1st. Civ. No. A150198

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
FIRST APPELLATE DISTRICT, DIVISION 5

PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff - Respondent,
v.

JOAQUIN GONZALES,

Defendant - Appellant.

Appeal from the Superior Court for the County of Alameda
The Honorable Leo Dorado, Judge Presiding
Case No. H58965

BRIEF OF AMICI CURIAE THE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA IN SUPPORT OF DEFENDANT-APPELLANT JOAQUIN GONZALES

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 (SBN 240701)
Andrew Crocker (SBN 291596)
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 Foundation, and American Civil Liberties Union Foundation of Northern California

Additional counsel listed on following page.

Jennifer S. Granick (SBN 168423)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel.: 415-343-0758
jgranick@aclu.org

Vasudha Talla (SBN 316219)
Matthew Cagle (SBN 286101)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Tel.: 415-621-2493
vtalla@aclunc.org
mcagle@aclunc.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTRODUCTION AND SUMMARY OF ARGUMENT

In 2017, the California Supreme Court recognized the power of Automated License Plate Reader (ALPR) data to reveal intimate details of our lives. The Court held that "ALPR data showing where a person was at a certain time could potentially reveal where that person lives, works, or frequently visits." *ACLU Found. v. Super. Ct.*, 3 Cal. 5th 1032, 1044 (2017). And yet, for many years now, with little to no oversight, law enforcement agencies and private companies have been quietly using ALPRs to scan and record the locations of billions of vehicles' license plates across the country.

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. ALPR systems collect and store data on every vehicle they encounter, 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 if agencies do not collect their own data or maintain their own databases. Some agencies purge their data after a limited period of time, but in many cases, this data is retained for more than five years or even 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 may be 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 v. United States,* 138 S. Ct. 2206, 2214 (2018) (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 "a too permeating police surveillance," *id*. (quotation marks and citation omitted), the Fourth Amendment's warrant requirement applies. And because the government has not shown in this case that an exception to the warrant requirement justifies 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.

ALPR cameras automatically capture images of every license plate that comes into view.[1] They are mounted on vehicles like squad cars (frequently with four to six

[1] 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.*, Excerpts of Record 209, *United States v. Yang*, No. 18-

cameras for each vehicle), on fixed objects like street light poles, and even on movable trailers that can be placed temporarily and covertly at locations of interest.[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 also record extremely detailed GPS coordinates for each plate scanned. For example, the coordinates of the two scans introduced in this case placed the license plate to within three house numbers on a street.[5] Officers using the system can access even more precise GPS

10341 (9th Cir.) , Dkt. No. 7 (Testimony of Todd J. Allen Hodnett), ("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). *Id.*

[2] The Center for Human Rights and Privacy, *Northern California Fusion Center Has 3 Covert ALPR Trailers to Loan Out*, https://www.cehrp.org/northern-california-fusion-center-has-3-covert-alpr-trailers-to-loan-out/.

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

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

[5] *See* People's Exhibit 32 at 4.

information, accurate enough to record an ALPR camera's location to a 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 while they are operating.[8] Fixed ALPRs have a continuous connection to an ALPR server. Depending on their placement, ALPRs also scan vehicle plates 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]

ALPR systems and databases are maintained and used by both government agencies and private companies. Surveys conducted in 2013 by the federal Bureau of

---

[6] *See* LA Sheriff's Dept. *Automated License Plate Reader (ALPR) Training Presentation* at 9, available at https://www.eff.org/node/74081 (listing GPS coordinates with 5 and 6 decimal places); Excerpts of Record 431-32, *United States v. Yang*, No. 18-10341 (9th Cir.), Dkt. No. 7 (ALPR cameras recorded with six decimal places); *Decimal degrees*, Wikipedia, https://en.wikipedia.org/wiki/Decimal_degrees (noting at six decimal places, GPS 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] Hodnett Testimony, ER 193-194.

[9] *See* 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.

Justice Statistics found that 93% of police departments in cities with 1 million or more people, as well as 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.

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. For example, in the Bay Area over the course of 11 months in 2016 and 2017, Vallejo scanned 21.7 million plates, Piedmont scanned 21.3 million plates, and Fremont scanned 14.5

---

[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).

