IN THE

COURT OF APPEALS OF VIRGINIA

RECORD NO. 0737-25-1

COMMONWEALTH OF VIRGINIA

Appellant,

VS.

RONNIE D. CHURCH

Appellee.

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA IN SUPPORT OF APPELLEE

Matthew W. Callahan, VSB # 99823
ACLU Foundation of Virginia
PO Box 26464
Richmond, VA 23261-6464
Telephone: (804) 523-2146
Facsimile: (804) 649-2733
Email: mcallahan@acluva.org

Jennifer Lynch, *pro hac vice* pending
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: jlynch@eff.org

Sidney W. Thaxter, *pro hac vice* pending
Elizabeth Franklin-Best, *pro hac vice* pending
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, DC 20036
Telephone: (202)465-7654
Facsimile: (202)872-8690
Email: sthaxter@nacdl.org
Email: elizabeth@franklinbestlaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported digital civil liberties organization. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States, including in Virginia. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as *amicus* in the U.S. Supreme Court and many others in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1100–01 (2020); *Neal v. Fairfax Cnty. Police Dep't*, 812 S.E.2d 444 (2018).

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous *amicus* briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. NACDL has a particular interest in cases that involve surveillance technologies and programs that

pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the U.S. Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), and as *amicus* in *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The American Civil Liberties Union of Virginia ("ACLU-VA") is the Virginia state affiliate of the national ACLU. ACLU-VA has appeared frequently before this Court and other Virginia courts, advocating for the rights to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, section 10 of the Virginia Constitution.

STATEMENT OF THE CASE

Amici concur with the Statement of the Case set forth in the Brief of the Appellee.

STATEMENT OF FACTS

Amici concur with the Statement of Facts set forth in the Brief of the Appellee.

STANDARD OF REVIEW

Amici concur with the Standard of Review set forth in the Brief of the Appellee.

ASSIGNMENTS OF ERROR

Amici concur with the Assignments of Error set forth in the Brief of the Appellee.

INTRODUCTION AND SUMMARY OF ARGUMENT

As with cell phones, cars have long been "such a pervasive and insistent part of daily life" that for many individuals, owning and driving one "is indispensable to participation in modern society." *Carpenter v. United States*, 585 U.S. 296, 298 (2018) (cleaned up); *see United States v. Jones*, 565 U.S. 400 (2012) (holding long-term tracking of vehicle unconstitutional under the Fourth Amendment, with five concurring Justices endorsing the reasoning ultimately adopted by the majority in *Carpenter*). Our vehicles take us to sensitive and private places like our homes, doctors' offices, and places of worship. And yet, for many years now, with little to no oversight, law enforcement agencies and private companies have been quietly scanning and recording the locations of vast numbers of vehicles across the country, amassing databases of billions of location points reflecting the locations and movements of ordinary people.

This "Automated License Plate Reader" ("ALPR") data is collected on every vehicle, regardless of whether individual drivers are suspected of criminal activity. ALPR data includes not just the plate number but also a photograph of the vehicle, its make, model, color, distinctive features, and detailed location, time, and date information that can later place the vehicle to within feet of the original scan. This data is stored in massive databases that are accessible to federal, state, and local law enforcement agencies, even where, as in this case, those agencies do not collect their

own data or maintain their own databases. And this data is retained according to *ad hoc* arrangements between law enforcement agencies and ALPR system vendors.

Private entities have collected ALPR data for years, but recent versions of these systems—supercharged with video capabilities and artificial intelligence, constantly powered through solar cells, abundantly financed with venture capital, and aggressively marketed to local police as a nationally networked surveillance tool—have made these systems an entirely different ballgame. Today, ALPR data can be used not just to identify and locate a particular vehicle, but in the case of Flock—a private company that maintains the ALPR system queried by police in this case—to identify that vehicle's owner, driver, and who they associate with, as well as phone numbers, criminal records, and even a vehicle's bumper stickers or state of disrepair. And because ALPR data is stored for months or years, ALPR databases allow for retrospective searches that enable law enforcement to infer driving patterns, associations, and sensitive details about drivers' lives. At bottom, searches of ALPR databases seriously threaten to undermine the "degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 585 U.S. at 305 (cleaned up), because they give police a capability unimaginable in the past—the ability to enter a virtual time machine and view suspects' past movements (and much more) "with just the click of a button," *id.* at 311. The Fourth Amendment's warrant requirement exists to prevent this capability from feeding

"too permeating police surveillance." *Id*. at 305 (cleaned up). And because the government uses these ALPR capabilities without warrants, and has not shown that exigent circumstances justify the warrantless search of the ALPR database that occurred here, the plate scan and all evidence collected as a result should be suppressed.

ARGUMENT

I. ALPR Systems are Nearly Ubiquitous and Collect Vast Amounts of Detailed Data.

A. ALPRs Automatically and Indiscriminately Collect Vehicle Location Data.

By design, ALPR collection is indiscriminate. ALPR cameras automatically scan the license plate of every vehicle that comes into view, and they do so "24/7 with coverage that never sleeps."[1] ALPR cameras now blanket most larger towns, and as the Norfolk police chief has stated in describing Norfolk's ALPR network, "it would be difficult to drive anywhere of any distance without running into a camera."[2]

ALPR systems consist of cameras that scan plates, software that processes images and extracts and analyzes data, and searchable databases that store the data

[1] Flock Safety, https://perma.cc/NE2R-DV5C.

