



June 25, 2015

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

Honorable Tani Cantil-Sakauye, Chief Justice
and the Associate Justices
Supreme Court of California
350 McAllister Street
San Francisco, CA 94102-4783

Re: *Amicus Letter of the Electronic Privacy Information Center in Support of Petition for Review of American Civil Liberties Union Foundation of Southern California and Electronic Frontier Foundation v. Superior Court for the State of California, County of Los Angeles, Court of Appeal Second Appellate District Case No. B259392, Supreme Court of the State of California Case No. S227106*

Dear Chief Justice Cantil-Sakauye and Associate Justices of the Court:

Pursuant to Rule 8.500(g) of the California Rules of Court, the Electronic Privacy Information Center (“EPIC”) submits this *amicus* letter urging the Court to grant review of the above-entitled case. EPIC supports the arguments made by Petitioners in the Petition for Review.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC promotes open government, litigates federal Freedom of Information Act (“FOIA”) cases, and provides information to the public obtained as a result of FOIA litigation.

EPIC routinely participates as *amicus curiae* before federal and state courts concerning emerging civil liberties issues: *See, e.g., Los Angeles v. Patel*, No. 13-1175 (U.S. June 22, 2015) (searches of hotel records), *Riley v. California*, 134 S. Ct. 2473 (2014) (cellphone searches); *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) (Standing for Fourth Amendment challenges); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (reliability of search techniques); *United States v. Jones*, 132 S. Ct. 945 (2012) (GPS tracking); *Herring v. United States*, 555 U.S. 135 (2009) (searches based on inaccurate government databases); *Hübel v. Sixth Judicial Dist. Ct. of Nevada, Humboldt Cty.*, 542 U.S. 177 (2004) (demands for identification); *State v. Earls*, 214 N.J. 564 (2013) (Cell phone tracking); *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (GPS tracking).

EPIC has a longstanding interest in promoting safeguards for personal privacy and increased government transparency. In particular, EPIC works to ensure new surveillance

technologies do not erode our core constitutional protections. Pervasive mass surveillance techniques offend the right of individuals to go about their daily lives freely without the threat of constant tracking. EPIC has previously urged regulators and courts to take meaningful steps towards protecting the privacy interests of motorists. *See, e.g.* Comments of EPIC to the National Highway Traffic Safety Administration, August 13, 2004, Docket No. NHTSA-2004-18029, (supporting strong privacy safeguards for automobile Event Data Recorders (EDRs), including a clear consumer right to control the collection and dissemination of their driving data);¹ Brief for EPIC *et al.* as *Amici Curiae* Supporting Petitioner, *Herring*, 555 U.S. 135 (2009) (advocating for suppression of evidence obtained from search of error-prone criminal justice record systems); Brief for EPIC as Amicus Curiae Supporting Appellant, *Connolly*, 454 Mass. 808 (2009) (arguing that absent a warrant requirement, GPS tracking systems in the law enforcement context threaten to enable pervasive mass surveillance); Brief for EPIC *et al.* as Amici Curiae Supporting Respondent, *Jones*, 132 S. Ct. 945 (2012) (arguing that police must obtain a warrant prior to monitoring a GPS tracking device on an individual's car).

Open record laws, such as California's Public Records Act, ensure citizens' right to access public information and help proper oversight of government activities. Law enforcement programs that are based on the routine collection of personal information absent any suspicion of criminal conduct require careful oversight. These are almost precisely the government programs for which open government laws are established.²

EPIC support's Petitioners argument that data collected by Automatic License Plate Readers ("ALPRs") are not law enforcement records of investigations and thus not exempted under Gov't Code § 6254(f). The Court should grant review and decide this case to ensure that Gov't Code § 6254(f) is not used as a broad exemption to shield law enforcement's indiscriminate bulk collection from public scrutiny.

I. The Role of Open Record Laws

As the government's ability to collect information about individuals has expanded, open record laws have become an important tool for government oversight. The federal Freedom of Information Act is celebrated every year on the birthday of President James Madison, who wrote, "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."³

Access to government records is such a fundamental right of citizenship in California that "the right of access to information concerning the conduct of the people's business" is enshrined in Article 1 of the California Constitution. In 2004, California voters overwhelmingly approved Proposition 59, amending the California Constitution to require that "[a] statute, court rule, or

¹ Available at https://epic.org/privacy/drivers/edr_comm81304.html.

