procedures
- V. Training
- VI. Restrictions on the Sale and Sharing of Data
- VII. Security Procedures
- VIII. Record Keeping and Reporting
- IX. Maintenance
- X. Violations

Related Documents:

1. OPR-492: LPR Systems
2. OPR-710: Operation of Police Vehicles
3. ADM-510: In Car Video System
4. PD 643 - Request to Enter a Flock Custom Hotlist

Supersedes:

1. S.O. 23-002: Flock Safety, dated July 25, 2023

I. Definitions

- A. Audit trail: all records of queries and responses in the Flock Safety ALPR system, and all records of actions in which system data is accessed, entered, updated, shared, or disseminated, including the following:
1. Date and time of access.
 2. License plate number or other data elements used to query the system.
 3. Specific purpose for accessing or querying the system, including the offense type for any criminal investigation.
 4. Associated call for service or case number.
 5. Username of the person or persons who accessed or queried the system.
- B. Audit trail data: all forms of data collected or generated by the Flock Safety ALPR system for purposes of producing an audit trail.
- C. Automatic License Plate Recognition (ALPR) System: a system of one or more high-speed cameras used in combination with computer algorithms to convert images of license plates, vehicles, or a combination of both into computer-readable data.
- D. Custom hotlist: a hotlist manually created by NPD personnel.
- E. Flock Safety: an ALPR system vendor that contracts with NPD.
- F. Hotlist: A list of license plates and vehicles entered into the National Crime Information Center (NCIC) database, the Virginia Crime Information Network (VCIN) database, and any other database utilized by the Flock Safety ALPR system for comparison purposes.
- G. Notification: an alert from the Flock Safety ALPR system that a license plate or vehicle matches a license plate or vehicle in a database utilized by the Flock ALPR system for comparison purposes.
- H. Query: a search of the Flock Safety ALPR system data based on information entered by NPD personnel, including a full or partial license plate number, any identifying characteristics of a vehicle, the date, time, or location of an image, or any other data that is searchable within the Flock Safety ALPR system.
- I. System data: all forms of data collected or generated by the Flock Safety ALPR system including images of license plates, vehicles, any identifying characteristics of vehicles, the date, time, and location of an image, and any peripheral images collected from which analytical data may be extracted.

II. Responsibilities

- A. Authority to approve the use of the Flock Safety ALPR system will be vested in the Chief of Police or their designee.
- B. Supervisors in the Real Time Crime Center (RTCC) will act as the point of contact and liaison with Flock Safety. Their responsibilities include, but are not limited to the following:
 - 1. Ensuring that the Flock Safety ALPR system has been approved by the state Division of Purchases and Supply of the Department of General Services.
 - 2. Overseeing the installation, implementation, and maintenance of Flock Safety ALPR system equipment.
 - 3. Ensuring the Standard Operating Procedures (SOP), Operational General Order, and any necessary forms are developed based on the manufacture's recommendations, VCIN/NCIC regulations and appropriate legal mandates.
 - 4. Overseeing the development and timely administration of training for ensuring proficiency of Flock Safety ALPR users. This will include but is not limited to the following:
 - a. Ensuring that proficiency training is received by each user.
 - b. Documenting and forwarding training records to the Training Division.
 - c. Reviewing and revising all applicable training criteria on an as needed basis.
 - 5. Completing monthly audits of active custom hotlists to ensure that there is a corresponding PD 643 for each entry.
 - 6. Collecting and maintaining records to facilitate and satisfy the public reporting and audit trail requirements of the Flock Safety ALPR System usage and related actions. These reports must be submitted annually beginning April 1, 2027.
 - 7. Reviewing the policies and procedures in this General Order and making recommendations for any amendments.
 - 8. Designating Flock Safety ALPR system administrators.
- C. The Training Division will approve all recommended training and maintain all training records.
- D. NPD Supervisors will ensure that personnel under their direct command who use the Flock Safety ALPR System will follow the established guidelines and procedures.