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

million plates.[14] One stationary ALPR camera mounted in Fremont on westbound Stevenson Boulevard near the entrance to northbound Interstate 880 collected an average of 14,736 license plates and photographs each day during October 2017. ALPR systems maintained by other agencies around the country collect similarly large volumes of data. Los Angeles Police Department (LAPD) and Sheriff's Department together collect data on 3 million cars every week, and the Sheriff's Department, on its own, scanned 234.4 million plates during 2016 and 2017.[15] The City of Atlanta processes nearly 30 million plates each month using just 347 ALPR cameras.[16]

Local, state, and federal agencies are also now pooling their data through many independent, quasi-governmental regional databases. According to the State, fifty agencies in the San Francisco Bay Area share ALPR data via the Northern California Regional Intelligence Center (NCRIC). Respondent's Br. at 13. In the Los Angeles

---

[14] The Center for Human Rights and Privacy, *Fremont: 14.5 million vehicles scanned in 11 months*, https://www.cehrp.org/fremont-14-5-million-vehicles-scanned-in-11-months; NCRC ALPR Data Dec. 2016 – Oct. 2017, https://www.documentcloud.org/documents/6025063-NCRIC-ALPR-Data.html.

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

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

area, at least 26 agencies share data with each other.[17]

Private-vendor ALPR databases—which are also accessible to law enforcement—dwarf these government-maintained databases. In this case, the State obtained ALPR data directly from the NCRIC regional database. However, NCRIC also shares its data through a private database called LEARN that is maintained by Vigilant Solutions.[18] The LEARN database allows agencies across the country to pool their data. In a 2018 nationwide survey of 173 agencies, researchers from MuckRock and EFF found that agencies that contract with Vigilant for ALPR services collected more than 2.5 billion plate scans.[19] The agencies can choose with whom they share their data, and the same survey found that most agencies "were sharing data directly with around 160 other agencies."[20] 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. Through the LEARN database, NCRIC shares its own data with 59 other agencies across the country and has access to data from more than

---

[17] LA Sheriff's Dept. *Automated License Plate Recognition (ALPR) System* at 10 (Sept. 5, 2012), https://www.eff.org/files/2014/01/27/eff-aclu_alpr_pb_dec_exs_a-d.pdf.

[18] LEARN, *Agency Sharing Data Report*, *available at* http://www.documentcloud.org/documents/4502425-Data-Sharing-Report-Northern-California-Regional.html. Many of these agencies—like the Duluth Police Department, Monroe County Sheriffs Office, and Saugerties Police Department—have no apparent ties to the Bay Area.

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

[20] *Id*.

130 agencies.

The LEARN database includes not just data collected by law enforcement and other government agencies, but also commercially collected data. Vigilant's partner company, DRN, employs private contractors to collect plate scan data, which it markets to insurers, repossession companies, and others.[21] Private entities like shopping malls also collect and contribute data.[22] The LEARN database combines the commercial and government ALPR data, providing real-time and retrospective access to government agencies across the country.[23] Vigilant's marketing materials say the LEARN database is growing at a rate of 120 million plate scans a month, and DRN's commercial database alone currently includes over 6.5 billion scans.[24]

Even government agencies that do not maintain their own ALPR systems 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

---

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

[22] Taylor Hatmaker, *California malls are sharing license plate tracking data with an ICE-linked database*, Tech Crunch (Jul. 10, 2018), https://techcrunch.com/2018/07/10/alpr-license-plate-recognition-ice-irvine-company/

[23] *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").

[24] *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").

other agencies across their regions and also nationwide. For example, NCRIC shares its data with the IRS, Department of Homeland Security, FBI, National Park Service, U.S. Forest Service, and the California Department of Insurance, many of which may not have their own ALPR scanning systems or do not operate them in the Bay Area.[25]

Although the State asserts NCRIC retains ALPR data for one year, private vendors and other law enforcement agencies—some of which may be sharing their data via NCRIC's partnership with Vigilant—retain ALPR data for longer periods. In a survey of national ALPR use conducted by George Mason University, 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.[26] There are no indications that Vigilant ever purges its privately collected license plate data.[27]

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 almost all of the data collected is about drivers who are under no suspicion of criminal activity or risk to public safety. Public records requests in California have

---

[25] The Center for Human Rights and Privacy, *Fremont: 14.5 million vehicles scanned in 11 months*, https://www.cehrp.org/fremont-14-5-million-vehicles-scanned-in-11-months/; LEARN, *Agency Sharing Data Report*, *available at* http://www.documentcloud.org/documents/4502425-Data-Sharing-Report-Northern-California-Regional.html.