[2] Cianna Morales, *Norfolk, Va.'s Flock Cameras Spark Privacy Debate*, Government Technology (June 20, 2023), https://perma.cc/2ENS-NFDK.

once it is collected. ALPR cameras may be mounted on fixed points, squad cars, or movable trailers that can be placed temporarily and covertly at locations of interest.[3] In 2023, Norfolk installed 172 cameras around the city, although many more cameras have been identified in the vicinity.[4] The police department will not reveal where it has placed the cameras, but a nationwide effort by private citizens has identified many of the cameras' locations.[5] Camera distribution across the city has been uneven; police have placed more cameras in neighborhoods that have had more police attention in the past (traditionally poorer areas) than in areas with less (traditionally wealthier areas).[6]

ALPRs detect when a license plate enters the camera's field, capture a photograph or video of the car (including the plate) and its surroundings, and use Optical Character Recognition ("OCR") to capture the plate's alphanumeric data—

[3] Major Cities Chiefs Association, *Automated License Plate Reader Technology in Law Enforcement: Recommendations and Considerations* 1 (Feb. 2023), https://perma.cc/W3RT-EN32.

[4] *Flock Safety Cameras*, City of Norfolk, https://perma.cc/9XFN-RZXS (go to subheading Cameras, under Resources, under Police under Departments); *Norfolk*, DeFlock, https://perma.cc/6ATW-RVHU.

[5] Deflock, *supra* note 4.

[6] Morales, *supra* note 2.

in effect "reading" the plate.[7] ALPRs record data on every plate they scan, including the precise time, date, and place it was encountered, and upload this information, along with the captured photo or video, to a database in the cloud, making it accessible to law enforcement almost immediately after the scan. *United States v. Martin*, 753 F. Supp. 3d 454, 457 (E.D. Va. 2024).

ALPR systems record detailed geolocation data for each plate scanned, including not just the location of the ALPR camera itself, but the direction and specific lane in which the car was traveling. *See Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1095 (2020) (describing ALPR systems). Because the camera's exact position is known, the vehicle can be geolocated to within feet of its actual location.

Newer ALPR systems, like the Flock system in use in Norfolk, also use artificial intelligence to collect even greater detail about vehicles. Flock's system creates a "vehicle fingerprint"[8] that recognizes vehicle features and can allow law enforcement to search for vehicles based on paint color, type of vehicle, bumper stickers, and even highly specific details such as "blue SUV with a racing stripe" or

[7] Major Cities Chiefs Association, *supra* note 3, 1–2; *see also United States v. Martin*, 753 F. Supp. 3d 454, 458 (E.D. Va. 2024) (noting that some Flock cameras also have video and audio capabilities).

[8] Flock Safety, *Evidence at Scale: 6 Benefits of LPR For Law Enforcement*, Flock Safety Blog (Nov. 21, 2023), https://perma.cc/FH4M-ZQ9W.

"white F-150 with a ladder in the back."[9] Flock is also working on a new product that will supplement its ALPR data with aggregated data from "people lookup tools, data brokers, and data breaches to 'jump from LPR [license plate reader] to person.'"[10]

ALPR systems scan license plates regardless of any association with criminal activity. In a 2018 nationwide survey of 173 law enforcement agencies, EFF and MuckRock discovered that an average of 99.5% of the ALPR scans belonged to cars that were *not* associated with any crime.[11] City-collected data in Austin, Texas, in 2025 similarly showed only 0.2% of scans contributed to arrests.[12]

B. ALPRs Collect a Significant Amount of Data.

The vast majority of midsize and large law enforcement agencies use ALPR systems. In a 2020 survey, the federal Bureau of Justice Statistics found that 100% of police departments in cities with 1 million or more people, as well as more than

---

[9] Police1, *Flock Safety launches new AI-powered tools to accelerate police investigations*, Police1 (Feb. 19, 2025), https://perma.cc/7U5J-Q2KU.

[10] Joseph Cox, *License Plate Reader Company Flock Is Building a Massive People Lookup Tool, Leak Shows*, 404Media (May 14, 2025), https://perma.cc/7M27-HRQQ; Flock Safety, *Flock Nova™: Smarter Investigations, Faster Case Resolutions*, Flock Safety Blog (Feb. 13, 2023), https://perma.cc/H4SD-JS8X.

[11] Tanvi Misra, *Who's Tracking Your License Plate?*, Bloomberg Citylab (Dec. 6, 2018), https://perma.cc/6CLU-BLQF.

[12] Abigail Velez, *Flock CEO Responds to Austin Backlash as City Contract Nears Expiration*, CBS Austin (June 20, 2025), https://perma.cc/38XR-T7Q5.

three-quarters of departments serving 100,000 or more residents, used ALPR systems.[13] A 2024 survey conducted by the Virginia Department of Criminal Justice Services found that, of the 275 Virginia law enforcement agencies that responded to the survey, 82% of large departments and 74% of medium departments had ALPR systems.[14]

By scanning every license plate that comes into view—for some systems, nearly 2,000 plates per minute[15]—ALPRs collect an enormous volume of detailed data. One ALPR vendor claims its systems scan more than 500 million plates each month.[16] While Norfolk has not revealed how many plate scans it collects, other cities have. In Los Angeles, California, the Police and Sheriff's Departments together collect data on 3 million cars every week,[17] and Atlanta, Georgia, processes

---

[13] Sean E. Goodison & Connor Brooks, Bureau of Jus. Stat., U.S. Dep't of Just., NCJ 307405, *Local Police Departments, Procedures, Policies, and Technology, 2020 – Statistical Tables* 22 (Nov. 2023), https://perma.cc/XH47-QXMT.

