VIRGINIA: IN THE CIRCUIT COURT OF THE COUNTY OF FAIRFAX

HARRISON NEAL,	)
Plaintiff,	)
	)
v.	)
	)
FAIRFAX COUNTY POLICE DEPARTMENT, and COLONEL EDWIN C. ROESSLER, JR., chief of Police, Fairfax County Police Department.	) **Case No. CF-2015-5902**
Defendants.	)

BRIEF OF ELECTRONIC FRONTIER FOUNDATION (EFF)[1] AS AMICUS CURIAE IN SUPPORT OF PLAINTIFF

ARGUMENT

The Government Data Collection & Dissemination Practices Act protects data collected by Fairfax County Police ALPRs. This data can reveal private and personal information and can be used to "describe[ ], locate[ ], and index[ ]" an individual at a precise point in time. Va. Code Ann. § 2.2-3801. It is collected in an "information system," indexed via "identifiable particulars," and it creates a "record of [an individual's] presence," *id.*, that police can query at any time, even if there is no reason to suspect that person of criminal activity.

I. ALPRs Collect and Store Massive Amounts of Sensitive Data on Law-Abiding People

ALPRs automatically 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 and sometimes even its occupants.[2] This collection is indiscriminate: an officer turns the vehicle-mounted ALPR on at the start of the shift, and the devices scan plates continuously until the officer turns off the ALPR at the end of the shift. Fixed ALPRs have a continuous connection to the ALPR server and are never turned off.

---

[1] The interest of *amicus* is stated in EFF's motion for leave to file this brief, filed on July 29, 2016.
[2] *See* Ali Winston, *License Plate Readers Tracking Cars*, SF Gate (June 25, 2013) http://www.sfgate.com/bayarea/article/License-plate-readers-tracking-cars-4622476.php.

Not surprisingly, such indiscriminate collection results in the creation of vast databases. By scanning every license plate that comes into view—scans of up to 1,800 plates per minute[3]—ALPRs collect an enormous volume of data. For example, using only three fixed cameras, a regional law enforcement agency in Northern California was able to scan 3,232,405 license plates in just three months.[4] And two law enforcement agencies in Los Angeles, California are able to record almost the same amount of plate scan data—data on 3 million cars—every week.[5]

Yet only a tiny fraction of these scans shows any link to vehicle registration issues or criminal activity. Public records requests in California have revealed, for example, that of the 3.2 million plates scanned by the Northern California regional agency, only 720 plates—0.022%—were linked to criminal activity.[6] That means 99.088% of the data—3,231,685 plate scans—was collected on people whose vehicles provided no cause for suspicion.

Despite the fact that the vast majority of this location data is collected on law-abiding individuals, agencies often retain the data for years in massive databases managed by the police or private companies and shared widely with other federal, state and local law enforcement agencies. These databases allow officers to query a car's past locations for years into the future.

II. Location Data Reveals Private and Personal Details About Individuals

ALPRs pose significant risks to privacy and civil liberties. They can be used to scan and record vehicles at a lawful protest or house of worship; track all movement in and out of an area; gather

---

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

[4] *See* Letter re: "Automated License Plate Reader Pilot Report Out," Bay Area Urban Areas Security Initiative (July 14, 2016) *available at* http://bauasi.org/sites/default/files/resources/071416%20Agenda%20Item%206%20ALPR%20Pilot%20Report%20Out.pdf.

[5] *See* Jennifer Lynch, *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.

[6] *See supra* n. 4; *see also* ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, pp. 13-15 (July 2013) https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record (noting that typically, only about 0.2% of plate scans are linked to suspected crimes or vehicle registration issues).

information about certain neighborhoods or organizations; or place political activists on "hot lists" so that their movements trigger alerts.[7] The Supreme Court has recognized the sensitive nature of location data and the fact that it can reveal "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 United States v. Jones*, 132 S. Ct. 945, 955 (2012)(Sotomayor, J., concurring)).

