NO. 18-10341

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

JAY YANG,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
District of Nevada (Las Vegas)
Case No. 2:16-cr-00231-RFB-1

The Honorable Richard F. Boulware, II, District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF NEVADA IN SUPPORT OF APPELLANT

Nathan Freed Wessler
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Fl.
New York, NY 10004
Tel.: 212-549-2500
nwessler@aclu.org
bkaufman@aclu.org

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333
jlynch@eff.org
andrew@eff.org

Counsel for Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Nevada

Additional counsel listed on following page.

Jennifer S. Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel.: 415-343-0758
jgranick@aclu.org

Amy M. Rose
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
601 S. Rancho Drive, Suite B11
Las Vegas, Nevada 89106
Tel.: 702-366-1536
rose@aclunv.org

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Nevada state that they do not have parent corporations. No publicly held corporation owns 10% or more of any stake or stock in *amici curiae.*

Dated: March 18, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

STATEMENTS OF INTEREST 1

INTRODUCTION AND SUMMARY OF ARGUMENT 3

ARGUMENT 4

I. ALPR Systems Across the Country Collect and Store Massive Amounts of Data that Can be Used to Identify and Track Drivers. 4

A. ALPRs Automatically and Indiscriminately Capture License Plate Data. 4

1. ALPRs Collect a Significant Amount of Data. 8

2. ALPRs Collect Data on Everyone, Without Regard to Ties to Criminal Activity. 11

B. ALPR Data Can Reveal Private and Personal Details About Individuals. 12

C. The Threats to Privacy and Civil Liberties from ALPRs Are Well-Recognized. 19

II. Reviewing Collected ALPR Data Constitutes a Fourth Amendment "Search." 21

A. Individuals Maintain a Reasonable Expectation of Privacy in Their Movements. 21

B. ALPR Systems Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy. 22

1. Detailed Nature of the Data. 25

2. Indiscriminate Collection of Data. 27

3. Retrospective Searches. 28

III. Searches of ALPR Databases Require a Warrant. 29

CONCLUSION 32
CERTIFICATE OF COMPLIANCE 34
CERTIFICATE OF SERVICE 35

TABLE OF AUTHORITIES

Cases

ACLU Found. v. Super. Ct.,
3 Cal. 5th 1032 (Cal. 2017)..... 16

Cardwell v. Lewis,
417 U.S. 583 (1974)..... 21

Carpenter v. United States,
138 S. Ct. 2206 (2018)..... *passim*

Kyllo v. United States,
533 U.S. 27 (2001).....23, 25, 26

Neal v. Fairfax Cty. Police Dep't,
295 Va. 334 (Va. 2018)..... 16, 20

Skinner v. Ry. Labor Executives Ass'n,
489 U.S. 602 (1989)..... 31

Smith v. Maryland,
442 U.S. 735 (1979)..... 24

United States v. Carey,
172 F.3d 1268 (10th Cir. 1999)..... 32

United States v. Diaz-Castaneda,
494 F.3d 1146 (9th Cir. 2007)..... 22, 23

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013)..... 32

United States v. Ganias,
755 F.3d 125 (2d Cir. 2014)..... 31

United States v. Hulscher,
No. 4:16-CR-40070-01-KES, 2017 WL 657436 (D.S.D. Feb. 17, 2017)..... 32

United States v. Jones,
565 U.S. 400 (2012)..... *passim*

United States v. Katzin,
732 F.3d 187 (3d Cir. 2013)..... 30

United States v. Miller,
425 U.S. 435 (1976) 24

United States v. Sedaghaty,
728 F.3d 885 (9th Cir. 2013) 31

Vernonia School Dist. 47J v. Acton,
515 U.S. 646 (1995) 30

Other Authorities

About, Vigilant Solutions 9

Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, Associated Press (Feb. 23, 2012) 13

Ali Winston, *License Plate Readers Tracking Cars*, SF Gate (June 25, 2013) 6

Ali Winston, *License-plate Readers Let Police Collect Millions of Records on Drivers*, Center for Investigative Reporting (June 26, 2013) 19

ALPR Products and Solutions > Mobile Plate Hunter – 900, ELSAG North America 8

Amici Curiae Br. of Cal. State Sheriffs' Assoc., et al. *ACLU v. Super. Ct.*, No. S227106 (Cal. Sup. Ct. May 3, 2016) 15

Brian A. Reaves, *Local Police Departments, 2013: Equipment and Technology*, DOJ, Bureau of Justice Statistics (July 2015) 7

Cal. Office of Emergency Services, *License Plate Reader Participant Guide* (Mar. 2015) 18

CarDetector – Mobile Hit Hunter, Vigilant Solutions 9

Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, CUNY School of Law, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (Mar. 11, 2013) 20

Cynthia Lum, et al., *The Rapid Diffusion of License Plate Readers in U.S. Law Enforcement Agencies*, Ctr. for Evidence-Based Crime Pol'y, Geo. Mason Univ. (Dec. 2016) 7, 9

Cyrus Farivar, *We Know Where You've Been: Ars Acquires 4.6M License Plate Scans from The Cops*, Ars Technica (Mar. 24, 2015) 17

Dave Maass & Beryl Lipton, *What We Learned*, MuckRock (Nov. 15, 2018).....10, 11, 12