[14] Va. State Crime Comm'n, *2024 Annual Report* 9 (June 2025), https://perma.cc/Q97B-MXR3 ("2024 annual report") (citations omitted).

[15] Angel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Center (Sep. 10, 2020), https://perma.cc/659B-SVAW.f

[16] DRN Data, https://perma.cc/YTK5-9HHX.

[17] See Jennifer Lynch & Peter Bibring, *Secrecy Trumps Public Debate in New Ruling on LA's License Plate Readers*, EFF (Sep. 3, 2014), https://perma.cc/LN3Z-RRJB; Aaron Mendelson, *California Police Scanned More Than 1 Billion License*

nearly 30 million plates each month using just 347 ALPR cameras.[18] Even smaller cities and police departments with only a few cameras can collect over 150,000 plate scans per month.[19]

C. Police Have Real-Time Access to ALPR Data and Few Restrictions on Use.

Once an ALPR system scans a license plate, it and associated data almost immediately become available to the police who subscribe. All Norfolk police officers have real-time or near-real-time access to the data captured by Flock cameras, and police are able to log into Flock's system at any time from any computer or cell phone. *See* (R. 111, 116). Police use ALPR data in two main ways. They can create or subscribe to a "hot list" of license plates associated with vehicles believed to be connected to criminal activity or missing or wanted individuals.[20] These hotlists may be generated by the officer, by the department, or even by outside agencies such as FBI or NCIC. Once an officer creates or subscribes to a hotlist, the ALPR systems will then compare every future scan of a license plate against this list

---

Plates—Rarely Finding Cars on 'Hot Lists', LAist (Nov. 16, 2018), https://perma.cc/9R5L-YGR9.

[18] Josh Wade & Aaron Diamant, *Eyes on the Road*, Atl. Journal-Constitution (Nov. 8, 2018), https://perma.cc/NBX7-RTLR.

[19] *Id.* (noting that Gwinnett County police logged 152,734 plates in one month using only 8 cameras).

[20] *2024 Annual Report*, *supra* note 14 at 10.

and immediately alert the officer when that plate is read.[21]

Police can also, as in this case, access databases of any license plate scanned by an ALPR camera in order to identify the locations and movements of particular vehicles.[22] These databases may be maintained by government agencies, but may also be maintained by homeowners associations, apartment complexes, business districts, schools, *Martin*, 753 F. Supp. 3d at 458, national chain stores,[23] and malls across the country.[24] "So long as customers give their consent, other customers can access this data from Flock cameras in different jurisdictions or across the country." *Id*. Depending on how long the agency or private entity stores plate data, historical searches could access data dating back years.[25]

At the time Sergeant Myers searched for Mr. Church's plate in the Norfolk

---

[21] *Id.*

[22] *Id.* at 11.

[23] Jason Koebler, *Home Depot and Lowe's Share Data from Hundreds of AI Cameras with Cops*, 404Media (Aug. 6, 2025), https://perma.cc/2FSY-LXYC.

[24] Thomas Brewster, *America's Biggest Mall Owner is Sharing AI Surveillance Feeds Directly with Cops*, Forbes (May 6, 2024), https://perma.cc/9H3S-BNG5.

[25] *See 2024 Annual Report*, *supra* note 14 at 16 (Table 1 showing state retention periods ranging from three minutes to five years). Virginia has now limited ALPR data retention to 21 days, *see* Va. Code § 2.2-5517(E), but this limit applies only to Virginia law enforcement and its vendors. There is little to prevent Virginia officers from accessing ALPR data collected by agencies in other states, such as West Virginia or Kentucky, with no retention limits.

Police ALPR database, Virginia did not place any restrictions on how police could use ALPRs; "therefore, law enforcement could collect and search ALPR data for any purpose, keep data for an indefinite time period, and share data without any restrictions."[26] In Norfolk, police undergo minimal training about ALPR systems and have been subject to little oversight. *See* (R. 120) (noting one hour of training). Sergeant Myers testified that his agency required him to enter a justification for any search of the ALPR database, but he acknowledged he did not know if there was oversight to ensure he entered a justification related to his investigation as opposed to his lunch order. (R. 121).[27] And in this case, Sergeant Myers did not search ALPR data to place a suspect at the scene of a crime or even to prove any element of any charge but rather merely to try to establish if he had a "guilty mind." (R. 126–128).

D. Police Share ALPR Data With Little Oversight.

ALPR data can be shared among local, state, and federal agencies, as well private companies, through regional, state-wide, and national databases. Vendors like Flock that maintain ALPR data for both their law enforcement and private

[26] *2024 Annual Report*, *supra* note 14 at 14. Some local Virginia agencies adopted their own policies, though the Commission found these retention periods ranged from agency to agency. *Id.* at 15.

[27] Virginia's new ALPR law, enacted after Sgt. Myers conducted his search, now limits the use of ALPR systems to criminal investigations and searches for missing persons and requires audit trails. *See* VA HB2724; Va. Code § 2.2-5517.

customers facilitate this data sharing. As one Norfolk police lieutenant has noted, "[e]very jurisdiction that has Flock is able to share data with other jurisdictions and also see data that's being shared with them."[28] As recent reporting has revealed, this allows officers to search more than 6,800 different camera networks across the country, together maintaining data from more than 83,000 ALPR cameras.[29] Virginia's new ALPR law allows data sharing with outside agencies, including "allowing another law-enforcement agency to query system data, provided that the agency receiving such data shall comply with all of the provisions" of the law. Va. Code § 2.2-5517 (F)(1).

