In The
Supreme Court of Virginia

RECORD NO. 170247

HARRISON NEAL,

Appellant,

v.

FAIRFAX COUNTY POLICE DEPARTMENT, ET AL.,

Appellees.

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

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

Counsel for Amicus Curiae

Rachel Levinson-Waldman
(pro hac vice pending)
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

In The

Supreme Court of Virginia

RECORD NO. 170247

HARRISON NEAL,

***Appellant*,**

v.

FAIRFAX COUNTY POLICE DEPARTMENT, ET AL.,

Appellees.

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

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

Counsel for Amicus Curiae

Rachel Levinson-Waldman
(pro hac vice pending)
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

CONSTITUTIONAL PROVISIONS

STATUTES

OTHER AUTHORITIES

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-privacy-concerns/2011/11/18/gIQAuEApcN_story.html 12

ALPR Products and Solutions > Mobile Plate Hunter – 900, ELSAG North America, http://elsag.com/mobile.htm.......... 12

Amici Curiae Br. of Cal. State Sheriffs' Assoc., *et al*., *ACLU v. Super. Ct.*, Cal. Sup. Ct. Case No. S227106, 6, 18 (May 3, 2016), https://www.eff.org/files/2016/08/03/Amici_brief_of_ca._sheriffs_ca_police_chiefs_and_ca._peace_officers_iso_respondent.pdf 19

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_law-enforcement-officers-law-enforcers-misuse 24

Benjamin Weiser, *2 Former New York Police Officers Misused Database, U.S. Says,* N.Y. Times (Oct. 22, 2014), http://www.nytimes.com/2014/10/23/nyregion/us-accuses-2-former-police-officers-of-abusing-a-confidential-database.html? 25

Brad Flora, *What Do the Cops Have on Me?*, Slate (Dec 4, 2007), http://www.slate.com/articles/news_and_politics/explainer/2007/12/what_do_the_cops_have_on_me.html. 25

Brian A. Reaves, Local Police Departments, 2013: Equipment and Technology, Bureau of Justice Statistics, NCJ 248767 (July 2015), https://www.bjs.gov/content/pub/pdf/lpd13et.pdf 10

Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335....... 23, 24

Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime as well as Terrorism*, Reuters (June 21, 2013), http://www.reuters.com/article/usa-ny-surveillance-idUSL2N0EV0D220130621 10

Computers in Police Cars, Baltimore Sun (Nov. 28, 1994), http://articles.baltimoresun.com/1994-11-28/news/1994332162_1_patrol-officers-computer-police-cars 10

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 21

Cynthia Lum, et al, *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment*, Center for Evidence Based Crime Policy (Sept. 2010), http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf 22

Cyrus Farivar, *Louisiana Governor Vetoes License Plate Reader Bill, Citing Privacy Concerns*, ArsTechnica (June 20, 2015), https://arstechnica.com/tech-policy/2015/06/louisiana-governor-vetoes-license-plate-reader-bill-citing-privacy-concerns/ 23

Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from The Cops*, Ars Technica (Mar. 24, 2015), http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops 19, 20

Dave Maass, Mystery Show Debunks License Plate Privacy "Myth," EFF (June 15, 2015), https://www.eff.org/deeplinks/2015/06/mystery-show-podcast-debunks-license-plate-privacy-myth 25

Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302........... 24

Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, Columbus Dispatch (April 24, 2015), http://www.dispatch.com/content/stories/local/2015/04/23/sugar-grove-police-indicted.html 25

Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, Minneapolis Star Tribune (Aug. 17, 2012), http://www.startribune.com/local/minneapolis/166494646.html 19

Executive Office of the President, *Big Data and Privacy: A Technological Perspective* (May 2014), http://cvt.engin.umich.edu/wp-content/uploads/sites/173/2014/10/pcast_big_data_and_privacy_-_may_2014.pdf. 9

FTC's Ramirez: We're Expanding Definition of PII, IAPP (Aug. 24, 2016), https://iapp.org/news/a/ftcs-ramirez-were-expanding-definition-of-pii/ 8

George Joseph, *What Are License-Plate Readers Good For?*, The Atlantic CityLab (Aug. 5, 2016), http://www.citylab.com/crime/2016/08/what-are-license-plate-readers-good-for/492083/ 14

Intn'l Assoc. of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers (Sept. 2009), http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_ Assessment.pdf 20, 21

James Bridle, *How Britain Exported Next-Generation Surveillance*, Matter (Dec 18, 2013), https://medium.com/matter/how-britain-exported-next-generation-surveillance-d15b5801b79e 18

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 13

Jeremy Gillula & Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, EFF (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data 26

Jessica Rich, *Keeping Up with the Online Advertising Industry*, FTC (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry 8

Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" With Real-Time CCTV, License Plate Monitoring*, Fast Company (Aug. 8, 2012), https://www.fastcompany.com/3000272/ nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito 10

Neal Ungerleider, *This May Be The Most Vital Use of "Big Data" We've Ever Seen*, Fast Company (July 12, 2013), http://www.fastcolabs.com/3014191/this-may-be-the-most-vital-use-of-big-data-weve-ever-seen 9

Oppn. Br. of City of Los Angeles, *ACLU v. Super. Ct.*, 29, Cal. Ct. App. Case No. B259392 (Nov. 26, 2014), https://www.eff.org/files/2016/08/03/brf.calapp.city_opp_to_petition_for_writ_of_mandate.pdf 18

Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, The Guardian (Oct. 25, 2010), http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance, ... 15

Privacy Impact Assessment for Texas Dept. of Public Safety (Sept. 2014), http://www.txdps.state.tx.us/administration/crime_records/pages/LPRPIA.pdf 18

Rachel Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 Emory L.J. 537 (2017) 3

Report from Officer Cheryl Paris, Central Marin Police Authority, et al., to Bay Area UASI Approval Authority, *Re: Automated License Plate Reader Pilot Report Out,* Bay Area Urban Areas Security Initiative (July 14, 2016) http://bauasi.org/sites/default/files/resources/071416%20Agenda%20Item%206%20ALPR%20Pilot%20Report%20Out.pdf 14

Report of the VALC to the Governor & General Assembly of Virginia, 2 House & Senate Documents, S. Doc. 27 (1976) 5

Shawn Musgrave, *A Vast Hidden Surveillance Network Runs across America, Powered by the Repo Industry*, Boston Globe (Mar. 5, 2014), http://www.betaboston.com/news/2014/03/05/a-vast-hidden-surveillance-network-runs-across-america-powered-by-the-repo-industry 26

State of New Jersey, Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (Effective January 18, 2011), http://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf 17

Steve Connor, *Surveillance UK: Why this Revolution Is Only the Start*, The Independent (Dec. 21, 2005), http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html 17

Tim Cushing, *FOIA Request on Effectiveness of License Plate Readers Greeted with A Blank Stare By Virginia Police Department*, TechDirt (June 23, 2014), https://www.techdirt.com/articles/20140604/12404427462/foia-request-effectiveness-license-plate-readers-greeted-with-blank-stare-virginia-police-department.shtml 12, 14

Tom Jackman, *Despite Cuccinelli's Advice, N.Va. Police Still Maintaining Databases of License Plates*, Wash. Post (Jan. 16, 2014), https://www.washingtonpost.com/local/despite-cuccinellis-advice-nva-police-still-maintaining-databases-of-license-plates/2014/01/16/055ec09a-7e38-11e3-9556-4a4bf7bcbd84_story.html 15

Use of License-Plate Scanners Expands amid Privacy Concerns, Court Battles, Fox News (Sept. 2, 2015), http://www.foxnews.com/politics/2015/09/02/use-license-plate-scanners-increase-amid-more-concerns-court-battles-over.html 15

Vigilant Solutions, *Our Story*, https://vigilantsolutions.com/about 13

Virginia: Cops Spied on Motorists at Political Rallies, The Newspaper (Oct. 14, 2013), http://www.thenewspaper.com/news/42/4232.asp 14

INTEREST OF *AMICI CURIAE*

The Electronic Frontier Foundation (EFF) is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for more than 25 years. With more than 37,000 active dues-paying members nationwide, including about 900 in Virginia, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF has filed *amicus* briefs with the Supreme Court in cases involving the application of constitutional principles to emerging technologies, including *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015); *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012); and *City of Ontario v. Quon*, 560 U.S. 746 (2010). 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 a case specifically involving Automated License Plate Readers (ALPRs), currently pending in the California Supreme Court. *See ACLU Foundation of Southern Cal. & EFF v. Super. Ct*, Case No. S227106 (Cal. Sup. Ct. 2016).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues 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 *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (U.S. June 5, 2017) (No. 16-402); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 569 (2016); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *petition for cert. filed*, No. 17-2 (June 27, 2017); *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); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015). The Brennan

Center also publishes scholarship on the privacy of personal data, including automatic license plate reader data; *see* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 Emory L.J. 537 (2017).

Amici are increasingly concerned about the mass collection of data on the location of Americans, whether through the use of cell phone tracking technologies, GPS devices, or ALPRs. *Amici* write to provide background to the Court on the privacy implications of location data as well as its potential for abuse.

STATEMENT OF THE CASE

Amici concur with the Statement of the Case set forth in Appellant Neal's opening brief.

