SUPREME COURT COPY

Case No. S227106

SUPREME COURT
FILED
MAY 17 2016
Frank A. McGuire Clerk
Deputy

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA and ELECTRONIC FRONTIER FOUNDATION,

Petitioners,

v.

SUPERIOR COURT FOR THE STATE OF CALIFORNIA, COUNTY OF LOS ANGELES,

Respondent,

COUNTY OF LOS ANGELES, and the LOS ANGELES COUNTY SHERIFF'S DEPARTMENT, and the CITY OF LOS ANGELES, and the LOS ANGELES POLICE DEPARTMENT,

Real Parties in Interest.

After a Decision by the Court of Appeal,
Second Appellate District, Division Three, Case No. B259392
Los Angeles County Superior Court, Case No. BS143004
(Hon. James C. Chalfant)

APPLICATION FOR LEAVE TO FILE *AMICUS CURIAE* BRIEF AND *AMICUS CURIAE* BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PETITIONERS

MARC ROTENBERG, rotenberg@epic.org
*ALAN BUTLER (SBN 281291), butler@epic.org
JERAMIE SCOTT, jscott@epic.org
AIMEE THOMSON, thomson@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave. N.W., Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
Counsel for Amicus Curiae

TO THE HONORABLE TANI GORRE CANTIL-SAKAUYE, CHIEF JUSTICE OF THE SUPREME COURT OF CALIFORNIA:

Pursuant to California Rule of Court 8.250(f), non-profit organization the Electronic Privacy Information Center ("EPIC") respectfully requests leave to file the attached *amicus* brief in support of Petitioners American Civil Liberties Union Foundation of Southern California and Electronic Frontier Foundation. This brief is timely, as it was filed within 30 days after the last reply brief was filed.

STATEMENT OF INTEREST

The Electronic Privacy Information Center is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1] EPIC routinely participates as *amicus curiae* before federal and state courts in cases concerning open government laws. *See, e.g.*, *McBurney v. Young*, 133 S. Ct. 1709 (2013) (arguing that the Virginia Freedom of Information Act's citizens-only provision harms noncitizens' constitutionally protected rights); *FCC v. AT&T Inc.*, 562 U.S. 397 (2011) (arguing that the Freedom of Information Act exemption for "personal privacy" protects individuals, not corporations); *New York*

[1] In accordance with Rule 8.520(f)(4), the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

Times Co. v. DOJ, 756 F.3d 100 (2d Cir. 2014), *opinion amended on denial of reh'g*, 758 F.3d 436 (2d Cir. 2014), *supplemented*, 762 F.3d 233 (2d Cir. 2014) (arguing that memos prepared by the Office of Legal Counsel do not fall within Exemption 5 of the Freedom of Information Act); *Citizens for Responsibility & Ethics in Washington v. FEC*, 711 F.3d 180 (D.C. Cir. 2013) (arguing that a Freedom of Information Act "determination" must include a decision to grant or deny a request).

EPIC has published a leading FOIA litigation manual, EPIC, *Litigation Under the Federal Open Government Laws* (2010), and routinely files Freedom of Information requests and litigates Freedom of Information Act cases. *See, e.g*, *EPIC v. CBP*, ___ F. Supp. 3d ___ (D.D.C. 2016); *EPIC v. DHS*, 117 F. Supp. 3d 46 (D.D.C. 2015); *EPIC v. DOJ Criminal Division*, 82 F. Supp. 3d 307 (D.D.C. 2015); *see generally* EPIC, *EPIC FOIA Cases* (2016).[2]

EPIC's *amicus* brief presents arguments that materially add to and complement the briefs filed by Petitioners, without repeating those arguments. EPIC has significant experience with the federal Freedom of Information Act.

EPIC's brief will argue that the lower court's decision to exclude "investigative" records from public release will prevent

[2] http://epic.org/foia/.

meaningful oversight of programs that pose significant threats to the privacy of everyday Americans.

For all of the foregoing reasons, EPIC respectfully requests that the Court grant the application and accept the enclosed *amicus curiae* brief for filing and consideration.

Dated: May 5, 2016

Respectfully submitted,

/s/ Alan Butler

MARC ROTENBERG
ALAN BUTLER
JERAMIE SCOTT
AIMEE THOMSON
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. N.W.,
Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
Counsel for Amicus Curiae

Case No. S227106

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA and ELECTRONIC FRONTIER FOUNDATION,

Petitioners,

v.

SUPERIOR COURT FOR THE STATE OF CALIFORNIA, COUNTY OF LOS ANGELES,

Respondent,

COUNTY OF LOS ANGELES, and the LOS ANGELES COUNTY SHERIFF'S DEPARTMENT, and the CITY OF LOS ANGELES, and the LOS ANGELES POLICE DEPARTMENT,

Real Parties in Interest.