Even if agencies do not have their own ALPR systems or direct access to data, individual officers can get access through a "side-door."[30] For example, although Immigration and Customs Enforcement ("ICE") does not have a contract with Flock, a trove of Flock data obtained by researchers revealed thousands of "nation and statewide lookups by local and state police done either at the behest of the federal government or as an 'informal' favor to federal law enforcement, or with a potential

---

[28]Morales, *supra* note 2.

[29] Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman who got an Abortion*, 404Media (May 29, 2025), https://perma.cc/NRN6-HWTR.

[30] Joseph Cox & Jason Koebler, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404Media (May 27, 2025), https://perma.cc/C26L-SQYC.

immigration focus."[31] And, days before this brief was filed, it was revealed that Flock had permitted U.S. Customs and Border Protection ("CBP") to regularly search over 80,000 cameras through an undisclosed "pilot" program, including those of police departments that were unaware that information was being shared with CBP.[32] Similarly, although Illinois state law prohibits the sharing of ALPR data for purposes of enforcing federal immigration law or for enforcing other states' bans on abortion, Flock has shared Illinois ALPR data with both a Texas law enforcement agency searching for a woman they suspected had self-administered an abortion in violation of Texas law and with CBP for an undisclosed purpose.[33]

E. ALPR Location Data Can Reveal Detailed Private and Personal Details About Individuals.

Even a small amount of ALPR data can reveal a person's identity as well as sensitive information about that person. By storing data for long periods of time, ALPR databases allow officers to query months' or years' worth of information about a car's past locations. And the more cameras there are in a given area, the more

---

[31] *Id*.

[32] Jason Koebler, *CBP Had Access to More than 80,000 Flock AI Cameras Nationwide*, 404Media (Aug. 26, 2025), https://perma.cc/M6VB-T9L3.

[33] Cox & Koebler, *supra* note 30; John O'Connor, *License Plate Camera Company Halts Cooperation with Federal* Agencies, ABC News (Aug. 25, 2025), https://perma.cc/79FV-Z29H.

granular the data. This allows officers to make inferences about individuals that they could not have made without such historical data. ALPR data can reveal not only where a driver was on a given date and time in the past, but can also suggest where a driver may be in the future.[34] As one regional California agency recognized in its privacy impact assessment, "particularly when collected over an extended period of time," ALPR data "could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities."[35]

Newer systems, like Flock's, that incorporate AI to create a "vehicle fingerprint," collect even more revealing data. As mentioned above, Flock can track bumper stickers, which may have political statements, and other identifying information about a vehicle. And while officers currently need to access a separate system to identify an owner of a vehicle, Flock is developing a product that will

---

[34] Off. of the Att'y Gen. of N.J., *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* 4 (effective Jan. 18, 2011), https://perma.cc/5DXG-UPM4; Steve Connor, *Surveillance UK: Why This Revolution is only the Start*, The Independent (Dec. 22, 2005), https://perma.cc/K9XC-DJT3.

[35] Northern Cal. Reg'l Intel. Ctr., *Initial Privacy Impact Assessment for Automated License Plate Reader Technology* 3, https://perma.cc/CFB4-5RDE.

allow an officer to "jump from LPR [license plate reader] to person," all within in the same system.[36] Flock has also added features like "convoy analysis," which will list vehicles that frequently travel with a vehicle that is searched, and "multi-geo search" which will return a list of all cars that have been to a given number of locations.[37] These features make it even easier for law enforcement to track people's social networks and travel habits through ALPR systems.

License plate data is already being used to identify individuals and their personal characteristics and habits. In August 2012, the Minneapolis *Star Tribune* published a map displaying the 41 locations where license plate readers had recorded the mayor's car in the preceding year.[38] In 2018, local reporters in Atlanta were able to use ALPR data to map a vehicle's travels over the course of just one day.[39] Using Oakland Police Department ALPR data, *Ars Technica* was able to correctly guess the block where a city council member lived after less than a minute of research.[40]

---

[36] Cox, *supra* note 10.

[37] Ben Miller, *Flock Safety Gives Users Expanded Vehicle Location Abilities*, Government Technology (Sep. 1, 2021), https://perma.cc/Z8NT-G8JU.

[38] Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, Star Tribune (Aug. 17, 2012), https://perma.cc/5V27-YTBE.

[39] Josh Wade, *Follow the Trail of a License Plate*, Knight Lab, https://perma.cc/N9AW-ZBTF.

[40] Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from the Cops*, Ars Technica (Mar. 24, 2015), https://perma.cc/3DHK-

Ars Technica also ran the plate number from a random vehicle near a bar against the Oakland data; it found that "the plate had been read 48 times over two years in two small clusters: one near the bar and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[41] Given these capabilities, it is no wonder that the International Association of Chiefs of Police has cautioned that ALPR technology creates the risk "that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[42]

F. ALPR Systems Make Errors, Have Security Issues, and Fail to Prevent Misuse.

ALPR systems make errors that have led to dangerous police conduct on multiple occasions.[43] In several cases, license plate misreads have led police to stop innocent drivers and hold them at gunpoint while police searched their car. In a case in Colorado, a woman and her four children were forced to the ground in a parking

---

JCSY.

[41] *Id*.

[42] Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* 13 (Sep. 2009), https://perma.cc/95KZ-A4HC.