Decimal degrees, Wikipedia 6

Digital Recognition Network..... 8, 9

Eric Roper, *City Cameras Track Anyone, Even Minneapolis Mayor Rybak*, Minneapolis Star Tribune (Aug. 17, 2012)..... 16

Fremont: 14.5 million vehicles scanned in 11 months, The Center for Human Rights and Privacy 10

George Joseph, *What Are License-Plate Readers Good For?*, The Atlantic CityLab (Aug. 5, 2016)..... 12

Intn'l Assoc. of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers (Sept. 2009)..... 19, 20

James Bridle, *How Britain Exported Next-Generation Surveillance*, Matter (Dec 18, 2013)..... 14

Jennifer Lynch & Peter Bibring, *Secrecy Trumps Public Debate in New Ruling On LA's License Plate Readers*, EFF (Sept. 3, 2014)..... 8

Josh Wade & Aaron Diamant, *Eyes on the Road*, Atlanta Journal-Constitution 8

Josh Wade, *Follow the trail of a license plate*, Knight Lab 16

Justin Rohrlich, *In just two years, 9,000 of these cameras were installed to spy on your car*, Quartz (Feb. 5, 2019)..... 5

Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, The Atlantic (Apr. 22, 2016)..... 6

Kim Zetter, *Even the FBI Had Privacy Concerns on License Plate Readers*, Wired (May 15, 2015)..... 12

Las Vegas PD Lunch and Learn, Vigilant (Jul 26, 2017)..... 19

Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU (Jan. 25, 2016)..... 9

Mark Harris, *If you drive in Los Angeles, the cops can track your every move*, Wired (Nov. 13, 2018).....13, 17, 18

Megan Bryan, *83% of U.S. Adults Drive Frequently; Fewer Enjoy It a Lot*, Gallup (July 9, 2018) 27

Operational trials with the automatic number plate reader at the Dartford Tunnel 1982, WhatDoTheyKnow 19

Opp'n Br. of City of LA, *ACLU v. Super. Ct.*, No. B259392 (Cal. Ct. App. Nov. 26, 2014) 15

Paul Lewis, *CCTV Aimed at Muslim Areas in Birmingham to be Dismantled*, The Guardian (Oct. 25, 2010) 13

Privacy Impact Assessment for Texas Dept. of Public Safety (Sept. 2014) 15

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) 11

State of New Jersey, Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (Effective January 18, 2011) 14

Statement of Work: Access to License Plate Reader Commercial Data Service, U.S. Immigration & Customs Enforcement 23

Steve Connor, *Surveillance UK: Why this Revolution Is Only the Start*, The Independent (Dec. 21, 2005) 14

Use of License-Plate Scanners Expands amid Privacy Concerns, Court Battles, Fox News (Sept. 2, 2015) 12

What's Wrong with ANPR?: A report by No CCTV into Automatic Number Plate Recognition Cameras, No CCTV 3 (Oct. 2013) 20

You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements, ACLU (July 2013) 11

Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature Scientific Reports, Art. No. 1376 (2013) 14

STATEMENTS OF INTEREST[1]

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 nearly thirty years. With roughly 40,000 active donors, EFF represents technology users' interests in court cases and broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF regularly participates as amicus in the Supreme Court, this Court, and other courts in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Cotterman,* 709 F.3d 952 (9th Cir. 2013).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Nevada is a state affiliate of the

[1] Pursuant to Fed. R. App. Proc. 29(a), no counsel for a party authored this brief in whole or in part, and no person other than amicus or their counsel has made any monetary contributions to fund the preparation or submission of this brief. All parties have consented to the filing of this brief.

ACLU. The ACLU and ACLU of Nevada have frequently appeared before the Supreme Court and other federal and state courts in numerous cases implicating Americans' right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Jones*, 565 U.S. 400 (2012), and *United States v. Gilton*, -- F.3d --, 2019 WL 1008722 (9th Cir. Mar. 4, 2019).

INTRODUCTION AND SUMMARY OF ARGUMENT

As with cell phones, cars have long been "such a pervasive and insistent part of daily life" that for many individuals, owning and driving one "is indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018) (quotation marks and citation omitted). Our vehicles take us to sensitive and private places like our homes, doctors' offices, and places of worship. And yet, for many years now, with little to no oversight, law enforcement agencies and private companies have been quietly scanning and recording the locations of billions of vehicles' license plates across the country.

This "Automated License Plate Reader" ("ALPR") data is collected on every vehicle, regardless of whether individual drivers are suspected of criminal activity. ALPR data includes not just the plate number but also a photograph of the vehicle and detailed location, time, and date information that can later place the vehicle to within feet of the original scan. This data is stored in massive databases that are accessible to federal, state, and local law enforcement agencies, even where, as in this case, those agencies do not collect their own data or maintain their own databases. In many cases, this data is retained for more than five years, or even, as in this case, indefinitely.

ALPR data can be used not just to identify and locate a particular vehicle, but also, when combined with other easily accessible data, to identify that vehicle's

owner and driver. And because ALPR data is stored for years, ALPR databases allow for retrospective searches that enable law enforcement to infer driving patterns, associations, and sensitive details about drivers' lives. At bottom, searches of ALPR databases threaten to undermine the "degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 138 S. Ct. at 2214 (quotation marks and citation omitted), because they give police a capability unimaginable in the past—the ability to enter a virtual time machine and view suspects' past movements. To prevent this capability from feeding "too permeating police surveillance," *id*. (quotation marks and citation omitted), the Fourth Amendment's warrant requirement applies. And because the government has not shown that exigent circumstances justify the warrantless search of the ALPR database that occurred here, the plate scan and all evidence collected as a result should be suppressed.