STATEMENT OF FACTS

Amici concur with the Statement of Facts set forth in Appellant Neal's opening brief.

STANDARD OF REVIEW

Amici concur with the Standard of Review set forth in Appellant Neal's opening brief.

ASSIGNMENTS OF ERROR

Amici concur with the Assignments of Error set forth in Appellant Neal's opening brief.

ARGUMENT

Virginia’s Government Data Collection & Dissemination Practices Act (the “Act”) requires purging of data collected by Fairfax County Police Automated License Plate Readers (ALPRs). ALPR data should be considered “personal information” under the Act. Because it can reveal a wealth of private and personal information about where people travel, it is precisely the type of data the Virginia General Assembly was concerned about when it adopted the Act in 1976. ALPR data can be used to “describe[ ], locate[ ], and index[ ]” an individual’s location at a given point in time in the past and may allow predictions about where that person could be in the future. Va. Code Ann. § 2.2-3801. As such it creates a “record of his presence,” *id*., that police can use to place a person at a specific place and time, even if there is no reason to suspect that person of criminal activity. Because ALPR data implicates an individual’s privacy interest and is collected in an “information system,” indexed via “identifiable particulars” that are easily tied to an individual, this data is covered by the Act. *Id.* As such, this Court should hold that ALPR data collected on non-criminals is “personal information,” and order that data to be purged pursuant to the Act. Va. Code Ann. § 2.2-3806.

I. ALPR Systems Collect Data Covered by the Act

A. <u>Legislative History and the Former Attorney General's Advisory Opinion Show the Act Applies to ALPR Data</u>

Although the Act was enacted well before the proliferation of tools like ALPRs that are capable of mass and indiscriminate data collection, the Act's drafters likely would have considered ALPR data to be "personal information" covered by the Act.

As recognized by this Court, the Act was prompted by the "proliferation in the use of automated data processing equipment . . . that has enabled government and private industry to compile detailed information on individuals in every area of personal activity." *Hinderliter v. Humphries*, 224 Va. 439, 442 (1982). The Virginia Advisory Legislative Council, tasked at the time with examining the impact of data collection on privacy, acknowledged 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.* (citing *Report of the VALC to the Governor & General Assembly of Virginia*, 2 House & Senate Documents, S. Doc. 27 at 11 (1976)). ALPR data clearly fits within the types of personal data of concern to the General Assembly because it allows the government to monitor patterns of movements associated with identified vehicles, and to easily link that data to the "personal activities" of specific Virginia residents using data readily available through "intercommunicating" databases.

Former Virginia Attorney General Kenneth Cuccinelli agreed with this interpretation of the Act, determining that ALPR data falls within the Act's statutory definition of "personal information." 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).[1] In an advisory opinion, he concluded this data could, for example, "assist in locating an individual data subject, documenting his movements, or determining his personal property holdings." *Id*. He determined that no exemption under the Act applied to stored ALPR data that wasn't immediately linked to a criminal investigation, because "[i]ts future value to any investigation of criminal activity is wholly speculative." *Id*. He concluded that ALPR data collected through this "passive" use of the technology "may not lawfully be collected" pursuant to the Act. *Id*.

[1] https://www.thenewspaper.com/rlc/docs/2013/va-stopalpr.pdf.

B. **Other Agencies Tasked With Protecting Personal Data Recognize the Impact of "Big Data" and Data Aggregation on Privacy and Take an Expansive View of the Term Personal Information**

In contrast to Cuccinelli's advisory opinion, the Circuit Court interpreted the term "personal information" narrowly to find ALPR data were not covered by the Act. The lower court looked to cases from very different contexts that addressed privacy interests implicated by a single, isolated view of a license plate to erroneously determine that "license plate numbers are not personal information." *Neal v. Fairfax County Police Department, et al.*, Case No. CL-2015-5902, 6 (Nov. 18, 2016). However, the lower court's limited examination is inconsistent with modern, expansive definitions of personal data that recognize the impact of data aggregation over time and of easy access to multiple data sources linked to an individual.

In the past few years, as it has become clear how easy it is to aggregate seemingly innocuous and isolated pieces of data from disparate sources to create a full and revealing picture of an individual, agencies and organizations that work on privacy issues have broadened their definition of "personally identifying information." For example, the Federal Trade Commission (FTC) now regards "data as personally identifiable when it can be *reasonably linked* to a particular person, computer, or device."[2] Former FTC Chairwoman Edith Ramirez concluded, "[i]n many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test."[3] Likewise, the Director of the FTC's Bureau of Consumer Protection, Jessica Rich, observed:

"[e]ven without a name, you can learn a lot about people if you use a persistent identifier to track their activities over time."[4] Similar to an identifier like the MAC address on a cell phone,[5] license plates are persistent identifiers—they identify a particular vehicle that is easily linked to the vehicle's owner and can be tracked over time.