[43] *See 2024 Annual Report*, *supra* note 14 at 29 (detailing several misreads).

lot and held at gunpoint.[44] Police have detained, handcuffed, arrested, and interrogated innocent people, all because the ALPR misread their plate.[45]

ALPR data has also been misused and used for unlawful purposes. Officers from several agencies across the country have used ALPR data to stalk their wives or girlfriends.[46] New York police collected license plate data to track Muslims and identify mosque attendees.[47] Another officer who was a serial burglar even monitored license plate data "to determine if he had been identified as a suspect for his crimes."[48]

ALPR systems have had numerous security issues. In July 2025, researchers discovered that a misconfigured demo exposed Flock Safety's 83,000-camera nationwide network to inclusion in Google's search engine, including sensitive

[44] Jessica Porter, *Aurora Police Detain Black Family after Mistaking their Vehicle as Stolen*, Denver7 (Aug. 3, 2020), https://perma.cc/W7XY-E7BD.

[45] *See 2024 Annual Report*, *supra* note 14 at 29.

[46] Shawn Loging, *Kechi Police Lieutenant's Arrest puts Flock Technology under Scrutiny*, KWCH 12News (Nov. 4, 2022), https://perma.cc/YMP2-NG3R.

[47] Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), https://perma.cc/3LZE-5B2L.

[48] *See 2024 Annual Report*, *supra* note 14 at 30.

portions of its source code.[49] In 2024, the federal government warned of major vulnerabilities in Motorola's Vigilant ALPR systems, including default Wi-Fi passwords, unencrypted data, and unrestricted remote access.[50] Research in 2024 revealed that more than 125 law enforcement agencies reported a data breach or cyberattacks between 2012 and 2020.[51] In 2019, CBP's vendor providing ALPR technology for Border Patrol checkpoints was breached, with hackers gaining access to 50,000 license plate images.[52] And research in 2015 that found more than 100 ALPR cameras in Louisiana, California and Florida were connected to the internet in an unsecured fashion, many with publicly accessible websites that anyone could

[49] Joshua Garett, *How a Misconfigured Demo Exposed Flock Safety's 83,000-Camera Nationwide Tracking System*, Nexanet.AI Blog (July 15, 2025), https://perma.cc/DLK9-BGG3.

[50] Dave Maass & Cooper Quintin, *New ALPR Vulnerabilities Prove Mass Surveillance is a Public Safety Threat*, EFF (June 18, 2024), https://perma.cc/S7BJ-5KYP; *ICS Advisory: Motorola Solutions Vigilant License Plate Readers*, Cybersecurity and Infrastructure Sec. Agency (June 13, 2024), https://perma.cc/2YHQ-9F4T

[51] EFF, *When Cops Get Hacked at HOPE 2020*, at 00:00–00:10 (YouTube, Aug. 19, 2020), https://www.youtube.com/watch?v=58lICmpJTCk.

[52] Kevin Collier & Sergio Hernandez, *At Least 50,000 License Plates Leaked in Hack of Border Contractor not Authorized to Retain Them*, CNN (June 19, 2019), https://perma.cc/BSQ6-MWFE.

use to manipulate the controls of the cameras or siphon off data.[53] Just by visiting a URL, a malicious actor, without any specialized knowledge, could view live feeds of the cameras.[54]

II. Reviewing Collected ALPR DATA Constitutes a Fourth Amendment "Search."

A. Individuals Maintain a Reasonable Expectation of Privacy in Their Movements.

Mr. Church had a reasonable expectation of privacy in ALPR data accessed by the police because it revealed information about his location and whereabouts over time. This is true despite the fact that his plate was scanned while his car was at a public road. Supreme Court case law has explained that while individuals may have lessened expectations of privacy in certain information they reveal publicly, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 585 U.S. at 310; *Jones*, 565 U.S. at 400. As recognized by five concurring Justices in *Jones* and reaffirmed by the majority in *Carpenter*, "individuals have a reasonable expectation of privacy in the whole of their physical movements" because of the "privacies of life" those movements can

---

[53] Dave Maass & Cooper Quintin, *License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech*, EFF (Oct. 28, 2015), https://perma.cc/4CZL-7TB5.

[54] *Id.*

reveal. *Carpenter*, 585 U.S. at 310 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id*. at 415 (Sotomayor, J., concurring)).

In *Carpenter*, the Supreme Court held that a Fourth Amendment search occurs when the government tracks an individual's movements by accessing Cell Phone Location Information ("CSLI"), at least for more than seven days. *Id*. at 310 n.3. The Court recognized that the expectation of privacy at issue was not about "using a phone," but rather in the record of a person's location and movements revealed by data generated by the use of the phone. *Id*. at 315. Likewise, in this case, Mr. Church's expectation of privacy was not in individual aspects of his car or its license plate, but in the record of his movements revealed by ALPR data.

B. ALPR Systems Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

The Commonwealth argues that use of modern technology to seamlessly capture, aggregate, and search massive amounts of ALPR data as identical to the observation of a license plate and other characteristics of a single vehicle at a single point in time by an individual law enforcement officer. Other than the fact that both involve officers and license plates, they could not be more different.

In a series of cases addressing the power of sense-enhancing technologies "to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 585 U.S. at 305

(quoting *Kyllo v. United States,* 533 U.S. 27, 34 (2001)) (last alteration in original); *accord Jones*, 565 U.S. at 406. As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

Innovations like ALPR systems remove many of these types of practical limitations in the context of license plates and associated ALPR data. Indeed, as ICE explains, use of ALPR data "reduc[es] the work-hours required for physical surveillance."[55] Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Court has admonished lower courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 585 U.S. at 320.