ARGUMENT

I. ALPR SYSTEMS ACROSS THE COUNTRY COLLECT AND STORE MASSIVE AMOUNTS OF DATA THAT CAN BE USED TO IDENTIFY AND TRACK DRIVERS.

A. ALPRs Automatically and Indiscriminately Capture License Plate Data.

ALPRs are computer-controlled camera systems—generally mounted on vehicles or on fixed objects such as light poles—that automatically capture images

of every license plate that comes into view.[2] ALPRs can detect when a license plate enters the camera's field, capture a photograph of the car and its surroundings (including the plate), capture an infrared image of the plate at night,[3] and convert the image of the plate into alphanumeric data—in effect "reading" the plate. ALPRs record data on every plate they scan, including plate number and precise time, date, and place it was encountered, uploading this data to a central database almost immediately after the scan.[4] ALPR systems record extremely detailed GPS coordinates for each plate scanned. For example, the coordinates of the two scans in this case—recorded one second apart—were 36.164555º latitude by -115.265384º longitude and 36.164556º latitude by -115.265463º longitude.[5] These coordinates are accurate enough to record the ALPR camera's location to a

---

[2] Although most ALPR systems include integrated cameras and software, at least two companies market software that can be used with a smartphone or almost any other standalone camera. *See, e.g.,* Testimony of Todd J. Allen Hodnett, ER 209 ("Hodnett Testimony") (noting Vigilant sells a smartphone application); *see also* Justin Rohrlich, *In just two years, 9,000 of these cameras were installed to spy on your car*, Quartz (Feb. 5, 2019), https://qz.com/1540488/in-just-two-years-9000-of-these-cameras-were-installed-to-spy-on-your-car/ ("At least one company, OpenALPR, offers software for free, on Github. Anyone who downloads it can turn a single web-connected camera into an automatic license plate reader that can monitor traffic across a four-lane highway with 99% accuracy." OpenALPR is currently being used by police and private citizens on 9,200 cameras in 70 countries).

[3] Hodnett Testimony, ER 163-165, 175, 206-207.

[4] Hodnett Testimony, ER 192 (uploaded within 10 seconds).

[5] ER 431-32.

distance of two to four inches and within feet of the vehicle whose plate was scanned.[6] The images captured by the systems can reveal not just the plate itself, but also the vehicle's occupants.[7]

By design, ALPR collection is indiscriminate. ALPR operators turn on vehicle-mounted ALPRs at the start of their shifts, and the devices scan plates continuously until operators turn off the system at the end of their shift.[8] Fixed ALPRs have a continuous connection to an ALPR server. Vehicle plates are scanned not just while cars are in motion or parked on public roads, but also while they are parked in privately owned parking lots, on private streets, and driveways of homes.[9]

---

[6] Although the district court judge in this case stated the scan only placed Yang's vehicle within a certain block, the GPS coordinates were much more detailed than this. *See Decimal degrees*, Wikipedia, https://en.wikipedia.org/wiki/Decimal_degrees (noting at 6 decimal places, coordinates are accurate to within 43-111 mm and precise enough to recognize individual humans).

[7] *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.

[8] ER 193-194.

[9] *See* ER 261-62, 369, 372, 394-96 (explaining plate scans here took place inside a gated community); 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; Winston, *supra* note 7.

ALPR systems and databases are maintained and used by both government agencies and private companies. Surveys conducted in 2013 by the federal Bureau of Justice Statistics found that 93% of police departments in cities with 1 million or more people, and more than three-quarters of departments serving 100,000 or more residents, used their own ALPR systems.[10] A 2016 nationwide survey of law enforcement ALPR use noted "[A]LPR acquisition has most likely tripled" in the last ten years.[11]

ALPR data can be compared against a list of wanted vehicle plates, and users can set up "hotlists" so they are alerted as soon as a wanted plate is scanned.[12] Police and other users can also search accumulated data in future investigations to identify drivers' past movements and locations.

---

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

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

[12] ER 192-193 (timing of alerts); ER 198 (commercial data immediately available to government users).

1. ALPRs Collect a Significant Amount of Data.

By scanning every license plate that comes into view—scans of up to 1,800 plates per minute[13]—ALPRs collect an enormous volume of data. The Los Angeles Police Department (LAPD) and Sheriff's Department together collect data on 3 million cars every week.[14] The City of Atlanta scans even more plates, processing nearly 30 million each month using just 347 ALPR cameras.[15]

Private-vendor ALPR databases—which are also accessible to law enforcement—dwarf these government-maintained databases. VaaS International Holdings (which wholly owns Vigilant Solutions, the provider of the "LEARN" ALPR database used in this case) not only maintains data for government agencies, but, through its other wholly-owned subsidiary, DRN, also employs private contractors to collect plate scan data, which it markets to insurers, repossession companies, and others.[16] The LEARN database combines commercial and government ALPR data, providing real-time and retrospective access to

---

[13] *See* ELSAG North America, *Mobile Plate Hunter–900*, DuraTech USA https://www.duratechusa.com/Products/MPH900.htm.