After a Decision by the Court of Appeal,
Second Appellate District, Division Three, Case No. B259392
Los Angeles County Superior Court, Case No. BS143004
(Hon. James C. Chalfant)

AMICUS CURIAE BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PETITIONERS

MARC ROTENBERG, rotenberg@epic.org
*ALAN BUTLER (SBN 281291), butler@epic.org
JERAMIE SCOTT, jscott@epic.org
AIMEE THOMSON, thomson@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave. N.W., Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

OTHER AUTHORITIES

SUMMARY OF THE ARGUMENT

Automatic License Plate Readers ("ALPRs") are a technology of mass surveillance. This technology indiscriminately collects personal information, unrelated to any particular investigation, and should be subject to public scrutiny.

The lower court's interpretation of the "investigative record" exemption would undermine the purpose of California's Public Records Act. This is especially troubling given other similar programs—cell-site simulators, police body-worn cameras, and fusion centers—that pose significant threats to the privacy of everyday Americans. Public scrutiny is essential to counter the unique threats posed by these programs of broad-scale surveillance.

EPIC's experience obtaining important information about these programs under the federal FOIA and the reforms that followed demonstrate the need for public access to information about the Automated License Plate Reader technology.

ARGUMENT

I. Open records laws enable public scrutiny of surveillance technologies.

California law enforcement agencies are deploying new surveillance systems—Automated License Plate Readers, cell-site simulators, fusion centers, and police body-worn cameras—that indiscriminately collect data about individuals. These programs raise

substantial privacy concerns. The public's ability to obtain information about these programs is critical to prevent misuse and abuse.

A. Open Records laws have limited the use of cell-site simulators.

A cell-site simulator, also known as a "stingray,"[3] is a surveillance device that can monitor cell phone activity, identify and locate mobile devices, and even intercept mobile communications of individuals who are not the target of any particular investigation. Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J. L & Tech. 1, 16–18 (2014); Aimee Thomson, *Cellular Dragnet: Active Cell Site Simulators and the Fourth Amendment* 5–10 (Jan. 14, 2015).[4]

Prior to the release of documents under federal and state open government laws, *see, e.g.*, EPIC, *EPIC v. FBI - Stingray / Cell Site Simulator* (2016),[5] the public was largely unaware of the widespread

---

[3] The trademark "StingRay" refers specifically to the cell site simulator produced by Harris Corporation. *StingRay & AmberJack,* Harris Corporation, http://files.cloudprivacy.net/Harris_Stingray_product_sheet.pdf (last visited Apr. 29, 2016). The term "stingray," however, has become the genericized term for all cell site simulators.
[4] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546052.
[5] http://epic.org/foia/fbi/stingray/.

deployment of stingrays, and their use was not subject to congressional oversight, *see* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today (Aug. 24, 2015).[6] As a result of these disclosures, Congress convened hearings and the Department of Justice adopted new procedures.

The government has attempted to keep stingray use secret, in part by failing to disclose stingray devices to courts when submitting pen register applications. Pell & Soghoian, *supra*, at 34–40. As a result, state and local police departments have used stingrays thousands of times without judicial or legislative oversight. *See, e.g.*, Brett Clarkson, *Who's Tracking Your Cellphone Now? Could be the Cops*, SunSentinel (May 17, 2014)[7] ("Florida Department of Law Enforcement spokeswoman Gretl Plessinger said in an email: 'This technology has been utilized approximately 1,800 times by FDLE and Electronic Surveillance Support Teams.'").

But public awareness has grown in the last few years, thanks in part to public records requests, *e.g.*, EPIC, *EPIC v. FBI - Stingray / Cell Site Simulator* (2016); ACLU, *Stingray Tracking Devices: Who's*

---

[6] http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

[7] http://articles.sun-sentinel.com/2014-05-17/news/fl-cell-site-simulator-surveillance-florida-20140507_1_stingray-cellphone-simulator.

