In The

Supreme Court of Virginia

RECORD NO. 191129

FAIRFAX COUNTY POLICE DEPARTMENT, ET AL.,

Appellants,

v.

HARRISON NEAL,

Appellee.

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND BRENNAN CENTER FOR JUSTICE AT NYU LAW SCHOOL IN SUPPORT OF APPELLEE HARRISON NEAL

Matthew J. Erausquin
(VSB No. 65434)
CONSUMER LITIGATION ASSOCIATES, P.C.
1800 Diagonal Road, Suite 600
Alexandria, Virginia 22314
(703) 273-7770 (Telephone)
(888) 892-3512 (Facsimile)
matt@clalegal.com

Counsel for Amici Curiae

Naomi Gilens
(pro hac vice pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 463-9333 (Telephone)
(415) 436-9993 (Facsimile)
naomi@eff.org

Counsel for Amicus Curiae

Rachel Levinson-Waldman
(admitted pro hac vice)
BRENNAN CENTER FOR JUSTICE AT NYU LAW SCHOOL
1140 Connecticut Avenue NW,
Suite 1150
Washington, DC 20036
(202) 249-7193 (Telephone)
(202) 223-2683 (Facsimile)
levinsonr@brennan.law.nyu.edu

Counsel for Amicus Curiae

THE LEX GROUP ♦ 1108 East Main Street ♦ Suite 1400 ♦ Richmond, VA 23219
(804) 644-4419 ♦ (800) 856-4419 ♦ Fax: (804) 644-3660 ♦ www.thelexgroup.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

LEGISLATIVE MATERIAL

OTHER AUTHORITIES

INTEREST OF AMICI CURIAE

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit civil liberties organization that has worked to protect privacy and free speech rights for nearly 30 years. With more than 35,000 active dues-paying members nationwide, including many in Virginia, EFF represents the interests of its members in both court cases and broader policy debates surrounding the application of the law in the face of emerging technologies. EFF has served as amicus in numerous U.S. Supreme Court cases involving the application of constitutional principles to location-tracking technologies, including *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 565 U.S. 400 (2012). EFF has also served as counsel or amicus in numerous cases involving privacy in location data at all levels of the federal and state court systems, including previously in *Neal v. Fairfax,* 812 S.E.2d 444 (Va. 2018) ("*Neal I*").

The Brennan Center for Justice at NYU School of Law (the Center) is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Center's Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic

intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Carpenter*, 138 S. Ct. 2206; *Riley*, 134 S. Ct. 2473; *Jones*, 132 S. Ct. 945; *United States v. Ackerman*, No. 17-3238, 2020 WL 916073 (10th Cir. February 26, 2020); *United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 1186 (2018); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 569 (2016); *United States v. Houston*, 813 F.3d 282 (6th Cir. 2016), *petition for reh'g en banc denied* (Apr. 14, 2016); *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016), *petition for cert. docketed*, No. 16-6308 (Oct. 4, 2016); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *Neal I,* 812 S.E.2d 444; and *Alasaad v. Nielsen*, 419 F.Supp.3d 142 (D. Mass 2019). The Brennan Center also publishes scholarship on the privacy of personal data, including but not limited to automatic license plate reader data; *see*, *e.g.*, Rachel Levinson-Waldman, *Cell Phones*, *Law Enforcement*, *and the Right to Privacy* (2018); and Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L.J. 537 (2017).

STATEMENT OF THE CASE

Amici concur with the Statement of the Case set forth in Respondent Neal's response brief.

STATEMENT OF FACTS

Amici concur with the Statement of Facts set forth in Respondent Neal's response brief.

STANDARD OF REVIEW

Amici concur with the Standard of Review set forth in Respondent Neal's response brief.

ASSIGNMENTS OF ERROR

Amici concur with the Assignment of Error set forth in Respondent Neal's response brief.

ARGUMENT

The Fairfax County Police Department, like thousands of other law enforcement agencies around the country, uses a technology called automated license plate readers (ALPRs) to indiscriminately scan the license plates of vehicles driving through the county. Despite the fact that more than 99% of vehicles scanned are not associated with any criminal activity, the Department stores detailed data on the time, date, and location of each scan for 364 days. This data, individually and in the aggregate, reveals the rich and complex details of people's locations, movements, and associations over time.