- E. NPD Flock Safety ALPR system administrators will be responsible for adding personnel as system users, reviewing data sharing requests with other jurisdictions for acceptance or approval, and conducting an audit of the Flock Safety ALPR system every thirty (30) days.

III. Permitted Uses and System Access

A. Permitted Purposes

1. The Flock Safety ALPR system, including downloads, queries, and hotlists, may be used only in the following circumstances per Virginia law:
 - a. As part of a criminal investigation into an alleged violation of the Code of Virginia or any ordinance of any county, city, or town where there is reasonable suspicion that a crime was committed.
 - b. As part of an active investigation related to a missing or endangered person or a person associated with human trafficking.
 - c. To receive notifications related to a missing or endangered person, a person with an outstanding warrant, a person associated with human trafficking, a stolen vehicle, or a stolen license plate.
2. The Flock Safety ALPR system may be used for official and legitimate use only in connection with the law enforcement purposes set forth in this General Order and applicable law.
3. The Flock Safety ALPR system will not be used to interfere with individuals engaging in lawful activities or tracking individuals on the basis of the content of lawfully protected speech.

- B. NPD Flock Safety ALPR system cameras will be positioned to capture only vehicles that are exposed to public view (e.g., vehicles on a public roadway or a place that is publicly accessible, such as public parking lots).

C. System Access

1. Officers are required to sign into the Flock Safety ALPR system at the beginning of each shift, such that the technology is available for use throughout their shift based on operational needs. The Flock Safety ALPR system can be minimized or otherwise remain in the background.
2. NPD personnel will ensure that they are logged into the Flock Safety ALPR system under the username assigned to them.
3. NPD personnel will not share their ALPR system credentials with others.

4. NPD personnel will only utilize city issued equipment to access the ALPR system.
5. NPD personnel will not allow any unauthorized individual to access the ALPR system.

D. Queries

1. Queries may be used only in connection with a permitted purpose listed under section III(A). A query made in connection with a crime also requires reasonable suspicion.
2. The user must enter the following information in the corresponding data fields of the Flock Safety ALPR system to initiate a query:
 - a. Parameters (e.g., license plate, vehicle characteristics, time, and/or location).
 - b. Case number or call for service number.
 - c. Offense type and reasonable suspicion. Examples:
 - (1) Retail theft – vehicle observed fleeing the scene
 - (2) Stolen vehicle – victim reported vehicle stolen
 - (3) Missing or endangered person – reported by family
3. Through the Flock Safety ALPR system, audit logs will record the user who made the query, the parameters of the query, the date and time of the query, the offense type, and a concise basis for reasonable suspicion.

E. Custom Hotlists

1. A license plate or vehicle added to a custom hotlist must be in connection with a permitted purpose listed under section III(A). A license plate or vehicle added in connection with a crime requires reasonable suspicion.
2. Prior to creating a custom hotlist, the investigator must obtain approval from a Detective Division supervisor by submitting a PD 643. Signed PD 643 forms will be forwarded to the Sergeant assigned to the RTCC.
3. The offense type and supporting reasonable suspicion must be described in the “Justification for Entry” section on PD 643.
4. Examples where the manual entry of a license plate into a custom hotlist is permitted include, but are not limited to the following:

- a. Be On Look Out (BOLO) for a vehicle as part of a criminal investigation supported by reasonable suspicion
 - b. Stolen vehicle or license plate
 - c. AMBER/SILVER alert
 - d. Child abduction
 - e. Wanted person with an outstanding warrant
 - f. Missing or endangered person
5. NPD personnel who create a custom hotlist are responsible for setting the expiration date of the custom hotlist to no longer than 21 days from creation. If after 21 days, it remains necessary to extend the expiration date of the custom hotlist, personnel must complete a new PD 643. The extension will not exceed an additional 21 days. At the conclusion of the extension, the custom hotlist will automatically be purged from the Flock Safety ALPR System.