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

[27] *See* Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU (Jan. 25, 2016, 10:30 AM), https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

revealed, for example, that out of nearly 4 million plates scanned by three cameras maintained by the Central Marin Police Authority, only 985 plates—0.025%—were linked to criminal activity.[28] That means 99.975% of the data—3,995,111 plate scans—was collected from vehicles under no suspicion. Similar rates were recorded in other California Bay Area cities, including Piedmont (0.028%),[29] Dublin (.09%),[30] Fairfield (0.09%),[31] and Livermore (.01%).[32] Of the 173 agencies surveyed by EFF and MuckRock, "on average, only .5%—that is, one half of one percent—of license

---

[28] *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* ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* 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, a fraction of 1 percent of reads are hits — and an even smaller fraction result in an arrest).

[29] The Center for Human Rights and Privacy, *Piedmont License Plate Reader Analysis Shows 99.97% of Data Collected is Useless*, https://www.cehrp.org/piedmont-license-plate-reader-analysis-shows-99-97-of-data-collected-is-useless/

[30] Dublin Police Department, *Agency Dashboard Detection Report*, *available at* https://www.documentcloud.org/documents/4858004-Dublin-Police-Department-OH-Detection-Hits-2017.html

[31] Fairfield Police Department, *Dashboard Hit Ratio Report*, *available at* https://www.documentcloud.org/documents/4439320-Fairfield-Police-Department-Hit-Ratio-Report.html

[32] Livermore Police Department, *Dashboard Hit Ratio Report*, *available at* https://www.documentcloud.org/documents/4936555-Livermore-Police-Department-Detections-Hits-2016.html. *See also* Maass & Lipton, *supra* note 20. ("99.5% of the license plates scanned were not under suspicion at the time the vehicles' plates were collected").

plate scans" were linked to a hotlist.[33]

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

As even NCRIC has recognized, ALPRs impact individuals' privacy rights.[34] ALPR scans can be used to identify individuals and learn sensitive details about their lives. They can be used to scan and record vehicles at a lawful protest or house of worship,[35] track all cars that enter or leave a town,[36] gather information about certain neighborhoods[37] or organizations, or place political activists on "hot lists" so that their movements trigger alerts.

Law enforcement agencies across the country already recognize the power of ALPR data to identify *individuals*, not just their vehicles. NCRIC notes that license

---

[33] Maass & Lipton, *supra* note 20.

[34] NCRIC, *Northern California Regional Intelligence Center Initial Privacy Impact Assessment for Automated License Plate Reader Technology*, https://ncric.org/html/NCRIC%20ALPR%20PIA.PDF; *see also* 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.

[35] *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.

[36] 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.

[37] *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.

plate numbers can be used to determine a vehicle's registered owner as well as information about them.[38] LAPD has said that 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 "can lead to identification of those persons/witnesses associated" with plate scans.[41]

Even a small amount of ALPR data can reveal a person's identity as well as sensitive information about that person. The quantity of location data points that ALPRs record depends on the density of ALPR cameras in a given area, but even where the cameras are relatively less densely deployed, ALPR data can be just as

---

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

[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] Tex. Dep't of Pub. Safety, *Privacy Impact Assessment for the Texas Department of Public Safety (DPS) Collection, Storage, Management and Use of Automated License Plate Reader Data* at 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. April 28, 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.

revealing as other kinds of tracking technology like GPS devices or cell phone location information. Scientists working with location data have determined that, given humans' unique patterns of travel, "even coarse datasets provide little anonymity."[42] These researchers found they could uniquely characterize 50% of people using only two randomly chosen time and location data points.[43]

Because ALPR data may be retained for many years, ALPR datasets almost always include many more than two data points on each vehicle. For example, here NCRIC recorded 92 scans of Mr. Gonzales' license plate. By storing data for long periods of time, ALPR databases allow officers to query a car's past locations for years into the future. This allows officers to make inferences about individuals that they could not have made without such historical data. For example, ALPR data can reveal not only where a driver was on a given date and time in the past, but can also suggest where a driver may be in the future.[44] NCRIC recognizes in its privacy impact assessment that ALPR data, "particularly when collected over an extended period of

---

[42] 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.