[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.

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

[16] *See* Digital Recognition Network, https://drndata.com/.

government agencies across the country.[17] VaaS president Todd Hodnett noted in this case that roughly 65% of the data contained in the LEARN database comes from private contractors.[18] Vigilant's marketing materials say the LEARN database is growing at a rate of 120 million data points a month, and DRN's commercial database alone currently includes over 6.5 billion scans.[19]

Private vendors and law enforcement retain ALPR data for long periods of time. In George Mason University's survey of national ALPR use, researchers found 12.7% of responding agencies stored data for two to four years, 11.8% stored it for five to seven years, and 15.0% stored it indefinitely.[20] There are no indications from the facts of this case that Vigilant ever purges its privately collected license plate data.[21]

---

[17] *About*, Vigilant Solutions, https://vigilantsolutions.com/about ("A hallmark of Vigilant's solution, the ability for agencies to share real-time data nationwide amongst over 1,000 agencies and tap into our exclusive commercial LPR database").

[18] ER 186.

[19] *Id*; *see also* Digital Recognition Network, https://drndata.com/ (noting 6,500,000,000 "total vehicle sightings") (last visited March 14, 2019); *CarDetector – Mobile Hit Hunter*, Vigilant Solutions, https://www.vigilantsolutions.com/wp-content/uploads/PSL_Mobile_Hit_Hunter_MHH_VS.pdf (Vigilant maintains a "private LPR network that scans approximately 1,240,000 vehicles each day across all major metropolitan areas").

[20] Lum, et al., *supra* note 11, at 29.

[21] *See* Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU (Jan. 25, 2016, 10:30 AM).

Even government agencies that do not maintain their own ALPR systems—such as the Postal Inspection Service in this case—can still take advantage of data gathered by others. Vigilant and the law enforcement agencies that collect and maintain their own ALPR data share that data with many other agencies across their regions and also nationwide. For example, 28 agencies in the San Francisco Bay Area share ALPR data via the Northern California Regional Intelligence Center, including agencies like IRS, Department of Homeland Security, FBI, National Park Service, and the California Department of Insurance, which either do not have their own ALPR systems or do not operate them in the Bay Area.[22]

However, even the data available in regional databases is only a fraction the size of the data accessible to agencies like the Postal Inspection Service that contract with Vigilant. In a 2018 nationwide survey of 173 agencies that collect their own data and share it with Vigilant, researchers from MuckRock and EFF found that agencies that contract with Vigilant for ALPR services collected more than 2.5 billion plate scans.[23] The agencies can choose with whom they share their data, and the same survey found that most agencies "were sharing data directly

---

[22] *Fremont: 14.5 million vehicles scanned in 11 months*, The Center for Human Rights and Privacy, https://www.cehrp.org/fremont-14-5-million-vehicles-scanned-in-11-months/.

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

with around 160 other agencies."[24] Ten agencies were sharing data with more than 800 other agencies, and in some cases, agencies were sharing data with other agencies they had never even heard of.[25]

2. ALPRs Collect Data on Everyone, Without Regard to Ties to Criminal Activity.

ALPRs scan vehicles regardless of any association with criminal activity. This means the vast majority of data is collected on drivers who are under no suspicion of criminal activity or risk to public safety. 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 linked to criminal activity.[26] That means 99.975% of the data—3,995,111 plate scans—was collected from vehicles under no suspicion. Similar rates were recorded in

---

[24] *Id*.

[25] *Id*.

[26] *See* Report from Officer Cheryl Paris, Central Marin Police Authority, et al., to Bay Area UASI Approval Authority, *Re: Item 6: 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 at 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).

New York (0.01%) and North Carolina (0.08%).[27] Of the 173 agencies surveyed by MuckRock, "on average, only .5%—that is, one half of one percent—of license plate scans" were linked to a hotlist.[28]

B. ALPR Data Can Reveal Private and Personal Details About Individuals.

As even the FBI has recognized, ALPRs impact the privacy rights of Americans.[29] 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,[30] gather information

[27] George Joseph, *What Are License-Plate Readers Good For?*, CityLab (Aug. 5, 2016), http://www.citylab.com/crime/2016/08/what-are-license-plate-readers-good-for/492083/. *See also* Maass & Lipton, *supra* note 23 ("99.5% of the license plates scanned were not under suspicion at the time the vehicles' plates were collected").

[28] Maass & Lipton, *supra* note 23.

[29] Kim Zetter, *Even the FBI Had Privacy Concerns on License Plate Readers*, Wired (May 15, 2015, 8:00 AM), https://www.wired.com/2015/05/even-fbi-privacy-concerns-license-plate-readers.

[30] 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.

about certain neighborhoods[31] or organizations,[32] or place political activists on "hot lists" so that their movements trigger alerts.

Because ALPR data may be retained for five years or more, ALPR databases allow officers to query a car's past locations for years into the future. Officers search these databases constantly. LAPD officers, for example, query ALPR databases 200-300 times per day.[33] For many agencies, including those like the Postal Inspection Service that access Vigilant's LEARN database, there are no restrictions on these searches.[34]

Although ALPRs do not generally record as many individual points of location data as devices like dedicated GPS trackers, ALPR data can be just as revealing as other kinds of tracking technology. Scientists working with location data have determined that, given humans' unique patterns of travel, "even coarse

---

[31] *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.