In 2018, this Court recognized that the Department's passive collection of license plate data, including "the GPS location, time, and date when the image was captured 'afford a basis for inferring personal characteristics, such as . . . things done by or to' the individual who owns the vehicle, as well as a basis for inferring the presence of the individual who owns the vehicle in a certain location at a certain time." *Neal I*, 812 S.E.2d at 450 (quoting Va. Code § 2.2-3801) (omission in original). The Court recognized that the Department's actions constituted "sweeping randomized surveillance and collection of personal information." *Id.* at 451. On remand, the circuit court further recognized that, because the Department's "ALPR system provides a means through which a link to the identity of a vehicle's owner can be readily made," the Department's passive use of the ALPR system violates the Virginia Government Data Collection and Dissemination Practices Act (Data Act). *Neal v. Fairfax*, No. CL-2015-5902, 2019 WL 1438078 at *4 (Va. Cir., Apr. 1, 2019). The Virginia Legislature passed the Data Act to protect the public from the increased threat to civil liberties created by technology like ALPRs. Va. Code § 2.2-3800(B)1-2. This Court should uphold the circuit court and order the Department to purge any and all passive ALPR data.

ALPR data can reveal detailed information about "an individual's life and associations." *Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1104 (Mass. 2020). Much like the cell site location information (CSLI) at issue in the recent U.S.

Supreme Court case *Carpenter v. United States*, ALPR data "allow[s] the police to reconstruct people's past movements without knowing in advance who police are looking for, thus granting police access to 'a category of information otherwise [and previously] unknowable.'" *Id.* (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (second alteration in original)). Also as with CSLI, it is virtually impossible to avoid having one's license plate data collected. Like 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*, 138 S. Ct. at 2220. And yet, by driving a car, drivers must give up detailed information on their locations to the law enforcement agencies and private companies around the country that quietly scan and record the locations of billions of vehicles' license plates, regardless of whether individual drivers are suspected of criminal activity.

Although location information can reveal sensitive and private information about individuals even when it is not directly connected to data that would traditionally be considered personally identifying—such as a name or a driver's license number—police officers can use ALPR data to identify a particular vehicle, to detect patterns of travel, and, within a matter of seconds, to identify the vehicle's owner. The ability to link license plate numbers to individuals is a core feature of

ALPR databases, and one on which law enforcement officers rely to investigate crimes.

Because the Fairfax County Police Department ALPR database allows officers to easily link license plate information to specific individuals, the database constitutes an "information system." As the circuit court correctly concluded, the ALPR data is therefore covered by the Government Data Collection and Dissemination Practices Act.

I. ALPR systems are "information systems" under the Data Act.

As this Court previously explained, "the determination of whether the ALPR database is an 'information system' under the Data Act turns on whether [the database] contains 'the name, personal number, or other identifying particulars' of an individual." *Neal I*, 812 S.E.2d at 450. A license plate number is an "identifying particular" under the statute because the "total components" of the ALPR record-keeping process provide information related to the individual to whom a specific plate is registered. *Id*. Thus, the ALPR database is part of an "information system" under the Data Act because it provides the means for discerning personally identifiable information.[1]

[1] As this Court recognized in *Neal I*, and as the U.S. Supreme Court subsequently agreed, license plate scans provide "a basis for inferring the presence of the individual who owns the vehicle in a certain location at a certain time." *Neal I*, 812 S.E.2d at 450; *see also Kanas v. Glover*, 140 S. Ct. 1183, 1188 (2020) (holding

There is no dispute, in this case, that the ALPR database allows police officers to connect license plate numbers with specific individuals in a matter of moments. *See Neal v. Fairfax*, No. CL-2015-5902, 2019 WL 1438078 at *4 (Va. Cir., Apr. 1, 2019) (explaining that an officer can access a license plate number from the ALPR software and cross-reference the plate number with the specific individual to whom the plate is registered by opening a second program through "a few clicks on the screen, all from the driver's seat of a police cruiser"). This is true for officers in almost any jurisdiction in the country—squad car computer systems are designed to determine almost instantaneously not just who owns the car in front of them but also where that person lives, their associated driving records, and any outstanding warrants. According to the Justice Department's Bureau of Justice Statistics, "[m]ore than 90% of local police departments serving 25,000 or more residents provided patrol officers with in-field computerized access to vehicle records, driving records, and outstanding warrants."[2] Departments serving larger

---

that it is reasonable to infer that driver of car is the person to whom the plate is licensed).