Similarly, the Executive Office of the President recognized the privacy issues associated with the aggregation of data from multiple sources ("big

[2] *FTC's Ramirez: We're Expanding Definition of PII*, IAPP (Aug. 24, 2016) (emphasis added), https://iapp.org/news/a/ftcs-ramirez-were-expanding-definition-of-pii/.

[3]*Id*.

[4] Jessica Rich, *Keeping Up with the Online Advertising Industry*, FTC (Apr. 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[5] "[E]very smart phone contains a unique identifier known as a MAC address . . . [that] remains the same regardless of the network and transmits even without actually connecting to the Internet." *See* Adam Tanner, *Here's How Others Can Easily Snoop On Your Cell Phone*, Forbes (Feb. 18, 2014) (quoting Latanya Sweeney, former chief technologist at the FTC), http://www.forbes.com/sites/adamtanner/2014/02/18/heres-how-others-can-easily-snoop-on-your-cell-phone/#dc19fd3cd336.

data"), noting that analytics "can be applied to those data, ultimately to make inferences and draw conclusions" about individuals. This allows "non-obvious and sometimes private information" to be "derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues."[6] For example, purchasing habits may allow marketers to determine a woman is pregnant even before she tells her friends and family.[7] Twitter posts can signal prescription medication abuse.[8] And social media behavior may reveal early signs of suicidal thoughts among veterans.[9]

Like private companies, law enforcement agencies are increasingly relying on data analytics to process small pieces of data from disparate

[6] Executive Office of the President, *Big Data and Privacy: A Technological Perspective* ix (May 2014), http://cvt.engin.umich.edu/wp-content/uploads/sites/173/2014/10/pcast_big_data_and_privacy_-_may_2014.pdf.

[7] See, e.g., Kashmir Hill, How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, Forbes (Feb. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#654593b634c6.

[8] Abeed Sarkar et al., *Social Media Mining for Toxicovigilance: Automatic Monitoring of Prescription Medication Abuse from Twitter*, 39 Drug Safety 231 (2016), https://link.springer.com/article/10.1007%2Fs40264-015-0379-4.

[9] Neal Ungerleider, *This May Be The Most Vital Use of "Big Data" We've Ever Seen*, Fast Company (July 12, 2013), http://www.fastcolabs.com/3014191/this-may-be-the-most-vital-use-of-big-data-weve-ever-seen.

sources. For example, the New York Police Department's surveillance network integrates information from surveillance cameras, license plate readers, radiation detectors, 911 calls, criminal records, and other databases. Officers can bring up a "massive personal history . . . from any suspect in a matter of seconds."[10] Even officers in smaller jurisdictions can use their squad car computer systems 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 U.S. Department of Justice'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."[11] Departments serving

[10] Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" With Real-Time CCTV, License Plate Monitoring*, Fast Company (Aug. 8, 2012), https://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito. *See also* Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime as well as Terrorism*, Reuters (June 21, 2013), http://www.reuters.com/article/usa-ny-surveillance-idUSL2N0EV0D220130621.

[11] Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology*, Bureau of Justice Statistics, NCJ 248767, 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.

larger populations have in-car access to even more data, including the National Crime Information Center's 21 individual property and person databases and more than 100 other data sources.[12]

As the lower court recognized, protected data are not limited to the categories specifically included within the Act's definition of "personal information." *Neal*, Case No. CL-2015-5902 at 5. Given easy access to data from multiple sources as well as the power of software to reveal sensitive and private information from data that, disaggregated, may not be considered sensitive, courts and governments should take an expansive view of what is considered "personal information."

II. ALPR Systems Collect and Store Massive Amounts of Sensitive Data on Law-Abiding People

ALPRs automatically and indiscriminately scan and record the license plate number and the time, date, and precise location of every passing vehicle, along with an image of the vehicle and its immediate surroundings.

[12] National Crime Information Center, FBI, https://www.fbi.gov/services/cjis/ncic; 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/.

The images captured by the systems can reveal not just the plate itself, but also the vehicle's occupants.[13]

This collection is indiscriminate. Officers turn on vehicle-mounted ALPRs at the start of their shifts, and the devices scan plates continuously until the officers turn off the ALPRs at the end of their shifts. Fixed ALPRs have a continuous connection to the ALPR server and are never turned off. By scanning every license plate that comes into view—scans of up to 1,800 plates per minute[14]—ALPRs collect an enormous volume of data. In 2014, Fairfax County alone had 2,731,429 plate scans in its database.[15] By 2011, District of Columbia ALPR cameras were capturing more than a million data points a month.[16] And since 2014, two law enforcement agencies in

[13] *See* Ali Winston, *License Plate Readers Tracking Cars*, SF Gate (June 25, 2013) (license plate image clearly showed man and his daughters stepping out of vehicle in their driveway), http://www.sfgate.com/bayarea/article/License-plate-readers-tracking-cars-4622476.php.