[43] *Id*.

[44] State of New Jersey, *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* at 4 (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").

time—could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities."[45]

When ALPR systems are linked to sophisticated algorithms, officers can learn even more about drivers and their driving patterns. LAPD's system, designed by Palantir, 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] LAPD's system also uses "machine learning to recognize the color, make, and style of vehicles photographed by ALPR cameras, as well as accessories like spare tires."[48] This allows officers to easily search by, for example, a vehicle's distinctive color, not just its plate number. These tools can also display the plate numbers of all vehicles that were in a given area at a given time,[49] which can reveal not only who was at that location but also potential

---

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

[46] 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..

[47] *Id*.

[48] *Id*.

[49] *Id*.

associations among drivers, such as drivers traveling together.[50]

For private ALPR vendors, the ability to identify, track, and learn detailed information about actual people is the entire point—and vendors explicitly market their technology to law enforcement on that basis. For example, Vigilant's website has advertised that "90 percent of the time individuals are within 1,000 feet of their car."[51] Its training materials state that "LPR isn't just an enforcement tool; it can assist with keeping track" of people.[52] 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."[53] 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.[54] Vigilant also markets a face recognition technology that could be used, along with ALPR, to identify individuals from the photographs collected as part of the license plate scan.[55]

---

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

[51] Hodnett Testimony, ER 337-38.

[52] 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).

[53] *Id*. at 131.

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

[55] *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

Across the country, people have already used license plate data to identify individuals and their personal characteristics and habits. In August 2012, the Minneapolis *Star Tribune* published a map displaying the 41 locations where license plate readers had recorded the mayor's car in the preceding year.[56] 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.[57] 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.[58] *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 bar and a much larger cluster 24 blocks north in a residential area—likely the driver's home."[59] 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

---

enhance investigations").

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

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

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

[59] *Id*.

driveway.[60]

Two state supreme courts, including California's, have raised alarms about the power of ALPRs to identify individuals and sensitive information about their lives. The California Supreme Court recognized that ALPR data "could potentially reveal where [a] person lives, works, or frequently visits [and] . . . could also be used to identify people whom the police frequently encounter, such as witnesses or suspects under investigation." *ACLU Found.*, 3 Cal. 5th at 1044. Likewise, 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 . . . 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 (2018). On remand, the Virginia trial court held the retention of ALPR data not linked to an active investigation violated state law and required the Fairfax police department to purge their data.[61]

---

[60] Winston, *supra* note 7; Int'l Assoc. of Chiefs of Police, *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, 11 (Sept. 2009), https://www.theiacp.org/sites/default/files/all/k-m/LPR_Privacy_Impact_Assessment.pdf (noting "Certain contextual photos may contain digital images of the vehicle's driver and/or passengers").

[61] Nathan Sheard & Jennifer Lynch, *Victory! Fairfax, Virginia Judge Finds that Local Police Use of ALPR Violates the State's Data Act*, Electronic Frontier Foundation (Apr. 16, 2019), https://www.eff.org/deeplinks/2019/04/victory-fairfax-virginia-judge-finds-local-police-use-alpr-violates-states-data.

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.[62] Once they were put into use in the 1980s, a report for the Greater London Council Police Committee stated, "The development of [ALPR] use . . . is most alarming. . . . [T]he use of devices that read car number plates automatically, leave mass surveillance as a policy to be determined independently by the police. This possibility in a democracy is unacceptable."[63]

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."[64] And, indeed, communities that have faced excessive police surveillance, including through ALPRs, have feared engaging in political activism,

---

[62] *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.

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

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

expressing religious observance, and exercising other constitutional rights.[65] 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 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 Location and Movements.