[2] Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology*, Bureau of Justice Statistics, NCJ 248767 at 1 (July 2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf. Baltimore Police appear to have had access to these data sources since at least 1995. *Computers in Police Cars*, Baltimore Sun (Nov. 28, 1994), http://articles.baltimoresun.com/1994-11-28/news/1994332162_1_patrol-officers-computer-police-cars.

populations have in-car access to even more data, including the National Crime Information Center's twenty-one individual property and person databases and more than one hundred other data sources.[3]

The fact that ALPR systems are part of an information system designed to identify *individuals*, not just their vehicles, accords with former Virginia Attorney General Kenneth Cuccinelli's Advisory Opinion Letter on ALPR data collection and with statements by other law enforcement agencies around the country. When confronted with the question of the Data Act's application to ALPR systems in 2013, Cuccinelli determined ALPR data can, for example, "assist in locating *an individual data subject*, documenting his movements, or determining his personal property holdings."[4] Law enforcement agencies around the country agree. The Los Angeles Police Department has stated that ALPR data can be used "to identify driving patterns of a *particular individual*."[5] The California State Auditor,

---

[3] National Crime Information Center, FBI, https://www.fbi.gov/services/cjis/ncic; *see also* Matt Burns, *Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients*, TechCrunch (Jan. 11, 2015), https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/.

[4] Advisory Opinion Letter from Kenneth T. Cuccinelli, Op. Va. Att'y Gen., to Col. W.S. Flaherty, Superintendent Va. Dept. of State Police (Feb. 13, 2013), 2013 WL 653025 (emphasis added).

[5] Opp'n Br. of City of Los Angeles at 29, *ACLU v. Super. Ct.*, No. B259392 (Cal. Ct. App. Nov. 26, 2014) (emphasis added), available at

explaining the technology's potential for misuse, noted that it "is easy for a law enforcement officer" to tie "a license plate to an individual's identity," and that ALPR images then facilitate tracking that individual's movements.[6] And the Texas Department of Public Safety has noted, "because most law enforcement data systems have been designed with traffic stops in mind, it is very easy for a police officer to obtain information about *vehicle owners and drivers* from license plate information."[7]

Tying license plates to individuals is one of the most important features of ALPR systems. In its marketing to law enforcement agencies, Vigilant Solutions, one of the largest aggregators of ALPR data in the country, makes clear: an ALPR system "isn't just for finding stolen vehicles."[8] Rather, Vigilant states that ALPR

---

https://www.eff.org/files/2016/08/03/brf.calapp.city_opp_to_petition_for_writ_of_mandate.pdf.

[6] Cal. State Auditor, *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects*, Report No. 2019-118 (Feb. 2020) at 23, https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf.

[7] Privacy Impact Assessment for Texas Dept. of Public Safety at 4 (Sept. 2014) (emphasis added), http://www.txdps.state.tx.us/administration/crime_records/pages/LPRPIA.pdf.

[8] Vigilant Solutions, Vigilant PlateSearch, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/.

data "can assist with keeping track" of people.[9] And Vigilant advertises ALPR's potential to aid law enforcement in "developing leads and solving crimes" by allowing law enforcement to identify suspects, witnesses, and alibis[10]—all with "just a few clicks on the screen, all from the driver's seat of a police cruiser." *Neal v. Fairfax*, No. CL-2015-5902, 2019 WL 1438078 at *4 (Va. Cir., Apr. 1, 2019). Amici the Virginia Commonwealth Attorneys only underscore this point by emphasizing how law enforcement relies on ALPR data to identify specific individuals, such as "a suspected burglar whose license plate was captured," or "a suspected serial bank robber whose license plate was identified." Br. of Amici Curiae Virginia Commonwealth's Attorneys (filed Apr. 20, 2020) at 9. In each of these examples, the value of the license plate data lies wholly in law enforcement's ability to connect it to an identifiable individual.