[14] *See ALPR Products and Solutions > Mobile Plate Hunter – 900*, ELSAG North America, http://elsag.com/mobile.htm.

[15] Tim Cushing, *FOIA Request on Effectiveness of License Plate Readers Greeted with A Blank Stare By Virginia Police Department*, TechDirt (June 23, 2014), https://www.techdirt.com/articles/20140604/12404427462/foia-request-effectiveness-license-plate-readers-greeted-with-blank-stare-virginia-police-department.shtml.

[16] 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-privacy-concerns/2011/11/18/gIQAuEApcN_story.html.

Los Angeles, California, have been collecting data on 3 million cars every week.[17]

Private vendor ALPR databases—which are also accessible to law enforcement—dwarf these agency-maintained databases. One such vendor, Vigilant Solutions, employs private contractors to collect its own plate scan data, which it then merges with data from partner government agencies.[18] Vigilant says its dataset includes over 5 billion scans and is growing at a rate of 120 million data points a month.[19]

Yet only a tiny fraction of these scans show any link to vehicle registration issues or criminal activity. Public records requests in California have revealed, for example, that out of nearly 4 million plates scanned by a Northern California regional agency, only 985 plates—0.025%—were

[17] *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.

[18] Vigilant Solutions, *Our Story* ("A hallmark of the Vigilant solution is the ability for agencies to share real-time data nationwide amongst over 1,000 agencies and tap into our exclusive commercial LPR database of over 5 billion vehicle detections."), https://vigilantsolutions.com/about.

[19] *Id.*; *see also* Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, The Atlantic (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436.

linked to criminal activity.[20] That means 99.075% of the data—3,995,109 plate scans—were collected from people whose vehicles provided no cause for suspicion. Similar rates were recorded in New York (0.01%) and North Carolina (0.08%).[21] Although the Fairfax Police Department has said it does not maintain records on its own ALPR hit rate,[22] in a 2009 joint project with the Virginia State Police, it had a recovery rate of just 0.6%.[23]

Despite the fact that the vast majority of this location data is collected from law-abiding individuals, agencies often retain the data for years in massive databases managed by the police or private companies and

[20] *See* Report from Officer Cheryl Paris, Central Marin Police Authority, et al., to Bay Area UASI Approval Authority, *Re: Automated License Plate Reader Pilot Report Out,* Bay Area Urban Areas Security Initiative (July 14, 2016), http://bauasi.org/sites/default/files/resources/071416%20Agenda%20Item%206%20ALPR%20Pilot%20Report%20Out.pdf. *See also You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, ACLU 13-15 (July 2013) (noting that typically, only about 0.2% of plate scans are linked to suspected crimes or vehicle registration issues), https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record.

[21] George Joseph, *What Are License-Plate Readers Good For?*, The Atlantic CityLab (Aug. 5, 2016), http://www.citylab.com/crime/2016/08/what-are-license-plate-readers-good-for/492083/.

[22] Tim Cushing, *FOIA Request On Effectiveness of License Plate Readers Greeted with A Blank Stare by Virginia Police Department*, TechDirt (June 23, 2014), https://www.techdirt.com/articles/20140604/12404427462/foia-request-effectiveness-license-plate-readers-greeted-with-blank-stare-virginia-police-department.shtml.

[23] *Virginia: Cops Spied on Motorists at Political Rallies*, The Newspaper (Oct. 14, 2013), http://www.thenewspaper.com/news/42/4232.asp.

shared widely with other federal, state, and local law enforcement agencies.[24] These databases allow officers to query a car's past locations for years into the future.

III. Location Data Reveals Private and Personal Details About Individuals

As even the FBI has recognized, ALPRs pose risks to privacy and civil liberties.[25] They can be used to scan and record vehicles at a lawful protest or house of worship; track all cars that enter or leave a town;[26] gather information about certain neighborhoods[27] or

[24] *See, e.g.*, Tom Jackman, *Despite Cuccinelli's Advice, N.Va. Police Still Maintaining Databases of License Plates*, Wash. Post (Jan. 16, 2014) ("In 2012, many police departments in the Washington area signed a memorandum of understanding to share their databases with each other."), https://www.washingtonpost.com/local/despite-cuccinellis-advice-nva-police-still-maintaining-databases-of-license-plates/2014/01/16/055ec09a-7e38-11e3-9556-4a4bf7bcbd84_story.html.