Mr. Gonzales had an expectation of privacy in ALPR data accessed by the State because it revealed information about his location and movements over time. This is true despite the fact that his plate was scanned while his car was on a public road. Recent Supreme Court case law has clarified that while individuals may have lessened expectations of privacy in certain information they reveal publicly, "[a]

[65] *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), https://www.law.cuny.edu/wp-content/uploads/page-assets/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

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 Court 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 *Carpenter*, the Supreme Court held that a Fourth Amendment search occurs when the government tracks an individual's movements by accessing cell phone location information ("CSLI"), at least for more than seven days. *Id*. at 2220. The Court recognized that the expectation of privacy at issue was not about "using a phone," but rather in the record of a person's location and movements revealed by data generated by use of the phone. Likewise, here Mr. Gonzales' expectation of privacy was not in individual aspects of his car or its license plate, but in the record of his location and movements as revealed by ALPR data.

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

The State argues that this Court should treat 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* Respondent Br. at 17, 19 (citing *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151 (9th Cir. 2007)). Other than the fact that both

involve 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 U.S. 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. As ICE explains, use of ALPR data "reduc[es] the work-hours required for physical surveillance."[66] Recognizing the potential for technologies like these to enable invasive surveillance on a mass scale, the Supreme 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 State, including *Diaz-Castaneda* and *United States v. Knotts*, 460 U.S. 276

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

(1983), predate *Jones* and *Carpenter* and do not involve sophisticated tracking technologies like ALPR.[67]

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.

In *Carpenter*, the Court laid out several factors to consider when evaluating the Fourth Amendment implications of new tracking technologies like CSLI or ALPR. These include the detailed nature of the data collected, the indiscriminate nature of the data collection, and the ability to conduct retrospective searches. ALPR data implicates all of these factors.

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

[67] The State also relies on *United States v. Yang*, No. 2:16-cr-231- RFB, 2018 WL 576827 (D. Nev. Jan. 25, 2018), but fails to note that the district court's decision is currently on appeal to the Ninth Circuit. *See United States v. Yang*, No 18-10341 (9th Cir.)

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 to 100 feet); *supra* at pp. 12-13 (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. As the Supreme Court explained in *Carpenter*, "[m]apping 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)). ALPR data raises identical concerns.

Although ALPR systems may sometimes compile fewer individual data points than GPS tracking or CSLI, even a small number of ALPR data points facilitate inferences about individuals' travels habits, including the homes, businesses and neighborhoods they frequent. *See supra* 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 officer did in this case, they search the millions of records it contains.[68] As a result, this is a search of long-term location data even though agents may only rely on a small number of records produced in response to their queries. *See Carpenter*, 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 the 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

[68] Although in this case, only two ALPR records or "reads" were introduced in evidence, the officer appears to have requested searched of the database for nearly 18 months of data—from June 2014 to December 2015—result in 92 reads. *See* People's Exhibit 32.

some cases to see a neighbor. In one survey, Gallup found that 84% of Americans drive frequently, and 64% drive every day.[69] ALPR systems are indiscriminate. They scan the plates of all cars that come into view, not just those owned or driven by suspected criminals. 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 logged by an ALPR system and made accessible to law enforcement without any suspicion of wrongdoing.

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.

In *Carpenter*, law enforcement was able to access location data that was

[69] 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.

collected five to six months in the past. *See United States v. Carpenter*, No. 12-20218, 2013 U.S. Dist. LEXIS 172508, at *3 (E.D. Mich. Dec. 6, 2013) (robberies occurred as early as Dec. 13, 2010, but CSLI was not requested until May 2 and June 7, 2011). The similarly retrospective nature of ALPR systems is illustrated by the facts in this case. Mr. Gonzales was not a suspect when his vehicle's plate was scanned, and the State concedes it did not have enough evidence to arrest him at first. Respondent's Br. at 12.[70] However, he was arrested five months after the scan when an officer queried the license plate of a vehicle recorded by a witness's video in the NCRIC database. Like CSLI, the lengthy retention periods for ALPR data allow these 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

[70] *See* People's Exhibit 32 at 2 (showing 91 scans between June 1, 2014 and December 15, 2015).

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. *Robey v. Superior Court*, 56 Cal. 4th 1218, 1224 (Cal. 2013) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967)).

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. Notably, in *Jones* the Court did not apply the so-called automobile exception, raised by the State here, 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); *Collins v. Virginia*, 138 S. Ct. 1663, 1673 (2018) (rejecting argument that "the automobile exception is a categorical one that permits the warrantless search of a vehicle anytime, anywhere").

Here, unlike *Carpenter*, law enforcement did not seek or obtain *any* court

process prior to searching NCRIC's ALPR 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"). 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.