Upholding the circuit court's opinion that ALPR data is part of an "information system" subject to the Data Act also aligns with the Act's legislative history. As noted by this Court, the Act was prompted by the "proliferation in the use of automated data processing equipment . . . that has enabled government and

---

[9] Cal. Office of Emergency Services, *License Plate Reader Participant Guide* at 145 (Mar. 2015), available at https://www.eff.org/files/2019/03/08/pra-lpr_redacted.pdf.

[10] Vigilant Solutions, Vigilant PlateSearch, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/.

private industry to compile detailed information on individuals in every area of personal activity." *Hinderliter v. Humphries*, 297 S.E.2d 684, 685 (Va. 1982). The Virginia Advisory Legislative Council, tasked at the time with examining the impact of data collection on privacy, noted the "potential gross abuse of the power of *intercommunicating data banks*" and recommended "setting reasonable, easily implemented standards of conduct" to protect Virginia residents. *Id*. at 686 (emphasis added) (quoting Report of the VALC to the Governor & General Assembly of Virginia, 2 House & Senate Documents, S. Doc. 27 at 11 (1976)). The Department's ALPR system is, in effect, part of an "intercommunicating data bank" that, as the circuit court recognized, "provides a means through which a link to the identity of a vehicle's owner can be readily made." As such, it is an "information system" subject to the Data Act.

II. ALPR systems collect a significant amount of data.

By design, ALPR collection is indiscriminate. ALPR cameras automatically scan and capture images of every license plate that comes into view, regardless of any association with criminal activity. In a 2018 nationwide survey, EFF and

Muckrock discovered that an average 99.5% of cars scanned were not associated with any crime.[11]

By scanning every license plate that comes into view—up to 3,600 plates per minute[12]—ALPRs collect an enormous volume of data. Atlanta, for example, processes nearly 30 million plates each month using just 347 ALPR cameras.[13] In Los Angeles, the Police and Sheriff's Departments collect data on 3 million cars each week.[14] The 173 law enforcement agencies surveyed in the 2018 EFF and Muckrock study scanned more than 2.5 billion license plates.[15]

---

[11] *See* Tanvi Misra, *Who's Tracking Your License Plate?*, Citylab (Dec. 6, 2018), https://www.citylab.com/equity/2018/12/automatedlicense-plate-readers-privacy-data-security-police/576904/.

[12] *Neal v. Fairfax*, No. CL-2015-5902, 2019 WL 1438078 at *2 (Va. Cir., Apr. 1, 2019).

[13] Josh Wade & Aaron Diamant, *Eyes on the Road*, Atlanta Journal-Constitution, http://specials.ajc.com/plate-data/.

[14] *See* Jennifer Lynch & Peter Bibring, *Secrecy Trumps Public Debate in New Ruling on LA's License Plate Readers*, EFF (Sept. 3, 2014), https://www.eff.org/deeplinks/2014/09/secrecy-trumps-public-debate-new-ruling-las-license-plate-readers; Aaron Mendelson, *California Police Scanned More Than 1 Billion License Plates - Rarely Finding Cars On 'Hot Lists'*, LAist (Nov. 16, 2018), https://laist.com/2018/11/16/license_plate_readers_eff_analysis.php.

[15] *See* Tanvi Misra, *Who's Tracking Your License Plate?*, Citylab (Dec. 6, 2018), https://www.citylab.com/equity/2018/12/automatedlicense-plate-readers-privacy-data-security-police/576904/.

What is more, ALPR use by government agencies is rapidly increasing. In 2013, the Bureau of Justice Statistics found that 93% of police departments in cities with 1 million or more residents, as well as more than three-quarters of departments serving 100,000 or more residents, used their own ALPR systems.[16] A 2014 nationwide survey of law enforcement ALPR use noted that the acquisition of ALPRs "has most likely tripled" in the previous ten years.[17]

Besides law enforcement agencies, private vendors who regularly contract with them and others also collect vast amounts of ALPR data on their own and aggregate it with information collected by police. Vigilant Solutions collects license plate data from federal, state, and local law enforcement agencies, in addition to using its own stable of private contractors to scan license plates around the country.[18] It stores this information in a database that totals more than six billion scans and is growing at a rate of more than 150 million plate scans each

---

[16] Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology*, Bureau of Justice Statistics, NCJ 248767 at 4 (July 2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf.