Although ALPRs are not generally used to monitor or track a single individual's movements, unlike the GPS tracking at issue in *Jones*, the data collected 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."[8] These researchers found they could uniquely characterize 50% of people using only two randomly chosen time and location data points.[9] 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.[10] It can even be used to find drivers who are travelling together.[11]

Law enforcement agencies across the country and vendors like Vigilant and DRN recognize the power of ALPR data to identify individuals.[12] The Los Angeles Police Department has said that ALPR

---

[7] *See* Cyrus Farivar, *Rich California Town Considers License Plate Readers for Entire City Limits*, Ars Technica (Mar. 5, 2013) http://arstechnica.com/tech-policy/2013/03/rich-california-town-considers-license-plate-readers-for-entire-city-limits; 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; 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; Richard Bilton, *Camera Grid to Log Number Plates*, BBC (May 22, 2009) http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8064333.stm.

[8] 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.

[9] *Id.*

[10] 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 (discussing using ALPR data to "build[] up the lifestyle of criminals—where they are going to be at certain times.").

[11] James Bridle, *How Britain Exported Next-Generation Surveillance*, Matter (Dec 18, 2013) https://medium.com/matter/how-britain-exported-next-generation-surveillance-d15b5801b79e#.3tysomcwu.

[12] *See Stakeout Pattern & Crime Analytic Tool*, Vigilant Solutions, https://vigilantsolutions.com/stakeout (ALPR data used "to locate possible witnesses and suspects in pattern and serial crimes").

data "can be used to draw inferences about an individual's driving patterns and whereabouts" and that, with ALPR data, a person "could try to identify driving patterns of a particular individual in order to locate that person."[13] 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."[14] And California police and sheriffs' organizations have stated that the information in ALPR databases "may include or lead to unsuspecting individual drivers' potentially private and sensitive information" and "can lead to identification of those persons/witnesses associated" with plate scans.[15]

Police tracking of the public's movements can have a significant 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 consider themselves under constant surveillance."[16] 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.[17]

III. 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

---

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

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

[15] *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) *available at* https://www.eff.org/files/2016/05/19/amicus_brief_of_ca._sheriffs_ca_police_chiefs_and_ca._peace_officers_iso_respondent.pdf.

[16] Intn'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report*, 13 (Sept. 2009) http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf.

[17] 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.

extortion after looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners."[18] And a state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[19] Many of the 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."[20] In Ohio, officers looked through the database to find information on an ex-mayor's wife, along with council people and spouses. Police have also given license plate data to reporters.[21] None of these examples were prompted by a traffic stop or criminal suspicion.[22]

CONCLUSION

Taken in the aggregate, ALPR data can create a revealing history of a person's movements, associations, and habits. Because this data is easily linked to an individual and has the potential for abuse, it should be protected by the Government Data Collection & Dissemination Practices Act.

---

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

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

[20] 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.

[21] 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 (discussing ease with which reporter was able to get driver information linked to specific license plate numbers from a police officer).

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

Dated: 5 August 2016

Respectfully submitted,

Stephen B. Pershing
Virginia Bar No. 31012
1416 E Street, N.E.
Washington, D.C. 20002
(202) 642-1431 (v/f)
sbpershing@gmail.com

Jennifer Lynch
Electronic Frontier Foundation
California State Bar No. 240701
815 Eddy St.
San Francisco, CA 94109
Tel.: 415-436-9333 x136
Fax: 415-436-9993
email: jlynch@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of August, 2016, I served a true and correct copy of the foregoing document by electronic mail and by U.S. Mail, postage prepaid, to the following:

Kimberly P. Baucom
Assistant County Attorney
Office of the Fairfax County Attorney
12000 Government Center Parkway, Suite 549
Fairfax, Virginia 22035
Kimberly.PaceBaucom@fairfaxcounty.gov

Rebecca K. Glenberg
Hope R. Amezqauita
American Civil Liberties Union Foundation of Virginia, Inc.
701 East Franklin Street, Suite 1412
Richmond, Virginia 23219
rglenberg@acluva.org
hamezquita@acluva.org

Edward S. Rosenthal
Christina M. Brown
Rich Rosenthal Brincefield Manitta Dzubin & Kroeger, LLP
201 North Union Street, Suite 230
Alexandria, Virginia 22314
esrosenthal@rrbmdk.com
cmbrown@rrbmdk.com

Andrew J.M. Bentz, Esq.
Jones Day
51 Louisiana Ave., N.W.
Washington, D.C. 20001
abentz@jonesday.com

Stephen B. Pershing