[32] *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.

[33] Mark Harris, *If you drive in Los Angeles, the cops can track your every move*, Wired (Nov. 13, 2018), https://www.wired.com/story/drive-los-angeles-police-track-every-move.

[34] ER 204.

datasets provide little anonymity."[35] These researchers found they could uniquely characterize 50% of people using only two randomly chosen time and location data points.[36] This means even a small amount of ALPR data can reveal sensitive information about an individual. When ALPR data is aggregated and retained for long periods of time, it can reveal not only where a driver was on a given date and time in the past, but can also suggest where a driver may be in the future.[37] It can even be used to find drivers who are travelling together.[38]

Law enforcement agencies across the country already recognize the power of ALPR data to identify *individuals*, not just their vehicles. LAPD has said that

---

[35] Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The privacy bounds of human mobility*, 3 Nature Scientific Reports 1376 (2013), http://www.nature.com/articles/srep01376.

[36] *Id*.

[37] State of New Jersey, Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data (effective Jan. 18, 2011), http://www.state.nj.us/lps/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf (noting ALPR data can be used "to predict when and where future crimes may occur[.]"); Steve Connor, *Surveillance UK: why this revolution is only the start*, The Independent (Dec. 22, 2005), http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html (ALPR data used to "build[] up the lifestyle of criminals—where they are going to be at certain times").

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

ALPR data can be used "to identify driving patterns of a particular individual."[39] 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."[40] 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.[41]

Two state supreme courts have also recognized the power of ALPRs to identify individuals and sensitive information about their lives. The Virginia Supreme Court held last year that photographs and data associated with license plate scans constitute "personal information" under the state's data privacy law and noted they "afford a basis for inferring [an individual's] personal characteristics . . .

---

[39] *See* Opp'n Br. of City of LA at 29, *ACLU v. Super. Ct.*, No. B259392 (Cal. Ct. App. Nov. 26, 2014), *available at* https://www.eff.org/files/2016/08/03/brf.calapp.city_opp_to_petition_for_writ_of_mandate.pdf.

[40] *Privacy Impact Assessment for the Texas Department of Public Safety (DPS) Collection, Storage, Management and Use of Automated License Plate Reader Data*, Tex. Dep't of Pub. Safety 4 (Sept. 2014), http://www.txdps.state.tx.us/administration/crime_records/pages/LPRPIA.pdf.

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

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 v. Fairfax Cty. Police Dep't*, 295 Va. 334, 346–47 (Va. 2018). Likewise, the California Supreme Court recognized that "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.*, 3 Cal. 5th 1032, 1044 (Cal. 2017).

This kind of identification already occurs. In August 2012, the Minneapolis *Star Tribune* published a map displaying the 41 locations where license plate readers had recorded the mayor's car in the preceding year.[42] In 2018, local reporters in Atlanta were able to use ALPR data to map a vehicle's travels over the course of just one day.[43] Using Oakland Police Department ALPR data, *Ars Technica* was able to correctly guess the block where a city council member lived after less than a minute of research.[44] *Ars Technica* was also able to run the plate

---

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

[43] Josh Wade, *Follow the trail of a license plate*, Knight Lab, https://uploads.knightlab.com/storymapjs/ca566c1c597556a26043831ed5f47a6d/license-plate-readers/index.html.

[44] Cyrus Farivar, *We know where you've been: Ars acquires 4.6M license plate scans from the cops*, Ars Technica (Mar. 24, 2015, 6:00 AM),

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 bar and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[45]

When ALPR systems are linked to sophisticated algorithms, officers can learn even more about drivers and their driving patterns. For example, LAPD's system provides officers with a "chart showing how many times a plate has been searched," as well as a frequency analysis that "displays a table showing those hits by time of day, and day of the week."[46] "These can help detectives spot patterns, such as where a vehicle's driver might live or work."[47] Officers can also learn the plate numbers of all vehicles that were in a given area at a given time.[48] This can reveal not only who was at that location but also potential associations among drivers.

Vigilant markets its technology to law enforcement based on ALPR's ability to identify, track, and learn detailed information about actual people. Its website

---

http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops.

[45] *Id*.

[46] Harris, *supra,* note 33.

[47] *Id*.

[48] *Id*.

has advertised that "90 percent of the time individuals are within 1,000 feet of their car."[49] Its training materials state that "LPR isn't just an enforcement tool; it can assist with keeping track" of people.[50] Vigilant states its LEARN database contains "analytical search engines which have been used to establish suspect/victim travel patterns and identify vehicles used in crimes."[51] And its training materials also note that, because license plate data can be connected to so much other available data, it is possible to determine other information about a person, such as where their mother lives, that they have moved, and that they are attending junior college.[52]

As discussed above, ALPRs do not just record license plate and location data. Every scan also includes a photograph of the plate and vehicle. This allows many systems to extract additional details about the vehicle and its occupants. For example, LAPD's system, designed by Palantir, uses "machine learning to recognize the color, make, and style of vehicles photographed by ALPR cameras, as well as accessories like spare tires."[53] Vehicle photographs may also include bumper stickers, which could reveal information about a person's political or

---

[49] Hodnett Testimony, ER 337-38.