[17] Cynthia Lum, et al., *The Rapid Diffusion of License Plate Readers in U.S. Law Enforcement Agencies: A National Survey*, Geo. Mason Univ. Ctr. for Evidence-Based Crime Pol'y at 10 (Dec. 2016), http://cebcp.org/wp-content/lpr/LPR-National-Survey-Report-2016.pdf.

[18] *See* Vigilant Solutions, Vigilant PlateSearch, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/.

month.[19] Vigilant Solutions encourages law enforcement agencies "to share [license plate data] with other law enforcement agencies to gain access to billions of detections nationwide."[20] Using this database, even small police departments can access a vast trove of plate information from across the country. For instance, the Burr Ridge Police Department of Burr Ridge, Illinois, which serves a town in Illinois with a population of only 10,559 in the last census, uses Vigilant Solutions to share its plate data with more than one thousand local, regional, and federal agencies, and receives plate data from hundreds more,[21] as does the Byron Police Department of Byron, Georgia—a town with a population of under 5,000 at the last census.[22]

---

[19] *See* Vigilant Solutions, Find Scofflaws, http://www2.vigilantsolutions.com/find-scofflaws.

[20] *See* Vigilant Solutions, Vigilant PlateSearch, https://www.vigilantsolutions.com/products/license-plate-recognition-lpr/.

[21] 2020 Vigilant Data Sharing Information – Automated License Plate Reader (ALPR) (Burr Ridge Police Department), Muckrock (Jan. 28, 2020), https://www.muckrock.com/foi/burr-ridge-7596/2020-vigilant-data-sharing-information-automated-license-plate-reader-alpr-burr-ridge-police-department-87008/#file-840456; *see also* U.S. Census Bureau, Burr Ridge Village, Illinois, https://www.census.gov/quickfacts/burrridgevillageillinois.

[22] 2020 Vigilant Data Sharing Information - Automated License Plate Reader (ALPR) (Byron Police Department), Muckrock (Jan. 29, 2020), https://www.muckrock.com/foi/byron-5061/2020-vigilant-data-sharing-information-automated-license-plate-reader-alpr-byron-police-department-

The vast quantity of ALPR information that law enforcement and private actors collect is easily and widely shared among local, regional, state, and federal law enforcement agencies, along with other private companies. In 2019, a regional information-sharing collective of federal, state, and local law enforcement agencies in Northern California called the Northern California Regional Intelligence Sharing Center collected more than 40 million license plate scans from 29 different agencies in 90 days.[23] A similar fusion center in Maryland, called the Maryland Coordination and Analysis Center, received more than 450 million license plate scans in 2018 from twelve different state and local agencies.[24] EFF and Muckrock's 2018 national survey found that most agencies "were sharing data directly with around 160 other agencies."[25] Ten agencies were sharing data with

---

87009/#file-838790; *see also* U.S. Census Bureau, Byron City, Georgia, https://www.census.gov/quickfacts/byroncitygeorgia.

[23] 2020 Vigilant Data Sharing Information - Automated License Plate Reader (Northern California Regional Intelligence Center), Muckrock (Mar. 9, 2020), https://www.muckrock.com/foi/california-52/2020-vigilant-data-sharing-information-automated-license-plate-reader-northern-california-regional-intelligence-center-90306/#file-850292.

[24] Letter from David Engel, Director, Md. Coordination and Analysis Ctr., to Md. House Judiciary Committee (Feb. 22, 2019), https://assets.documentcloud.org/documents/6146047/Maryland-State-Police-PS3-509-E-2019.pdf.

[25] Dave Maass & Beryl Lipton, *What We Learned*, MuckRock (Nov. 15, 2018), https://www.muckrock.com/news/archives/2018/nov/15/alpr-what-we-learned/.

more than 800 other agencies.[26] In some cases, agencies were sharing data with other agencies they had never even heard of.[27]

III. Plate location data reveals highly sensitive personal information.

Each piece of information within the vast ocean of data ALPRs collect can reveal sensitive information about a person. And when those pieces are put together—as they are by Virginia law enforcement officers querying aggregate stored data of a vehicle's past travels—they can reveal a rich and detailed picture of a person's life.