² See 154 Cong. Rec. S201-S202 (Jan. 23, 2008) (statement of S. Leahy) ("More than two centuries ago, Patrick Henry proclaimed that '[t]he liberties of a people never were, nor ever will be, secure, when the transactions of their rulers may be concealed from them.' I could not agree more. ").

³ Marc Rotenberg *et al.*, *The Open Government Clinic: Teaching the Basics of Lawyering*, 48 Ind. L. Rev. 149, 154-55 (2014) (quoting Letter from James Madison, former President of the United States, to W. T. Barry, Lieutenant Governor of Kentucky (Aug. 4, 1822) (on file with the Library of Congress)).

other authority, including those in effect on the effective date of this subdivision, shall be broadly construed if it furthers the people's right of access, and narrowly construed if it limits the right of access." Cal. Const. art. I, § 3(b)(2). Proposition 59 was widely supported—it received unanimous approval by both the California Assembly and the California State Senate prior to receiving the support of eighty-three percent of the electorate.

Open records laws are critical for the functioning of democratic government because they ensure that the public is fully informed about matters of public concern.⁴ As this Court recognized in *CBS v. Block*:

Implicit in the democratic process is the notion that government should be accountable for its actions. In order to verify accountability, individuals must have access to government files. Such access permits checks against the arbitrary exercise of official power and secrecy in the political process.

725 P. 2d 370 (1986). In this case, blocking public access to the bulk collection of innocent residents' location data eliminates the public's right to place checks on the arbitrary exercise of law enforcement's official power.

Public scrutiny of government actions is essential to a healthy democracy. Transparency facilitates public oversight, which is particularly important in the law enforcement context where surveillance capabilities could be used to invade the privacy of innocent citizens.

In California, public access to information about government programs has often led to greater protection for individual privacy. For example, in 2014, the San Jose Police Department ("SJPD") obtained and attempted to use a surveillance drone without public notice.⁵ Once the community became aware of the drone, the public's strong objections resulted in a public meeting with San Jose police officials.⁶ This public scrutiny of the drone's usage led directly to a department commitment to use the drone only for specific purposes, rather than general surveillance.⁷ Additionally, the SJPD has tabled the use of the drone and committed to a community outreach effort in order to develop policies and procedures limiting drone surveillance.⁸

This example of public oversight of drone deployment in San Jose, enabled by public awareness of the program, is precisely on point for the matter now before the Supreme Court of California. An expansive application of Section 6254(f) would prevent public oversight of new surveillance programs, weaken democratic institutions, and leave the public in the dark about government surveillance programs that impact upon them, their families, and neighbors.

⁴ Maria H. Benecki, *Developments Under the Freedom of Information Act—1987, 1988* DUKE L.J. 566, 600, 605 (1988) (recognizing that public interests are served by disclosure).

⁵ Robert Salonga, *Drones Over San Jose: Worries Fly at Public Hearing*, San Jose Mercury News, Nov. 13, 2014, http://www.mercurynews.com/crime-courts/ci_26927967/san-jose-drone-debate-launches-citys-first-public.

⁶ *Id.*

⁷ Matt Bigler, *Controversial Police Drone Inches Closer to Flight in San Jose*, CBS San Francisco, Apr. 9, 2015, <http://sanfrancisco.cbslocal.com/2015/04/09/a-controversial-police-drone-inches-closer-to-flight-in-san-jose/>.

⁸ Press Release: San Jose Police Provide Statement Regarding Purchase of Unmanned Aerial System (UAS), Aug. 5, 2014, <http://www.sjpd.org/iNews/viewPressRelease.asp?ID=1874>.

II. Implications for Indiscriminate Bulk Collection by Law Enforcement

ALPR systems indiscriminately collect the license plate data of every passing vehicle. As we have previously explained:

Automated License Plate Reader (ALPR) systems employ optical recognition on video images in order to read license plates on motor vehicles. These camera systems can be mounted on motor vehicles, such as police cars, or placed in stationary locations, affixed to the entrances of bridges, tunnels, or other landmarks. The data gathered by the ALPRs can be stored, compared to information in databases, or linked to other applications.⁹

The opinion of the Court of Appeals that this sweeping bulk data collection is exempt from disclosure because it is a law enforcement investigatory record has far reaching implications, preventing the public from acting as a check on overreach by law enforcement agencies. With the Court of Appeal's broad expansion of the term "investigation", law enforcement can easily conceal bulk collection from public scrutiny.