In *Carpenter*, the Supreme Court held that a Fourth Amendment search occurs when the government tracks an individual's movements by collecting CSLI from a cellular service provider, at least for more than seven days. *Id*. at 315–316. The Court noted that under *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v.*

[55] *Statement of Work: Access to License Plate Reader Commercial Data Service* at 288, ICE First Interim Response, *ACLU v. ICE*, 18-cv-04105 (N.D. Cal. 2018) , *available at* https://perma.cc/4PZ4-3HGL.

Miller, 425 U.S. 435 (1976), individuals ordinarily do not have a reasonable expectation of privacy in business records that they voluntarily disclose to third parties or to the public at large. *Id*. at 308. However, it declined to extend *Smith* and *Miller* to the collection of CSLI, listing several factors that distinguish tracking individuals' cell phones from more primitive forms of surveillance. *Id*. at 309–312. The en banc Fourth Circuit subsequently applied this insight in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, finding that police violated the Fourth Amendment by operating an aerial surveillance program that captured blurry photographs of people's movements throughout the city of Baltimore without suspicion and without requiring a warrant to consult. 2. F.4th 330 (4th Cir. 2021) (en banc).

ALPRs infringe on individuals' expectations of privacy for much the same reason that the Global Position System ("GPS") monitoring of vehicles at issue in *Jones*, the tracking of cell phones in *Carpenter*, and the aerial surveillance in *Leaders of a Beautiful Struggle* do: they facilitate detailed, pervasive, cheap, and efficient tracking of millions of Americans in previously unthinkable ways.

1. Detailed Nature of the Data.

First, the *Carpenter* Court noted that "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 585 U.S. at 309.

As described above, ALPR databases like the one accessed by the government here share these characteristics. GPS coordinates associated with ALPR records can place vehicles at highly specific locations at specific times, locating an individual's car with more precision than the cell phone data at issue in *Carpenter* or even the GPS tracker in *Jones*. *See id*. at 312 (CSLI accurate to within one-eighth to four square miles); *Jones*, 565 U.S. at 403 (GPS device accurate to within 50–100 feet); *supra* Section I.A. (ALPR location data accurate to within feet of the vehicle).

Furthermore, ALPR data allows the government to track people to locations that reveal private information about their lives. That is because the geographical precision of ALPR data facilitates inferences about individuals' locations in homes, offices, hotel rooms, and other spaces that receive the highest protection under the Fourth Amendment, and for which warrantless searches using both traditional and technological means are forbidden. *Kyllo*, 533 U.S. at 40. "Mapping a cell phone's location over the course of [time] provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them, his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 585 U.S. at 311 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). ALPR data raises identical concerns.

Although ALPR systems may sometimes compile fewer individual data points than GPS tracking or CSLI, even a small number of ALPR data points facilitate inferences about individuals' travels habits, including the homes, businesses and neighborhoods they frequent. *See supra* Section I.E. After all, "[t]he datasets in *Jones* and *Carpenter* had gaps in their coverage, too," but "in both cases, the surveillance still surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of individuals' movements." *Leaders of a Beautiful Struggle*, 2 F.4th at 342–43; *see id.* at 343 (discussing how even where location collection has gaps, the sensitivity of certain locations such as the home will often allow police to "deduce identity"). And it is of no matter that the government extrapolates a person's whereabouts using ALPR data rather than observing them directly because "the Court has already rejected the proposition that 'inference insulates a search.'" *Carpenter*, 585 U.S. at 312 (quoting *Kyllo*, 533 U.S. at 36). Every time a government agent queries an ALPR database, as the police did in this case, they search the millions of records it contains. As a result, this is a search of long-term location data even though agents may only rely on a small number of records produced in response to their queries. *See Carpenter*, 585 U.S. at 310 n.3 (period of location data accessed by government is "pertinent period" for determining whether a search occurred); *United States v. Smith*, 110 F.4th 817, 837–38 (5th Cir. 2024), *petition for cert. filed*, No. 24-7237 (U.S. May

13, 2025) (holding that geofence "warrants" are unconstitutional general warrants because "[w]hile the *results* of a geofence warrant may be narrowly tailored, the *search* itself is not" and that "[a] general warrant cannot be saved simply by arguing that, after the search has been performed, the information received was narrowly tailored to the crime being investigated.").

The Commonwealth argues that because it could, in theory, deploy 172 officers 24 hours a day to stand in the positions of the ALPR cameras, the ALPR dragnet merely "enhances the ability of law enforcement to perform duties they already could complete of their own accord" and is therefore constitutional. Opening Br. 2, 28. But those officers would not come close to duplicating the effects of the ALPR dragnet. Even imagining that 172 officers, working without food or breaks, could take note of and memorize the license plate numbers, direction, time, and surrounding detail of every car that passed by them, they would not be able to instantaneously relay all this information back to a central hub that could be queried by any other officer—a query that could then be supplemented by information from any other law enforcement database. In other words, they would not be able to instantly create a searchable database of images with total recall across weeks of data.

Even the Commonwealth's argument that ALPRs merely "augment" the naked eye, Opening Br. 27–28, does not shield this technology from constitutional

scrutiny. The Supreme Court has held that "sense-enhancing technology" could not be used "absent a warrant" where such use failed to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 305 (quoting *Kyllo*, 533 U.S. at 34). Far from blessing this kind of surveillance, "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns" while making clear that the prolonged tracking required a warrant. *Leaders of a Beautiful Struggle*, 2 F.4th at 341. Such is the case with the prolonged tracking here, where ALPRs track people in ways that the framers of the Fourth Amendment would have assumed was impossible.