ALPR systems record the precise time, date, and place that the scan occurred, including the direction and specific lane in which the cars were traveling.[28] This data can place vehicles at specific locations at specific times in the past, pinpointing an individual's car with even more precision than cell phone data or GPS trackers. *See Carpenter*, 138 S. Ct. at 2218 (cell phone location

---

[26] *Id.*

[27] *Id.*

[28] *See* Tanvi Misra, *Who's Tracking Your License Plate?*, Citylab (Dec. 6, 2018), https://www.citylab.com/equity/2018/12/automated-license-plate-readers-privacy-data-security-police/576904/; Allison Klein & Josh White, *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns*, Wash. Post (Nov. 19, 2011), https://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacyconcerns/2011/11/18/gIQAuEApcN_story.html.

information accurate to within one-eighth to four square miles); *United States v. Jones*, 565 U.S. 400, 403 (2012) (GPS device accurate to within 50 to 100 feet).

Such information opens the door to a universe of inferences about private aspects of people's lives. As the California Supreme Court recognized, "ALPR data showing where a person was at a certain time could potentially reveal where that person lives, works, or frequently visits. ALPR data could also be used to identify people whom the police frequently encounter, such as witnesses or suspects under investigation." *ACLU Found. v. Super. Ct.*, 400 P.3d 432, 439-40 (Cal. 2017).

Moreover, by storing passively collected license plate data for long periods of time, ALPR databases allow law enforcement officers to access months' worth of information about a car's past locations. "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Carpenter*, 138 S. Ct. at 2218. Now, much like cell phone location information and GPS tracking, ALPRs allow the police to "travel back in time to retrace a person's whereabouts . . . [and] police need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day" as long as the data is retained. *Id.*; *see also McCarthy*, 142 N.E.3d at 1104. For that reason, Massachusetts's highest court recently recognized that a one-year retention period,

like that of the FCPD, "certainly is long enough to warrant constitutional protection." *McCarthy*, 142 N.E.3d at 1104.

Courts have agreed that location data can reveal "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *Riley v. California*, 573 U.S. 373, 396 (2014) (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). And, when ALPR data is aggregated and retained over long periods of time, it can not only reveal details about a driver's past movements, but can also suggest where a driver may be in the future.[29] For instance, when *Ars Technica* ran the plate number from a random vehicle near a bar against Oakland Police Department ALPR data, it quickly determined that "the plate had been read 48 times over two years in two small clusters: one near the bar

[29] *See* N.J. Office of Att'y Gen., *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* 4 (effective Jan. 18, 2011) ("'Crime trend analysis' refers to the analytical process by which stored ALPR data is used . . . to predict when and where future crimes may occur[.]"), http://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; Steve Connor, *Surveillance UK: Why This Revolution Is Only the Start*, The Independent (Dec. 22, 2005) (discussing use of ALPR data to "build[] up the lifestyle of criminals—where they are going to be at certain times"), http://www.independent.co.uk/news/science/surveillance-uk-why-thisrevolution-is-only-the-start-520396.html.

and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[30]

Given the detailed personal information that location data reveals, the U.S. Supreme Court has acknowledged that individuals have a reasonable expectation of privacy in their location data over time. *See Carpenter*, 138 S. Ct. at 2217 (holding that law enforcement requests for six-month-old location information violate reasonable expectation of privacy).

IV. The tracking of license plate information chills protected First Amendment activity.

Scanning and recording the location of vehicles' license plates not only logs people's travels but also reveals their "privacies of life." *Carpenter*, 138 S. Ct. at 2217. So doing can allow law enforcement to make "inferences . . . that implicate expressive and associative rights." *McCarthy*, 142 N.E.3d at 1104.

Surveillance of such First Amendment-protected activities has a chilling effect on civil liberties and speech. The International Association of Chiefs of Police has cautioned that ALPR technology "risk[s] 'that individuals will become more cautious in the exercise of their protected rights of expression, protest,

---

[30] Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from The Cops*, Ars Technica (Mar. 24, 2015), https://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/.

association, and political participation because they consider themselves under constant surveillance.'" *Id.* at 1104 n.12 (quoting International Association of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, at 13 (Sept. 2009)).