IV. Procedures

A. Traffic Stops and Other Field Protocols

- 1. A traffic stop based on a notification from the Flock Safety ALPR system must be based on one of the permitted purposes listed in Section III(A).
- 2. **A notification from the Flock Safety ALPR System cannot be used as the sole reason for a traffic stop. Upon receipt of a notification personnel must take the following actions before commencing a traffic stop:**
 - a. Develop independent reasonable suspicion; or personnel must ensure that the notification was accurate by visually confirming that the vehicle's license plate numbers, letters, and issuing state and any other identifying characteristics match the information in the Flock Safety ALPR system.
 - b. For notifications based on VCIN/NCIC, personnel must also verify that the information received through VCIN/NCIC is accurate and current. The personnel will conduct the verification request by contacting the Emergency 911 Division (E911D) telecommunicator via radio. This process serves two purposes:
 - (1) Allows for a thorough notification verification check through the E911D; and

- (2) Initiates a Computer Aided Dispatch (CAD) documentation process and notifies the E911D of the potential request for assistance by other nearby units.
- c. After visually verifying that the information received matches the vehicle in question and verifying the notification through E911D, NPD personnel will take appropriate action after considering all variables and adhering to current NPD policies and procedures.
3. The following information must be recorded in On Call Records about each traffic stop made as a result of a notification:
 - a. Any stop made as a result of a notification and the reason for the notification in keeping with Section III(A).
 - b. The race, ethnicity, age, and gender of the driver of the vehicle stopped based on the notification.

B. Data Downloads

1. Personnel will not download system data unless such data is related to at least one of the purposes described in Section III(A).
2. If personnel download system data as part of an investigation, it will be stored in accordance with applicable evidentiary records law and policy.
3. Personnel may download audit trail data for purposes of generating audit reports.

C. Internal Audits

1. All Flock Safety ALPR records documenting the use of an ALPR, or access to or use of ALPR data, will be subject to review and audit by the Flock Safety ALPR system administrators. The purposes of these audits include to ensure compliance with the terms of this General Order and Virginia law.
2. The Flock Safety ALPR system administrators must conduct an audit of the ALPR system at least every thirty (30) days.
3. Audits will include a review of audit logs to ensure that queries are conducted for permitted purposes and that each user has input all required information.
4. The RTCC will complete monthly audits of custom hotlists to ensure that there is a corresponding PD 643 for each entry.

D. Data Retention and Destruction

1. The Flock Safety ALPR system will purge system data after twenty-one (21) days measured from the date of its capture.
2. The Flock Safety ALPR system will purge audit trail data after two (2) years measured from the date of its capture.
3. If the system data or the audit trail data is part of an ongoing investigation, prosecution, or civil action, such data will be retained by the law-enforcement agency until the following occurs.
 - a. The investigation concludes without any criminal charges, or
 - b. The final disposition of any criminal or civil matter related to the data.
4. System data and audit trail data are not subject to disclosure under the Virginia Freedom of Information Act (FOIA).

V. Training

- A. All NPD personnel must complete standardized training prior to gaining access and using the Flock Safety ALPR system. NPD personnel who have access to the Flock Safety ALPR system as of the date of the implementation of this order and who have not yet completed standardized training will be required to complete that training within sixty (60) days of the issuance of this order to maintain their access to the Flock Safety ALPR system.
- B. Standardized training will include the following:
 1. Completion of a video orientation course provided by Flock Safety relating to the proper operation and use of the Flock Safety ALPR system.
 2. An ALPR system certification course offered by Flock Safety.
 3. Training on the following topics administered and tracked through PowerDMS:
 - a. Review of the Virginia ALPR law and this General Order.
 - b. Setup and maintenance procedures.
 - c. Proper use guidelines.
 - d. Recordkeeping and audit trail requirements.
 - e. Query and hotlist functions and other forms of information entry and deletion.