2. Indiscriminate Collection of Data.

An equally important factor in the *Carpenter* Court's decision was the recognition that cell phone tracking allows the government to track essentially any person at any time. "[T]his newfound tracking capacity runs against everyone," the Court wrote, and "[o]nly the few without cell phones could escape this tireless and absolute surveillance." 585 U.S. at 312.

The same is true of ALPR systems. For the vast majority of Americans, the choice to drive on public streets is not a luxury; it is "indispensable to participation in modern society." *Id*. at 298. In many parts of the country, people have no choice

but to drive themselves to work, a grocery store, doctor's office, place of worship, even in some cases to see a neighbor. In one survey, Gallup found that 84% of Americans drive frequently, and 64% drive every day.[56] And once people drive on the public roads or even park in a privately owned lot or in their own driveway, there is little they can do to avoid having their precise location tagged by an ALPR system and made accessible to law enforcement without any suspicion of wrongdoing.

The indiscriminate nature of this surveillance serves to distinguish ALPRs from many of the targeted, individual forms of surveillance discussed in the Commonwealth's Opening Brief, such as the beeper placed on a single truck in *United States v. Knotts*, 460 U.S. 276 (1983),[57] the single airplane flown in *California v. Ciraolo*, 476 U.S. 207, 214–15 (1986) (involving a one-time, "simple visual observation[]" of curtilage from 1000 feet with "the naked eye"), or the pole cameras observing a single location in *United States v. Vankesteren*, 553 F.3d 286

[56] Megan Bryan, *83% of U.S. Adults Drive Frequently; Fewer Enjoy it a Lot*, Gallup (July 9, 2018), https://perma.cc/9M3G-JMUD.

[57] In *Carpenter*, the Supreme Court itself distinguished *Knotts*, which involved the limited question of movements "from one place to another." *Carpenter*, 585 U.S. at 306 (describing *Knotts* as addressing "a discrete 'automotive journey'" (quoting *Knotts*, 460 U.S. at 285)); *id*. at 315 ("[T]his case is not about . . . a person's movement at a particular time."). Moreover, the *Knotts* Court foresaw the problem addressed in *Jones* (and, later, *Carpenter*), warning that if law enforcement ever did manage, in the distant future, to implement "dragnet type law enforcement practices," there would be "time enough then to determine whether different constitutional principles" applied. 460 U.S. at 284.

(4th Cir. 2009) (Of course, all of these cases—even while being clearly distinguishable in their own right—pre-date *Carpenter*.). Indeed, the difference is so clear that Judge Gregory, the author of *Vankesteren*, was also later the author of the *en banc* opinion in *Leaders of a Beautiful Struggle* finding the Baltimore Police Department's aerial surveillance program of public places constituted a violation of the Fourth Amendment. *See generally,* 2 F.4th 330. As Judge Gregory noted in his opinion for the court, "[w]ithout technology, police can attempt to tail suspects, but [dragnet surveillance] is more like 'attach[ing] an ankle monitor' to every person in the city." *Leaders of a Beautiful Struggle*, 2 F.4th at 341 (citing *Carpenter*, 585 U.S. at 312). Because it targets *all* drivers on Norfolk's roads regardless of suspicion or law enforcement interest, the ALPR dragnet at issue in this case is governed squarely by *Carpenter*.

3. Retrospective Searches.

The third factor that led the Court in *Carpenter* to distinguish CSLI from traditional law enforcement surveillance was "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id.* at 312. As the Court explained, CSLI is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the

frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers." *Id*. ALPR records provide equivalent capabilities. Like CSLI, the lengthy and frequently unlimited retention periods for ALPR data allow these retrospective searches. *See Carpenter*, 585 U.S. at 312 (retention periods of up to 5 years).

The Fourth Circuit in *Leaders of a Beautiful Struggle* also held that ability to consult historic data helped create the kind of "detailed, encyclopedic" record that required a warrant to access. 2 F.4th at 341–42. In *Leaders*, a private contractor was conducting persistent aerial surveillance of Baltimore, which showed people and vehicles as blurred dots and blobs. *Id.* at 334. When certain crimes occurred, police would receive a report with responsive data from both before and after the crime. *Id*. These reports included the "tracks" of "vehicles and people present at the scene" as well as the locations they came from and went to. *Id.* Critically, these "tracks" were "often shorter snippets of several hours or less." *Id.* at 342. Nonetheless, the Fourth Circuit held that *Carpenter* applied because the tracks were culled from the contractor's 45-day repository. *Id.* at 341–42. The length of the "track" was not what counted, but the fact that police could to effectively "travel back in time" and observe someone's movements, such that "'[w]hoever the suspect turns out to be,' they have 'effectively been tailed' for the prior six weeks." *Id*. at 341. *Leaders* was clear that

this "retrospective quality of the data" distinguishes it from traditional forms of surveillance like security cameras. *Id.* at 342. As the court explained, "[p]eople understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time … [b]ut capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity." *Id.* at 345. As in *Carpenter*, it "enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at 342. As in *Leaders*, a geofence warrant is so unlike surveillance cameras that it "transcends mere augmentation of ordinary police capabilities," akin to a time machine that has no analog prior to the digital age. *Id.* at 345.