Studies have confirmed that police surveillance has exactly this effect. In Muslim communities subject to surveillance, including ALPR surveillance, people have been less likely to attend mosques, express religious observance in public, engage in political activism, or exercise other constitutional rights.[31]

V. ALPR data is easily abused.

Databases of individuals' location information are ripe for abuse. As the California State Auditor recently observed in a report on ALPR data safeguards that was prompted by law enforcement routinely flouting state transparency and accountability requirements, "[a] member of law enforcement could misuse ALPR images to stalk an individual or observe vehicles at particular locations and events, such as doctors' offices or clinics and political rallies."[32] Similarly, the Northern

---

[31] *See generally* Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, CUNY School of Law, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (Mar. 11, 2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[32] Cal. State Auditor, *Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data*

California Regional Intelligence Center recognized in its privacy impact assessment that, "particularly when collected over an extended period of time," ALPR data can "be misused to infer information" other than location "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."[33]

Such concerns are not merely theoretical. Many examples of abuse involve law enforcement targeting people engaged in First Amendment-protected activity. In 2008 and 2009, for example, the Virginia State Police used ALPRs to collect license plates of vehicles attending Palin and Obama rallies, as well as Obama's inauguration, "to allow for some record of attendees."[34] In 2010, Immigration and Customs Enforcement enlisted local police to collect license plates of patrons at a

---

It Collects, Report No. 2019-118 (Feb. 2020) at 36, https://www.auditor.ca.gov/pdfs/reports/2019-118.pdf.

[33] Northern California Regional Intelligence Center, *Initial Privacy Impact Assessment for Automated License Plate Reader Technology* at 3, https://ncric.org/html/NCRIC%20ALPR%20PIA.pdf.

[34] Letter from First Sergeant Bobbie D. Morris to First Sergeant Alvin D. Blankenship on Division Seven Heat Operations (Mar. 18, 2009), http://www.thenewspaper.com/rlc/docs/2013/va-alpr.pdf.

gun show.[35] In 1998, a police officer in Washington, D.C. "pleaded guilty to extortion after looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners."[36]

Recent history is also rife with examples of police officers misusing driver data to target women. In 2011, a state audit in Minnesota revealed that fully half of state law-enforcement personnel had misused driving records.[37] A female Minnesota police officer received a million-dollar settlement after discovering that more than 100 police officers had searched for her photograph and address in the state driver's license database,[38] and a female attorney for the state's largest police union learned that her license information was wrongly accessed more than 700

---

[35] Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-showcustomers-license-plates-come-under-scrutiny-1475451302.

[36] Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates,* Wall St. J. (Sept. 29, 2012), http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576296.

[37] Chris Francescani, *License to Spy*, Medium (Dec. 1, 2014) https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[38] Sarah Mui, *Ex-Cop Awarded More Than $1 Million After Officers Illegally Accessed Her Driver's License Info*, ABA Journal (Nov. 9, 2012), https://www.abajournal.com/news/article/ex-cop_awarded_more_than_1_million_after_officers_illegally_accessed/.

times.[39] Similarly, in Florida an officer ran 19 separate unauthorized searches for a bank teller he was reportedly flirting with.[40] A former police chief and police officer in Ohio were indicted on charges that they misused a police database to look up "a lot of women," including "[a]n ex-mayor's wife."[41] And a police officer in New York who was indicted for conspiring to kidnap, rape, and cannibalize women was also charged with using a police database to "locate potential victims."[42]

CONCLUSION

ALPR systems collect an enormous trove of sensitive information about license plate locations over time. The Fairfax County Police Department can, and

---

[39] Debra Cassens Weiss, *Why Is This Lawyer's Driver's License So Popular?*, ABA Journal (Apr. 10, 2013), https://www.abajournal.com/news/article/why_is_this_lawyers_drivers_license_so_popular.

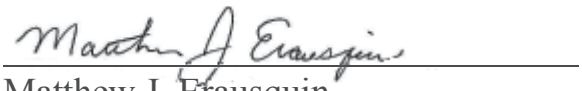
[40] Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, Orlando Sentinel (Jan. 22, 2013), http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_lawenforcement-officers-law-enforcers-misuse.