Got Them?[8] (collecting news reports of cell site simulator operations by state and local law enforcement agencies). In response to EPIC's federal FOIA suit against the FBI, the public first obtained in 2013 "non-disclosure" agreements between federal and state law enforcement agencies that had strictly limited information about stingray use for a decade. Ryan Gallagher, *FBI Files Reveal New Info on Clandestine Phone Surveillance Unit*, Slate (Oct. 8, 2013).[9]

In 2014, Senators Grassley and Leahy wrote to the Attorney General and the Secretary of the Department of Homeland Security regarding the use of cell site simulators. As a result, both agencies adopted procedures to limit the use of the devices. Press Release, Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program (Dec. 31, 2014);[10] DOJ, *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators* (Sept. 3, 2015);[11] Memorandum from Alejandro N. Mayorkas, Deputy Secretary of DHS, to Sarah Saldaña, Assistant Secretary, USCIS; Joseph Clancy, Director, U.S. Secret Service; R. Gil Kerlikowske,

---

[8] https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Apr. 29, 2016).
[9] http://www.slate.com/blogs/future_tense/2013/10/08/fbi_wireless_intercept_and_tracking_team_files_reveal_new_information_on.html.
[10] http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program.
[11] https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

Commissioner, U.S. Customs and Border Protection; Admiral Paul F. Zukunft, Commandant, U.S. Coast Guard; Peter Neffenger, Administrator, TSA; & L. Eric Patterson, Director, Federal Protective Service, at 4 (Oct. 19, 2015).[12]

The concerns about cell-site simulators that prompted the federal FOIA requests and led to the actions by the Congress and the response by federal agencies, have also given rise to changes in California and other states. Public records requests in California have also revealed that at least 13 police and sheriff's departments use stingrays, in addition to the California Department of Justice. They include: Alameda County District Attorney's Office, Anaheim Police Department, Freemont Police Department, Los Angeles Police Department, Los Angeles Sheriff's Department, Oakland Police Department, Sacramento County Sheriff's Department, San Bernardino County Sheriff's Department, San Diego Police Department, San Diego Sheriff's Department, San Francisco Police Department, San Jose Police Department, and Ventura County Sheriff's Department. Michael Bott & Thom Jensen, *9 Calif. Law Enforcement Agencies Connected To Cellphone Spying Technology*,

---

[12] https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf.

ABC 10 News (Mar. 6, 2014);[13] Matt Cagle, *Dirtbox Over Disneyland? New Docs Reveal Anaheim's Cellular Surveillance Arsenal*, ACLU of N. Cal. (Jan. 27, 2016);[14] Jon Campbell, *LAPD Spy Device Taps Your Cell Phone*, LA Weekly (Sept. 13, 2012);[15] Mike Katz-Lacabe, *Ventura County Sheriff Releases Unredacted FBI NDA for Harris StingRay*, Ctr. for Human Rights & Privacy (May 4, 2015);[16] K. Kaufmann, *Law Enforcement Officials: Cell Phone Disclosures Would Hurt Investigations*, Desert Sun (Feb. 15, 2014);[17] Melissa Mecija, *Local Police Dealt With Company That Makes Controversial Cellphone Tracking Technology*, ABC 10 News (Aug. 4, 2014).[18] But California has 509 state and local law enforcement agencies as of 2008 (the most recent census year), so current public knowledge covers only 2.7% of California agencies. Brian A. Reaves, *Census of State and Local Law Enforcement Agencies, 2008*, NCJ

---

[13] http://legacy.abc10.com/story/news/investigations/watchdog/2014/03/06/5-california-law-enforcement-agencies-connected-to-stingrays/6147381/.

[14] https://www.aclunc.org/blog/dirtbox-over-disneyland-new-docs-reveal-anaheim-s-cellular-surveillance-arsenal.

[15] http://www.laweekly.com/news/lapd-spy-device-taps-your-cell-phone-2176376.

[16] http://www.cehrp.org/ventura-county-sheriff-releases-unredacted-fbi-nda-for-harris-stingray/.

[17] http://www.desertsun.com/story/tech/2014/02/16/law-enforcement-officials-cell-phone-disclosures-would-hurt-investigations/5528517/.

[18] http://www.10news.com/news/local-police-dealt-with-company-that-makes-controversial-cellphone-tracking-technology-08052014.

233982, DOJ Bureau of Justice Statistics 15 (July 2011).[19]States have now imposed restrictions on stingray use. California has mandated that police officers in the state obtain a warrant before using stingrays during investigations. Cyrus Farivar, *California Cops, Want To Use a Stingray? Get A Warrant, Governor Says*, Ars Technica (Oct. 8, 2015)[20] (discussing S.B. 178, the California Electronic Communications Privacy Act). Other states have passed similar laws restricting cell phone location tracking. *E.g.*, Leg. Doc. 415, 126th Leg., 1st Reg. Sess. (Me. 2013);[21] S. B. SF 2466, 88th Leg., 3d Engrossment (Minn. 2014);[22] H. B. 603, 63rd Leg., Reg. Sess. (Mont. 2013);[23] H. B. 128, 2014 Leg., Gen. Sess. (Utah 2014).[24]