[25] Kim Zetter, *Even the FBI Had Privacy Concerns on License Plate Readers*, Wired (May 15, 2015), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers.

[26] For example, Ocean City, Maryland officials have said they will use license plate readers at "all major entry points." *Use of License-Plate Scanners Expands amid Privacy Concerns, Court Battles*, Fox News (Sept. 2, 2015), http://www.foxnews.com/politics/2015/09/02/use-license-plate-scanners-increase-amid-more-concerns-court-battles-over.html.

[27] *See* Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, The Guardian (Oct. 25, 2010), http://www.guardian.co.uk/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance.

organizations;[28] or place political activists on “hot lists” so that their movements trigger alerts.

Courts have recognized the sensitive nature of location data, especially when collected and stored over time. The U.S. Supreme Court held that location data reveals “a wealth of detail about [a person’s] familial, political, professional, religious, and sexual associations.” *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)). Likewise, the Massachusetts Supreme Judicial Court recognized that historical location data gives police access to something they would never have with traditional law enforcement investigative methods: the ability “to track and reconstruct a person’s past movements.” *Commonwealth v. Augustine*, 467 Mass. 230, 254 (2014). And nearly 30 years ago, the Oregon Supreme Court rejected law enforcement arguments that monitoring a car’s location violated no privacy interests purely because that car was traveling on public roads. As the court explained, that would mean “no movement, no location and no conversation in a ‘public place’ would in any measure be secure from the prying of the government. . . . That is nothing short of a staggering

[28] *See* Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012), http://www.ap.org/Content/AP-In-The-News/2012/Newark-mayor-seeks-probe-of-NYPD-Muslim-spying.

limitation upon personal freedom." *State v. Campbell*, 306 Or. 157, 172 (1988).

Although ALPRs do not generally collect data as detailed as GPS tracking, their data can be just as revealing. Scientists working with location data have determined that, given humans' unique patterns of travel, "even coarse datasets provide little anonymity."[29] These researchers found they could uniquely characterize 50% of people using only two randomly chosen time and location data points.[30] This means even a small amount of ALPR data could reveal sensitive information about an individual. When ALPR data is aggregated and retained for long periods of time, it can not only reveal 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.[31]

[29] Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature Scientific Reports 3, Art. No. 1376 (2013), http://www.nature.com/articles/srep01376.

[30] *Id*.

[31] State of New Jersey, Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (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. 21, 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-this-revolution-is-only-the-start-520396.html.

It can even be used to find drivers who are travelling together.[32] Law enforcement agencies across the country recognize the power of ALPR data to identify individuals. The Los Angeles Police Department has said that ALPR data can be used "to identify driving patterns of a particular individual in order to locate that person and perhaps do him or her harm."[33] 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."[34] And California police and sheriffs' organizations have stated that the information in ALPR databases "may include or lead to unsuspecting individual drivers' potentially private

[32] James Bridle, *How Britain Exported Next-Generation Surveillance*, Matter (Dec 18, 2013), https://medium.com/matter/how-britain-exported-next-generation-surveillance-d15b5801b79e.

[33] *See* Oppn. Br. of City of Los Angeles, *ACLU v. Super. Ct.*, 29, Cal. Ct. App. Case No. B259392 (Nov. 26, 2014), https://www.eff.org/files/2016/08/03/brf.calapp.city_opp_to_petition_for_writ_of_mandate.pdf.

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

and sensitive information," and "can lead to identification of those persons/witnesses associated" with plate scans.[35]

This identification has already occurred. In August 2012, the Minneapolis *Star Tribune* published a map displaying the 41 locations where license plate readers had recorded the Minneapolis mayor's car in the preceding year.[36] Using Oakland Police Department ALPR data obtained through a public records request, the online technology publication *Ars Technica* was able to correctly guess the block where an Oakland, California, city council member lived after less than a minute of research.[37] *Ars Technica* was also able to run the plate number from a random vehicle near a bar against the Oakland data to determine "the plate had been read 48 times over two years in two small clusters: one near the

[35] *See* Amici Curiae Br. of Cal. State Sheriffs' Assoc., *et al.*, *ACLU v. Super. Ct.*, Cal. Sup. Ct. Case No. S227106, 6, 18 (May 3, 2016), https://www.eff.org/files/2016/08/03/Amici_brief_of_ca._sheriffs_ca_police_chiefs_and_ca._peace_officers_iso_respondent.pdf.

[36] Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, Minneapolis Star Tribune (Aug. 17, 2012), http://www.startribune.com/local/minneapolis/166494646.html.