[50] Cal. Office of Emergency Services, *License Plate Reader Participant Guide* at 145, (Mar. 2015), *available at* https://www.eff.org/document/license-plate-reader-training-march-2015 (document obtained in public records request).

[51] *Id*. at 131.

[52] *Id*. at 155-56.

[53] Harris, *supra* note 33; ER 165.

social views, and may include recognizable views of the vehicle's occupants.[54] One California resident 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.[55] Vigilant markets a face recognition technology that could be used, along with ALPR, to identify such individuals.[56]

C. The Threats to Privacy and Civil Liberties from ALPRs Are Well-Recognized.

People have recognized the privacy implications of ALPRs for nearly as long as they have been in use. ALPRs were first developed in the United Kingdom in the 1970s to locate stolen vehicles.[57] Once they were put into use in the 1980s, a report for the Greater London Council Police Committee stated, "The development of [mass, suspicionless vehicle checks] is most alarming. . . . the use of devices that read car number plates automatically, leave mass surveillance as a policy to be

---

[54] Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, 6, 11 (Sept. 2009), https://www.theiacp.org/sites/default/files/all/k-m/LPR_Privacy_Impact_Assessment.pdf.

[55] Winston, *supra* note 7.

[56] *See, e.g., Las Vegas PD Lunch and Learn*, Vigilant (Jul 26, 2017) https://www.vigilantsolutions.com/event/las-vegas-pd-lunch-learn/ (meeting to discuss how "license plate recognition (LPR) and facial recognition tools can be used to enhance investigations").

[57] *See Operational trials with the automatic number plate reader at the Dartford Tunnel 1982*, WhatDoTheyKnow, https://www.whatdotheyknow.com/request/100679/response/256281/attach/4/Taylor%208a.pdf?cookie_passthrough=1.

determined independently by the police. This possibility in a democracy is unacceptable."[58]

It is widely understood that 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 creates the risk "that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[59] And, indeed, communities that have faced excessive police surveillance including ALPRs have feared engaging in political activism, expressing religious observance, and exercising other constitutional rights.[60] These concerns echo those expressed by the Virginia and California Supreme Courts in cases addressing ALPR data. *See Neal*, 295 Va. at 346–47 (concluding that "the Police Department's sweeping randomized

---

[58] What's Wrong with ANPR?: A report by No CCTV into Automatic Number Plate Recognition Cameras, No CCTV 3 (Oct. 2013) *What's Wrong with ANPR?: A report by No CCTV into Automatic Number Plate Recognition Cameras*, No CCTV 3 (Oct. 2013), http://www.no-cctv.org.uk/docs/Whats%20Wrong%20With%20ANPR-No%20CCTV%20Report.pdf.

[59] Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers* at 13.

[60] *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.

surveillance and collection of personal information does not" constitute an investigation or "intelligence gathering related to criminal activity" and remanding to determine if the police must purge the data). *ACLU Found. v. Super. Ct.*, 3 Cal. 5th 1032, 1044, (2017) (remanding to determine whether privacy concerns associated with disclosure of ALPR data outweigh the government's duty to disclose public records under the California Public Records Act).

II. REVIEWING COLLECTED ALPR DATA CONSTITUTES A FOURTH AMENDMENT "SEARCH."

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

The district court erred when it held that Mr. Yang had no expectation of privacy in ALPR data accessed by the government. ER 027. The court pointed out that under Supreme Court precedent "the physical characteristics of an automobile and its use generally result in a lessened expectation of privacy" because "'[a] car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.'" ER 023-024 (quoting *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974) (plurality opinion)).

However, the district court ignored recent Supreme Court case law clarifying that while individuals may have lessened expectations of privacy in certain information they reveal publicly, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter*, 138 S. Ct.

at 2217; *United States v. Jones*, 565 U.S. 400 (2012). As recognized by five concurring Justices in *Jones* and reaffirmed by the majority in *Carpenter*, "individuals have a reasonable expectation of privacy in the whole of their physical movements" because of the "privacies of life" those movements can reveal. *Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment); *id*. at 415 (Sotomayor, J., concurring)).

In this case, Mr. Yang's expectation of privacy was not in individual aspects of his car or its license plate, but in the record of his movements revealed by ALPR data.

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

The district court further erred by treating the use of modern technology to seamlessly capture, aggregate, and search massive amounts of ALPR data as identical to the observation of a license plate and other characteristics of a single vehicle by an individual law enforcement officer. *See* ER 024 (citing *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151 (9th Cir. 2007)). Other than the fact that both involve officers and license plates, they could not be more different.

In a series of cases addressing the power of sense-enhancing technologies "to encroach upon areas normally guarded from inquisitive eyes," the Supreme Court "has sought to 'assure [ ] preservation of that degree of privacy against

government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States,* 533 U.S. 27, 34 (2001)) (last alteration in original); *accord Jones*, 565 U.S. at 406. As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." 565 U.S. at 429 (Alito, J., concurring in judgment).

Innovations like ALPR systems remove many of these types of practical limitations in the context of license plates and associated ALPR data. Indeed, as Immigration and Customs Enforcement explains, use of ALPR data "reduc[es] the work-hours required for physical surveillance."[61] Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Court has admonished lower courts to remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2223. The cases relied on by the district court, including this Court's decision in *Diaz-Castaneda*, predate *Jones* and *Carpenter* and do not involve sophisticated tracking technologies like ALPR.