New surveillance technologies that facilitate indiscriminate bulk collection are becoming very inexpensive to procure and operate. As a result, these devices are being deployed broadly by state and local law enforcement agencies across the country, including in California. Many of these new devices, including police body cameras, drones, and Stingrays are already being used to collect sensitive personal information about innocent citizens.¹⁰

Body cameras are currently being integrated into a number of law enforcement agencies in California and other parts of the nation.¹¹ Body cameras point outwards towards the public capturing data on numerous people not suspected of a crime as officers patrol their beat. In the UK, facial recognition has already been coupled with body cameras.¹² Body cameras with facial recognition capabilities have the potential to collect massive amounts of data on the public similar to the way ALPR systems indiscriminately collect data in bulk on passing motor vehicles. The consequence would be to turn a device meant for police accountability into a device of mass surveillance shielded from public scrutiny.

As the US integrates drones into the national airspace, the cost of performing massive aerial surveillance will drop. Drones are a surveillance platform for aerial surveillance and can be combined with ALPR systems, facial recognition technology, and stingrays, among other surveillance technology. As the cost of new surveillance technologies drops and there

⁹ EPIC, EPIC FOIA: Automated License Plate Readers (FBI), <https://epic.org/foia/fbi/lpr/default.html>

¹⁰ Stingrays are a brand of IMSI Catchers, which are devices that act as fake cell towers capturing the all the data of cell phones within range. See *EPIC v. FBI – Stingray / Cell Cite Simulator* <http://epic.org/foia/fbi/stingray/> (2015).

¹¹ See *Body Cameras: Can Technology Increase Protection for Law Enforcement Officers and the Public Before the H. Subcomm on Crime and Terrorism of the S. Judiciary Comm.*, 114th Cong. (2015) (statement of Jeramie D. Scott, EPIC National Security Counsel), <https://epic.org/privacy/testimony/EPIC-Body-Camera-Statement-05-19-15.pdf>

¹² *Id.* at 3.

deployment increases, enabling bulk collection of private data, it is more necessary than ever to ensure that open records law ensure adequate transparency and public oversight.¹³

This Court should grant review of this case and ensure that the public has the opportunity to assess the privacy consequences of this new program of mass surveillance. Gov't Code § 6254(f) should not render meaningless California's commitment to open government.

Respectfully submitted,



MARC ROTENBERG
EPIC President and Executive Director

ALAN JAY BUTLER
EPIC Senior Counsel

CAITRIONA FITZGERALD
EPIC State Policy Coordinator

JERAMIE SCOTT
EPIC National Security Counsel
Electronic Privacy Information Center
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009

Counsel for Amicus Curiae EPIC

cc: All Counsel

¹³ *Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (“With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.”).

PROOF OF SERVICE BY MAIL

Re: *American Civil Liberties Union Foundation of Southern California and Electronic Frontier Foundation v. Superior Court for the State of California, County of Los Angeles*
Supreme Court of the State of California Case No. S227106

I, Jeramie D. Scott, declare that I am over the age of 18 and not a party to the above action. My business address is 1718 Connecticut Avenue, STE 200, Washington, DC 20009. I served a true copy of the attached Amicus Letter of the Electronic Privacy Information Center in Support of Petitioners on the following by placing a copy in an envelope addressed to the parties listed below, which was then sealed by me and deposited in the United States Mail, postage prepaid, at Washington, DC on June 25, 2015.

Peter Bibring
ACLU Foundation of Southern California
1313 West Eighth St.
Los Angeles, CA 90017
Counsel for ACLU Foundation of Southern California, Petitioner

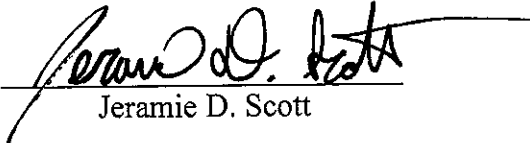
Jennifer Ann Lynch
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
Counsel for Electronic Frontier Foundation, Petitioner

Frederick Bennett
Superior Court of Los Angeles County
111 North Hills St., Room 546
Los Angeles, CA 90012
Counsel for Superior Court of Los Angeles County, Respondent

Tomas A. Guterres and Eric Brown
Collins, Collins, Muir & Stewart LLP
1100 El Centro St.
South Pasadena, CA 91030
Counsel for County of Los Angeles and Los Angeles Sheriff's Department, Real Party in Interest

Heather Leigh Aubry
Office of the City Attorney
200 North Main St, 800 City Hall East
Los Angeles, CA 90012
Counsel for City of Los Angeles and Los Angeles Police Department, Real Party in Interest

I declare under penalty of perjury that the foregoing is true and correct. Executed on June 25, 2015 at Washington, DC.


Jeramie D. Scott