The confluence of these factors—detailed location data collection about a vast swath of the American population allowing retrospective searches—is why technologies like ALPRs violate expectations of privacy under the Fourth Amendment. "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Carpenter*, 585 U.S. at 313–314. And access to technologies like these is "remarkably easy, cheap, and efficient compared to traditional investigative tools," *id*. at 311, thereby upending traditional protections against pervasive government monitoring on which Americans have long relied.

III. Searches of ALPR Databases Require a Warrant.

Because ALPR data can reveal private and sensitive details about a person's life—details that individuals reasonably expect to remain private—warrantless searches of ALPR databases by law enforcement to find evidence of criminal activity are *per se* unreasonable.

As the Supreme Court stated in *Carpenter*, warrantless searches "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" are typically unreasonable absent limited and specific exceptions. 585 U.S. at 316 (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652–53 (1995)). None of those exceptions apply here. Notably, in *Jones* the Court did not apply the so-called automobile exception to justify warrantless tracking of the location of a car. 565 U.S. at 412; *see also United States v. Katzin*, 732 F.3d 187, 204 (3d Cir. 2013) (holding that the automobile exception does not permit warrantless GPS tracking of a vehicle because the exception does not "permit [police] to leave behind an ever-watchful electronic sentinel in order to collect future evidence" based on the location of the car), *rev'd en banc on other grounds*, 769 F.3d 163 (3d Cir. 2014); *Collins v. Virginia*, 584 U.S. 586, 598 (2018) (rejecting argument that "the automobile exception is a categorical one that permits the warrantless search of a vehicle anytime, anywhere").

Here, unlike *Carpenter*, law enforcement did not seek or obtain *any* court process prior to searching the database. *See Carpenter*, 585 U.S. at 317 (government obtained CSLI records pursuant to a court order issued under the Stored Communications Act, which required it to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation"). It did not even obtain the data pursuant to a subpoena. *Id*. at 362–363 (Alito, J. dissenting) (noting with approval that court order in *Carpenter* "was the functional equivalent of a subpoena for documents"). Yet, as shown above, ALPR data can be just as revealing as CSLI, and therefore individuals maintain a similar reasonable expectation of privacy in it. For this reason, ALPR data should be subject to the same warrant requirement as CSLI—absent a clear showing of exigent circumstances, law enforcement must get a warrant before conducting searches of ALPR data. *See id*. at 320.

Even if the initial collection and retention of ALPR data were considered reasonable, that would not insulate a further query of that data without a warrant if that search is conducted to find evidence of criminal wrongdoing. When law enforcement "access" raw data gathered by surveillance, "it invades the recorded individuals' reasonable expectation of privacy, conducting a search." *Leaders of a Beautiful Struggle*, 2 F.4th at 344; s*ee also, e.g., Skinner v. Ry. Lab. Execs. Ass'n*, 489 U.S. 602, 616 (1989) (disaggregating initial physical collection of a blood or

breath sample from secondary search through "ensuing chemical analysis of the sample to obtain physiological data"). In a variety of contexts, courts have held that a warrant may be required to conduct later searches of even lawfully collected data, because the collection and the querying are distinct Fourth Amendment events. For example, in *United States v. Sedaghaty*, the Ninth Circuit required investigating agents to obtain a new warrant before searching computer hard-drives that had been lawfully seized pursuant to an earlier warrant. 728 F.3d 885, 913 (9th Cir. 2013); *see also United States v. Ganias*, 755 F.3d 125, 127–128 (2d Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016) (same); *United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999); *United States v. Hulscher*, No. 4:16-CR-40070-01-KES, 2017 WL 657436, at *3 (D.S.D. Feb. 17, 2017) (law enforcement must obtain a warrant to search data lawfully-collected by a different agency for a different purpose); *United States v. Hasbajrami*, 945 F.3d 641, 670 (2d Cir. 2019) ("[Q]uerying . . . stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable."). Thus, any search of a database of mass, suspicionless ALPR data, whether collected by law enforcement agencies or private entities, requires a warrant.

CONCLUSION

For the foregoing reasons, this Court should affirm the ruling of the Circuit Court and hold that the warrantless use of ALPR systems in this case violated the Fourth Amendment. The ALPR results should be suppressed, as should all evidence gathered as a result of that scan.

Dated: August 28, 2025

Respectfully submitted,

By: /s/ Matthew W. Callahan

RULE 5A:23(e)(2) STATEMENT

No party's counsel authored this *amicus* brief in whole or in part.

No party or party's counsel contributed money that was intended to fund preparing or submitting this brief.

No person—other than the *amici curiae*, their members, or their counsel—contributed money that was intended to fund preparing or submitting the brief.

CERTIFICATE OF SERVICE AND COMPLIANCE

I, Matthew W. Callahan, certify as follows:

(a) On August 28, 2025, an electronic copy of this *amicus* brief was filed, via VACES, with the Office of the Clerk, Court of Appeals of Virginia, 109 North Eighth Street, Richmond, VA 23219.

(b) One August 28, 2025, one electronic copy of this paper was served via email upon:

Counsel for Appellant: S. Hallie Hovey-Murray, Assistant Attorney General, from the Office of the Attorney General at oagcriminallitigation@oag.state.va.us and hhovey-murray@oag.state.va.us. and

Counsel for Appellee: Samantha Offutt Thames, Senior Appellate Attorney and Lauren Brice, Assistant Public Defender, from the Virginia Indigent Defense Commission at sthames@vadefenders.org and lbrice@vadefenders.org.

(c) This *Amicus* Brief contains 8038 words in compliance with Rule 5A:19(a).

/s/ Matthew W. Callahan