[41] Eric Lyttle, *Fairfield County Grand Jury Indicts Two Over Misuse of Database for Police, Columbus Dispatch* (Apr. 24, 2015), http://www.dispatch.

[42] Press Release, U.S. Attorney's Office, *Manhattan U.S. Attorney Announces Arrest of New York City Police Officer for Kidnapping Conspiracy and Illegally Accessing Federal Law Enforcement Database* (Oct. 25, 2012), https://archives.fbi.gov/archives/newyork/press-releases/2012/manhattan-u.s.-attorney-announces-arrest-of-new-york-city-police-officer-for-kidnapping-conspiracy-and-illegally-accessing-federal-law-enforcement-database.

does, link the license plate numbers collected to the specific individuals to whom vehicles are registered in order to investigate and solve crimes. Because the ALPR system provides the means for discerning personally identifiable information, the Virginia Government Data Collection and Dissemination Practices Act applies to ALPR data, and this Court should **AFFIRM.**

Respectfully Submitted,



Matthew J. Erausquin
VSB No. 65434
Consumer Litigation Associates, P.C.
1800 Diagonal Road, Suite 600
Alexandria, VA 22314
Tel: 703-273-7770
Fax: 888-892-3512
matt@clalegal.com

Naomi Gilens (*pro hac vice* pending)
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
Tel: 415-436-9333 x136
Fax: 415-436-9993
Email: naomi@eff.org

Rachel Levinson-Waldman (admitted *pro hac vice*)
Brennan Center for Justice at NYU Law School
1140 Connecticut Avenue NW, Suite 1150
Washington, DC 20036
Tel: 202-249-7193
Fax: 202-223-2683
levinsonr@brennan.law.nyu.edu

Counsel for Amici Curiae Electronic Frontier Foundation and Brennan Center for Justice

CERTIFICATE OF SERVICE AND COMPLIANCE

I hereby certify that on this May 15, 2020 a true and correct copy of the foregoing was served by email, to the following:

Edward S. Rosenthal
Lana M. Manitta
David C. Rohrbach
RICH ROSENTHAL BRINCEFIELD MANITIA DZUBIN & KROEGER, PLLC 500 Montgomery Street, Suite 600
Alexandria, Virginia 22314
Tel.: (703) 299-3440
Fax.: (703) 299-3441
ESRosenthal@RRBMDK.com
LMManitta@RRBMDK.com
DCRohrbach@RRBMDK.com

Eden Heilman
Jennifer Safstrom
AMERlCAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA, INC. 701 E. Franklin St., Suite 1412
Richmond, Virginia 23219
Tel.: (804) 644-8080
Fax.: (804) 649-2733
eheilman@acluva.org
jsafstrom@acluva.org

Counsel for Harrison Neal

Stuart A. Raphael
Trevor S. Cox
Matthew R. McGuire
HUNTON ANDREWS KURTH LLP
Riverfront Plaza, East Tower
951 East Byrd Street
Richmond, VA 23219
Tel.: (804) 788-8200
Fax.: (804) 788-8218
sraphae1@HuntonAK
comtcox@HuntonAK
commmcguire@HuntonAK.com

Elizabeth D. Teare
Karen L. Gibbons
Kimberly P. Baucom
FAIRFAX COUNTY ATTORNEY'S OFFICE
12000 Government Center Parkway
Fairfax, VA 22035
Tel.: (703) 324-2421
Fax.: (703) 324-2665
elizabeth.teare@fairfaxcounty.gov
karen.gibbons@fairfaxcounty.gov
kimberly.baucom@fairfaxcounty.gov

Counsel for Fairfax County Police Department; Colonel Edwin C Roessler, Jr., Chief of Police, Fairfax County Police Department

I further certify that I have caused to be filed 3 printed copies of the foregoing with the Clerk of this Court and an electronic copy, via VACES. I also certify the foregoing does not exceed 50 pages and that it complies with Rules 5:26 and 5:30 of the Rules of the Supreme Court of Virginia

Dated: May 15, 2020

MATTHEW J. ERAUSQUIN
VSB No. 65434