[61] Statement of Work: Access to License Plate Reader Commercial Data Service, U.S. Immigration & Customs Enforcement, *available at* https://www.aclunc.org/docs/DOCS_031319.pdf (p.288 of PDF).

In *Carpenter*, the Supreme Court held that a Fourth Amendment search occurs when the government tracks an individual's movements by collecting cell phone location information ("CSLI") from a cellular service provider, at least for more than seven days. *Id*. at 2220. The Court noted that under *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), individuals ordinarily do not have a reasonable expectation of privacy in business records that they voluntarily disclose to third parties or to the public at large. *Id*. at 2216. However, it declined to extend *Smith* and *Miller* to the collection of CSLI, listing several factors that distinguish tracking individuals' cell phones from more primitive forms of surveillance.[62] *Id*. at 2217-20.

Automated license plate readers infringe on individuals' expectations of privacy for much the same reason that the GPS monitoring of vehicles at issue in *Jones* and the tracking of cell phones in *Carpenter* do: they facilitate detailed, pervasive, cheap, and efficient tracking of millions of Americans in previously unthinkable ways.

[62] For this reason, the fact that the ALPR that captured Mr. Yang's license plate was mounted on a commercial vehicle rather than a government vehicle does not insulate it from Fourth Amendment protection. Just as *Carpenter* held that it is a search when the government collects CSLI from a cell phone provider that has compiled the records for its own purposes, it is a search when government agents access a private ALPR database compiled in part by private vehicles.

1. Detailed nature of the data.

First, the *Carpenter* Court noted that "like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." 138 S. Ct. at 2216.

As described above, ALPR databases like the one accessed by the government here share these characteristics. GPS coordinates associated with ALPR records can place vehicles at highly specific locations at specific times, locating an individual's car with more precision than the cell phone data at issue in *Carpenter* or even the GPS tracker in *Jones*. *See id*. at 2218 (CSLI accurate to within one-eighth to four square miles); *Jones* 565 U.S. at 403 (GPS device accurate to within 50–100 feet); *supra* at pp. 5-6 (ALPR location data accurate to within 2-4 inches of the camera and within feet of the vehicle).

Furthermore, ALPR data allows the government to track people to locations that reveal private information about their lives. That is because the geographical precision of ALPR data facilitates inferences about individuals' locations in homes, offices, hotel rooms, and other spaces that receive the highest protection under the Fourth Amendment, and for which warrantless searches using both traditional and technological means are forbidden. *Kyllo*, 533 U.S. at 40. "Mapping a cell phone's location over the course of [time] provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped

data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

Although ALPR systems may compile fewer individual data points than GPS tracking or CSLI, even a small number of ALPR data points facilitate inferences about individuals' travels habits, including the homes, businesses and neighborhoods they frequent. *See supra* at sec. I.B. And it is of no matter that the government extrapolates a person's whereabouts using ALPR data rather than observing them directly because "the Court has already rejected the proposition that 'inference insulates a search.'" *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo*, 533 U.S. at 36). Every time a government agent queries an ALPR database, as the postal inspector did in this case, they search the millions of records it contains.[63] As a result, this is a search of long-term location data even though agents may only rely on a small number of records produced in response to their queries. *See*

[63] Although this case involves only two ALPR records, the postal inspector appears to have requested a search of the entire LEARN database without limitation. *See* ER 072-073 (Affidavit of Postal Inspector Justin Steele) (noting only that he "obtained a vehicle detection report for the dark colored GMC Yukon bearing California license plate 7RIV310 through LEARN").

Carpenter, 138 S. Ct. at 2217 n.3 (period of location data accessed by government is "pertinent period" for determining whether a search occurred).

2. Indiscriminate Collection of Data.

An equally important factor in the *Carpenter* Court's decision was the recognition that cell phone tracking allows the government to track essentially any person at any time. "[T]his newfound tracking capacity runs against everyone," the Court wrote, and "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *Id*. at 2218.

The same is true of ALPR systems. For the vast majority of Americans, the choice to drive on public streets is not a luxury; it is "indispensable to participation in modern society." *Id*. at 2210. In many parts of the country, people have no choice but to drive themselves to work, a grocery store, doctor's office, place of worship, even in some cases to see a neighbor. In one survey, Gallup found that 84% of Americans drive frequently, and 64% drive every day.[64] And once people drive on the public roads or even park in a privately owned lot or in their own driveway, there is little they can do to avoid having their precise location tagged by an ALPR system and made accessible to law enforcement without any suspicion of wrongdoing.

---

[64] Megan Bryan, *83% of U.S. Adults Drive Frequently; Fewer Enjoy It a Lot*, Gallup (July 9, 2018), https://news.gallup.com/poll/236813/adults-drive-frequently-fewer-enjoy-lot.aspx.

3. Retrospective Searches.

The third factor that led the Court in *Carpenter* to distinguish CSLI from traditional law enforcement surveillance was "the retrospective quality of the data" which "gives police access to a category of information otherwise unknowable." *Id*. at 2218. As the Court explained, CSLI is akin to a time machine that allows law enforcement to look at a suspect's past movements, something that would be physically impossible without the aid of technology: "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers." *Id*. ALPR records provide equivalent capabilities.