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

bar and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[38]

ALPRs do not just record license plate and location *data*. Every scan also includes a photograph of the plate and vehicle. These photographs may include bumper stickers, which could reveal information about a person's political or social views, and may also include recognizable views of the vehicle's occupants.[39] One California resident, Michael Katz-Lacabe, discovered that his ALPR records included a photograph of himself and his two young daughters exiting their car when it was parked in their driveway.[40]

Police tracking of the public's movements can have 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, association, and political participation because they

[38] *Id*.

[39] Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* 6, 11 (Sept. 2009), http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.

[40] Ali Winston, *License-plate Readers Let Police Collect Millions of Records on Drivers*, Center for Investigative Reporting (June 26, 2013), http://cironline.org/reports/license-plate-readers-let-police-collect-millions-records-drivers-4883.

consider themselves under constant surveillance."[41] And, indeed, communities that have faced excessive police surveillance that has included ALPR tracking have feared engaging in political activism, expressing religious observance, and exercising other basic constitutional rights.[42]

IV. Americans—Including Fairfax County Residents—Recognize the Privacy Implications of Long-Term ALPR Data Storage

People instinctively recognize that ALPR data stored for periods of time burdens privacy interests. In 2009, the Virginia State Police stated, "[t]he retention of LPR data may result in a negative impact on public/legislators' perception of this program."[43] A 2010 survey of Fairfax County residents bears that out. The survey revealed that a "majority of respondents (53.4%) consider LPR data to be private information," and 46% of respondents believed the data should not be stored at all or "only

[41] Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* 13 (Sept. 2009), http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.

[42] *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.

[43] 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.

for a short period of time."[44] The survey's researchers recognized this was a remarkably high number, given that other survey questions indicated most respondents were not familiar with license plate scanning technology and "most community members have not heard any arguments made by privacy advocates with respect to LPR."[45] The study also noted that "comparatively few respondents supported the uses of both LPRs and of saved LPR data that might impact 'average' members of the community,"[46] indicating respondents were concerned about the use of ALPRs to record data on innocent people.

Virginia residents are not alone. After the Minneapolis *Star Tribune* published its story illustrating how license plate readers tracked the mayor's movements, there was intense public debate on appropriate data retention policies. At a public hearing, a state legislator and former police chief stated, "even though technology is great and it helps catch the bad guys, I

[44] Cynthia Lum, et al, *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment*, Center for Evidence Based Crime Policy 87-88 (Sept. 2010), http://cebcp.org/wp-content/evidence-based-policing/LPR_FINAL.pdf.

[45] *Id*. at 87.

[46] *Id.* at 90.

don't want the good guys being kept in a database."[47] In 2015, Louisiana Governor Bobby Jindal vetoed ALPR legislation that would have imposed a 60-day retention limit on ALPR data. In a statement, he expressed his concern that this "personal information . . . would be retained in a central database . . . for a period of time regardless of whether or not the system detects that a person is in violation of vehicle insurance requirements."[48] He stated that ALPR systems "pose a fundamental risk to personal privacy and create large pools of information belonging to law abiding citizens."[49]

V. ALPR Data is Ripe for Abuse

Past examples of improper and unlawful police use of driver and vehicle data suggest ALPR data will also be misused. For example, in 1998, a Washington, D.C., police officer "pleaded guilty to extortion after looking up the plates of vehicles near a gay bar and blackmailing the vehicle

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

[48] Cyrus Farivar, *Louisiana Governor Vetoes License Plate Reader Bill, Citing Privacy Concerns*, ArsTechnica (June 20, 2015), https://arstechnica.com/tech-policy/2015/06/louisiana-governor-vetoes-license-plate-reader-bill-citing-privacy-concerns/.

[49] *Id.*

owners."[50] In 2008, the Virginia State Police used ALPRs to scan the plates of all vehicles entering facilities for Palin and Obama rallies.[51] In 2010, Immigration and Customs Enforcement enlisted local police officers to use ALPRs to gather information about gun-show customers.[52] And a 2011 state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[53] Many of the recorded examples of database misuse—both in Minnesota and in other areas—involve male officers targeting women. For example, in Florida, an officer breached the driver and vehicle database to "look up a local bank teller he was reportedly flirting with."[54] In

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

[51] 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.

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

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

[54] 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_law-enforcement-officers-law-enforcers-misuse. *See also* Kim Zetter, *Cops Trolled Driver's License Database for Pic of Hot Colleague*, Wired (Feb 23, 2012), https://www.wired.com/2012/02/cop-database-abuse/.