- f. Training on any other subject deemed necessary and established by the Chief of Police or their designee.
- C. A user's completion of training will be recorded and stored by the RTCC and submitted to the Training Division.
- D. Additional training may be required based on manufacturer recommendations, recommendations by the RTCC, and as needed in response to changes in the Flock Safety system, policy, or law.

VI. Restrictions on Sharing System Data

- A. System data may be shared only in the following circumstances:
 - 1. With other Virginia law enforcement agencies for the purposes described above in section III(A).
 - 2. With a Commonwealth Attorney for the purposes described above in section III(A) or to comply with discovery obligations or a court order in a criminal proceeding.
 - 3. With a defendant or his counsel for purposes of complying with discovery or a court order in a criminal proceeding.
 - 4. Pursuant to a court order or a court-issued subpoena duces tecum in any criminal or civil proceeding.
 - 5. With an ALPR system vendor for maintenance or quality assurance purposes.
 - 6. To alert the public to an emergency situation, a missing or endangered person, a person associated with human trafficking, or a person with an outstanding warrant.
- B. Neither system data nor audit trail data will be sold.

VII. System Data Security

- A. System data will be encrypted in transit and at rest.
- B. All data collection points will be equipped with secure communication protocols to protect data in transit from interception and tampering.
- C. Access to system data will be restricted to authorized personnel.
- D. All data will be encrypted using industry-standard algorithms before being transmitted to servers.
- E. Flock Safety will be certified by the FBI's Criminal Justice Information Services (CJIS) and compliant with NDAA, SOC2 (Type II), SOC3, ISO 27001, Higher

Education Community Vendor Assessment Tool (HECVAT), HIPAA, and FERPA.

- F. Criminal Justice Information Services (CJIS) data must be securely stored.

VIII. Recordkeeping and Reporting

- A. RTCC is responsible for ensuring collection of all data needed to satisfy reporting requirements and compiling the annual report to the Virginia State Police required by Virginia law.
- B. The following information must be recorded and reported annually:
1. Total number of cameras that are part of the ALPR systems used by the NPD, broken down by the following categories:
 - a. Vehicle cameras
 - b. Permanent cameras adjacent to a highway
 - c. Temporary cameras adjacent to a highway
 2. The list of state and federal databases used (e.g. NCIC).
 3. The total times the ALPR system was queried including purposes and offense types.
 4. The race, ethnicity, age, and gender of any individual identified as suspect and charged as a result of a query.
 5. The number of vehicles stopped based on a notification.
 6. The race, ethnicity, age, and gender of the drivers of vehicles stopped based on a notification.
 7. Whether data is shared with other agencies and, if so, which agencies.
 8. The number of instances of unauthorized use and the nature and circumstances of the unauthorized use.
 9. The number of subpoenas, search warrants, and other third party requests for ALPR system data or audit trail data, the identities of the requestors, and whether data was provided unless this disclosure is prohibited by law.
- C. NPD will publicly post this General Order and the annual reports compiled pursuant to this General Order.

IX. Maintenance

- A. The RTCC will be responsible for overseeing the installation, implementation, and maintenance of Flock Safety ALPR equipment.

- B. Flock Safety equipment will not be manipulated by anyone except a technician authorized by Flock Safety. The RTCC supervisors will be responsible for the notification and coordination with Flock Safety when Flock Safety equipment requires attention.
- C. Any damage, manipulation, or hindering of Flock Safety equipment observed by an officer will be immediately reported to a supervisor who will notify the RTCC.
- D. Flock Safety will maintain the operability of each camera and is responsible for repairing damaged or malfunctioning cameras. Flock Safety maintains all records of repairs and maintenance.

X. Violations

- A. If any NPD personnel fail to comply with or adequately enforce the terms of this General Order, their authority to access or use the Flock Safety ALPR system may be temporarily suspended or permanently revoked. Supervisors in the RTCC may take such other action necessary to ensure compliance, including referring such personnel for disciplinary measures permitted under NPD policy.