The similarly retrospective nature of ALPR systems is illustrated by the facts in this case. Mr. Yang was not a suspect when the plate was scanned but only became one after the postal inspector reviewed security camera footage from the crime scene and queried the license plate of the vehicle in the footage in the LEARN database. Without this technology, the inspector would not have known where to search for the vehicle rented to Mr. Yang.[65] ER 018. Like CSLI, the lengthy and frequently unlimited retention periods for ALPR data allow these

[65] The rental agreement signed by Mr. Yang did not list the address where the postal inspector located the GMC Yukon, nor was the rental agency aware of its location until it was notified by the postal inspector. *See* ER 023, 433.

retrospective searches. *See Carpenter*, 138 S. Ct. at 2218 (retention periods of up to 5 years); *cf. supra*.

The confluence of these factors—detailed location data collection about a vast swath of the American population allowing retrospective searches—is why technologies like ALPRs violate expectations of privacy under the Fourth Amendment. "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Carpenter*, 138 S. Ct. at 2219. And access to technologies like these is "remarkably easy, cheap, and efficient compared to traditional investigative tools," *id*. at 2218, thereby upending traditional protections against pervasive government monitoring on which Americans have long relied.

III. SEARCHES OF ALPR DATABASES REQUIRE A WARRANT.

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

As the Supreme Court recently reiterated in *Carpenter*, warrantless searches "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" are typically unreasonable absent limited and specific exceptions.

Carpenter, 138 S. Ct. at 2221 (citing *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995)). None of those exceptions apply here.[66]

Here, unlike *Carpenter*, law enforcement did not seek or obtain *any* court process prior to searching the database. *See Carpenter*, 138 S. Ct. at 2221 (Government obtained CSLI records pursuant to a court order issued under the Stored Communications Act, which required it to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation"). It did not even obtain the data pursuant to a subpoena. *Id*. at 2247 (Alito, J. dissenting) (noting with approval that court order in *Carpenter* "was the functional equivalent of a subpoena for documents"). Yet, as shown above, ALPR data can be just as revealing as CSLI, and therefore individuals maintain a similar reasonable expectation of privacy in it. For this reason, ALPR data should be subject to the same warrant requirement as CSLI—absent a clear showing of exigent circumstances, law enforcement must get a warrant before conducting searches of ALPR data. *See id*. at 2223.

---

[66] Notably, in *Jones* the Court did not apply the so-called automobile exception to justify warrantless tracking of the location of a car. *See* 565 U.S. at 410 n.7. *See also United States v. Katzin*, 732 F.3d 187, 204 (3d Cir. 2013) (holding that the automobile exception does not permit warrantless GPS tracking of a vehicle because the exception does not "permit [police] to leave behind an ever-watchful electronic sentinel in order to collect future evidence" based on the location of the car), *rev'd en banc on other grounds*, 769 F.3d 163 (3d Cir. 2014).

This case involved data collected by private contractors and maintained for Vigilant's business purposes. For this reason, the postal inspector's search of that data could be analyzed along the same course as the privately collected CSLI data in *Carpenter*. However, ALPR data collected initially by law enforcement should be treated no differently, and a warrant would also be required to search through that data. For one, law enforcement's own collection and retention of large quantities of location data is a Fourth Amendment search. *See Jones*, 656 U.S. at 415–16 (Sotomayor, J., concurring); *id*. at 429–31 (Alito, J., concurring in the judgment). Moreover, even if that initial collection and retention were considered reasonable without a warrant, that does not insulate a further search of that data if it is conducted to find evidence of criminal wrongdoing. *See, e.g., Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602, 616 (1989) (disaggregating initial physical collection of a blood or breath sample from secondary search through "ensuing chemical analysis of the sample to obtain physiological data"). Case law shows that a warrant may be required to conduct later searches of even lawfully collected data. For example, in *United States v. Sedaghaty*, this Court required investigating agents to obtain a new warrant before searching computer hard-drives that had been lawfully seized pursuant to an earlier warrant. 728 F.3d 885, 913 (9th Cir. 2013); *see also United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014) (reversed on other grounds) (same); *United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir.

2013); *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999); *United States v. Hulscher*, No. 4:16-CR-40070-01-KES, 2017 WL 657436 (D.S.D. Feb. 17, 2017) (law enforcement must obtain a warrant to search data lawfully-collected by a different agency for a different purpose). Thus, any search of a database of mass, suspicionless ALPR data, whether collected by law enforcement agencies or private entities, requires a warrant.

CONCLUSION

For these reasons, this Court should reverse the district court and hold that the government's use of ALPR systems in this case was a search requiring a warrant. The ALPR scan should be suppressed, as should all evidence gathered as a result of that scan.

Dated: March 18, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch

Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
jlynch@eff.org
andrew@eff.org

Counsel for Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Nevada

Additional counsel listed on following page.

Nathan Freed Wessler
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: 212-549-2500
nwessler@aclu.org
bkaufman@aclu.org

Jennifer S. Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel.: 415.343.0758
jgranick@aclu.org

Amy M. Rose
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
601 S. Rancho Drive, Suite B11
Las Vegas, Nevada 89106
Tel.: 702-366-1536
rose@aclunv.org

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Nevada in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,968 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: March 18, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on March 18, 2019.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: March 18, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch

Counsel for Amici Curiae