Even if the initial collection and retention of ALPR data were considered reasonable, that would not insulate a further query of that data without a warrant if that search is conducted to find evidence of criminal wrongdoing. *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*, the Ninth Circuit Court of Appeals 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 requires a warrant.

CONCLUSION

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

Respectfully submitted,

Dated: May 28, 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

Vasudha Talla (SBN 316219)
Matthew Cagle (286101)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Tel.: 415-621-2493
vtalla@aclunc.org
mcagle@aclunc.org

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this Amicus Brief of Electronic Frontier Foundation, s proportionally spaced, has a typeface of 13 points or more, contains 7,194 words, excluding the cover, the tables, the signature block, verification, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: May 28, 2019

/s/ Jennifer Lynch
Jennifer Lynch

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

The undersigned declares,

I am over the age of 18 years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On May 28, 2019, I caused to be served copies of the foregoing documents described as:

BRIEF OF AMICI CURIAE THE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA IN SUPPORT OF DEFENDANT-APPELLANT JOAQUIN GONZALES

☑ BY TRUEFILING: I caused to be electronically filed the foregoing document with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website.

☑ BY FIRST CLASS MAIL: I caused to be placed the envelope for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid

I declare under the penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this document was executed on May 28, 2019.

By: /s/ Jennifer Lynch
Jennifer Lynch

SERVICE LIST

Melissa Meth — *Via E-File Service*
Office of the Attorney General
455 Golden Gate Avenue - Suite 11000
San Francisco, CA 94102-7004

Attorneys for Plaintiff -Respondent People of California

First District Appellate Project — *Via E-File Service*
475 Fourteenth Street, Suite 650
Oakland, CA 94612

Walter K. Pyle
2039 Shattuck Avenue - Suite 202
Berkeley, CA 94704

Attorneys for Defendant-Appellant Joaquin Gonzales

Alameda County Superior Court — *Via First Class Mail*
Appeals Division
1225 Fallon Street
Oakland, CA 94612

District Attorney — *Via First Class Mail*
Alameda County
1225 Fallon Street, 9th Floor
Oakland, CA 94612-4229

STATE OF CALIFORNIA California Court of Appeal, First Appellate District	***PROOF OF SERVICE*** **STATE OF CALIFORNIA** California Court of Appeal, First Appellate District

Case Name: **The People v. Gonzalez**
Case Number: **A150198**
Lower Court Case Number: **H58965**

1. At the time of service I was at least 18 years of age and not a party to this legal action.

2. My email address used to e-serve: **jlynch@eff.org**

3. I served by email a copy of the following document(s) indicated below:

Title(s) of papers e-served:

Filing Type	Document Title
APPLICATION - APPLICATION TO FILE AMICUS CURIAE BRIEF	A150198 Gonzales amicus application EFF ACLU
BRIEF - AMICUS CURIAE BRIEF	A150198 Gonzales amicus EFF and ACLU

Service Recipients:

Person Served	Email Address	Type	Date / Time
Jennifer Lynch Electronic Frontier Foundation	jlynch@eff.org	e-Serve	5/28/2019 5:02:41 PM
First District Appellate Project Court Added	eservice@fdap.org	e-Serve	5/28/2019 5:02:41 PM
Walter K Pyle Walter K. Pyle & Associates	walt@wfkplaw.com	e-Serve	5/28/2019 5:02:41 PM
Office Of The Attorney General Court Added	sfagdocketing@doj.ca.gov	e-Serve	5/28/2019 5:02:41 PM
Melissa Meth Attorney General's Office	melissa.meth@doj.ca.gov	e-Serve	5/28/2019 5:02:41 PM
Madeleine Mulkern	madeleine@eff.org	e-Serve	5/28/2019 5:02:41 PM
Andrew Crocker Electronic Frontier Foundation	andrew@eff.org	e-Serve	5/28/2019 5:02:41 PM

This proof of service was automatically created, submitted and signed on my behalf through my agreements with TrueFiling and its contents are true to the best of my

information, knowledge, and belief.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

5/28/2019

Date

/s/Madeleine Mulkern

Signature

Lynch, Jennifer (240701)

Last Name, First Name (PNum)

Electronic Frontier Foundation

Law Firm