Ohio, officers looked through the database to find information on an ex-mayor’s wife, along with council people and spouses. In Illinois, a police sergeant suspected of murdering two ex-wives used police databases to check up on one of his wives before she disappeared.[55] None of these database searches were prompted by a traffic stop or criminal suspicion.[56]

Officers may also access data to provide information to others unaffiliated with the police. For example, in 2014, two New York police officers were indicted after they were reportedly paid to tap into a confidential law enforcement database to obtain personal information about potential witnesses.[57] And police have provided license plate data to reporters.[58]

[55] Brad Flora, *What Do the Cops Have on Me?*, Slate (Dec 4, 2007), http://www.slate.com/articles/news_and_politics/explainer/2007/12/what_do_the_cops_have_on_me.html.

[56] Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, Columbus Dispatch (April 24, 2015), http://www.dispatch.com/content/stories/local/2015/04/23/sugar-grove-police-indicted.html.

[57] Benjamin Weiser, *2 Former New York Police Officers Misused Database, U.S. Says,* N.Y. Times (Oct. 22, 2014), http://www.nytimes.com/2014/10/23/nyregion/us-accuses-2-former-police-officers-of-abusing-a-confidential-database.html?.

[58] Dave Maass, *Mystery Show Debunks License Plate Privacy “Myth*,” EFF (June 15, 2015), https://www.eff.org/deeplinks/2015/06/mystery-show-podcast-debunks-license-plate-privacy-myth.

Data also suggest that ALPRs disproportionately impact people of color and the poor. For example, ALPRs attached to Oakland, California, police vehicles disproportionately captured license plates in minority neighborhoods, as compared to neighborhoods with a higher density of white families.[59] And some repossession companies that rely on ALPRs to find car owners who are behind on payments expressly target "low-income housing developments, since it's likely that a disproportionate number of residents in those areas are behind on auto payments, their cars ripe for repossession."[60] As noted above, these private databases are often accessible to law enforcement.

[59] Jeremy Gillula & Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, EFF (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[60] Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, The Atlantic (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/. *See also* Shawn Musgrave, *A Vast Hidden Surveillance Network Runs across America, Powered by the Repo Industry*, Boston Globe (Mar. 5, 2014), http://www.betaboston.com/news/2014/03/05/a-vast-hidden-surveillance-network-runs-across-america-powered-by-the-repo-industry.

CONCLUSION

ALPR data reveals a highly detailed history of our movements, associations, and habits. The Fairfax County Police Department greatly burdens our location privacy by gathering and storing ALPR data. So the Virginia Government Data Collection and Dissemination Practices Act applies to ALPR data, and requires the Fairfax County Police Department to purge its ALPR data.

Dated: August 1, 2017

Respectfully submitted by:

Matthew J. Erausquin

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

Counsel of Record for Amici Curiae Electronic Frontier Foundation and Brennan Center for Justice at NYU Law School

**pro hac vice* application pending

Adam Schwartz*
Electronic Frontier
Foundation
815 Eddy Street
San Francisco, CA
94109
Tel: 415-463-9333
Fax: 415-436-9993
adam@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

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

Counsel for Amicus Curiae Brennan Center for Justice at NYU Law School

CERTIFICATE OF SERVICE AND COMPLIANCE

I hereby certify that on August 1, 2017, three (3) printed copies were hand-delivered to the Clerk of this Court and an electronic copy was filed, via VACES. An electronic copy was served, via email, upon:

Leslie C. Mehta
Hope R. Amezquita
American Civil Liberties Union Foundation of Virginia, Inc.
701 East Franklin Street, Suite 1412
Richmond, Virginia 23219
Tel: (804) 644-8080
Email: lmehta@acluva.org
Email: hamezquita@acluva.org

Edward S. Rosenthal
Jessica R. Killeen
Rich Rosenthal Brincefield Manitta Dzubin & Kroeger, LLP
201 North Union Street, Suite 230
Alexandria, Virginia 22314
Tel: (703) 299-3440 x 208
Email: ESRosenthal@rrbmdk.com
Email: JRKilleen@rrbmdk.com

Counsel for Appellant Neal

Elizabeth Doyle Teare
Karen L. Gibbons
Kimberly P. Baucom
Office of the County Attorney
12000 Government Center Parkway, Suite 549
Fairfax, Virginia 22035
Tel: (703) 324-2421
Email: elizabeth.teare@fairfaxcounty.gov
Email: karen.gibbons@fairfaxcounty.gov
Email: kimberly.baucom@fairfaxcounty.gov

Counsel for Appellee Fairfax County Police Department, et al.

I further certify that the foregoing does not exceed fifty (50) pages and that I have otherwise complied with Rules 5:26 and 5:30 of the Rules of the Supreme Court of Virginia.

Dated: August 1, 2017

Matthew J- Erausquin
MATTHEW J. ERAUSQUIN
VSB No. 65434