Although these are promising developments, the public must still be able to review records the use of cell-site simulators. Despite the federal government's self-imposed warrant requirement, House Judiciary Committee leaders also sharply criticized the FBI for limiting disclosure of stingray information in a way that "shields the

---

[19] http://www.bjs.gov/content/pub/pdf/csllea08.pdf.
[20] http://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/.
[21] http://www.mainelegislature.org/legis/bills/bills_126th/chapters/PUBLIC409.asp.
[22] https://www.revisor.mn.gov/bills/text.php?number=SF2466&version=3&session=ls88&session_year=2014&session_number=0
[23] http://leg.mt.gov/bills/2013/billhtml/HB0603.htm.
[24] http://le.utah.gov/~2014/bills/static/hb0128.html.

technology from debate." Letter from Rep. F. James Sensenbrenner, Jr. and Rep. Sheila Jackson Lee to Mr. James B. Comey, Director, FBI (Mar. 25, 2016).[25] Transparency will help ensure agency compliance with newly imposed restrictions. Tim Cushing, *State AG: We Have A Warrant Requirement For Stingrays; State Police: FILE(S) NOT FOUND*, Techdirt (Mar. 2, 2016)[26] (discussing how Delaware State Police have no records of the warrants that the Delaware Attorney General says police must obtain before using stingrays). Transparency will also ensure that law and policy can appropriately respond to technological developments.

B. Police body-worn cameras raise substantial privacy concerns and shoud be subject to public scrutiny

The use of body-worn cameras ("BWCs") is increasing police surveillance of individuals across the country. In December 2014, the Obama Administration budgeted $75 million over three years to subsidize the purchase of 50,000 cameras. White House Press Release, *FACT SHEET: Strengthening Community Policing* (Dec. 1, 2014).[27] In 2015, the Department of Justice's Body-Worn Camera

---

[25] http://sensenbrenner.house.gov/uploadedfiles/stingray_technology_letter.pdf.

[26] https://www.techdirt.com/articles/20160223/12163533688/state-ag-we-have-warrant-requirement-stingrays-state-police-files-not-found.shtml.

[27] https://www.whitehouse.gov/the-press-office/2014/12/01/fact-sheet-strengthening-community-policing.

Pilot Implementation Program awarded nearly $20 million to purchase 21,000 cameras. Office of Justice Programs, DOJ, *Body-Worn Camera Program Fact Sheet.*[28] Six different locales in California were awarded funds through the pilot implementation program. *Id.*

Police body-worn cameras ("BWCs") are audio and video recording devices typically mounted on the chest, shoulder, or head area of the police officer. Bureau of Justice Assistance, DOJ, *Body-Worn Camera Toolkit: Technology* (2016).[29] These devices record the activities of individuals from the viewpoint of the officer. Generally, officers are expected to turn their cameras on whenever they are interacting with civilians in public. *Id.* Most body cameras also have a buffer to capture anywhere from 3-60 seconds of the footage prior to initiation, which means that they are recording at all times. National Institute for Justice, National Law Enforcement and Corrections Technology Center System, *Body-Worn Cameras for Criminal Justice: Market Survey* (Mar. 2014). The buffer or pre-event recording typically only includes the visual aspect but some BWCs also record audio. *See id.*

BWCs systems range in their technical capabilities. Most body cameras record in high definition at a minimal speed of 30 frames per

---

[28] https://www.bja.gov/bwc/pdfs/BWCPIP-Award-Fact-Sheet.pdf.
[29] https://www.bja.gov/bwc/Topics-Technology.html.

second. National Institute for Justice, *supra*. The cameras can record from 3-12 hours of video on one charge and often have a night mode for dark conditions. *Id.* Most if not all body cameras include a date and time stamp of the recordings and several BWC systems have GPS capabilities. *Id.*

The widespread use of BWCs will sharply increase indiscriminate surveillance of the public. In Los Angeles, one of the departments that received federal funding, law enforcement agencies are planning to purchase an additional 6,000 cameras to add to their 860 current BWCs. Kate Mather, *LAPD Report Defends Ambitious Plan to Outfit Officers with Body Cameras*, L.A. Times (Mar. 18, 2016). Last year between August and December the LAPD recorded and uploaded an average of 237 hours of BWC per day. LAPD, *LAPD's Body Worn Video Program – Supplemental Report* (Mar. 16, 2016).[30]

As the use of BWCs has expanded, so has the interest in using the cameras as a tool of surveillance. The body camera vendor, Strategic Systems Alliance, has body cameras capable of performing license plate and facial recognition.[31] Police in Colorado have already expressed interest in body cameras with facial recognition

---

[30] http://www.lapdpolicecom.lacity.org/032216/BPC_16-0081.pdf.
[31] http://www.stratersys.com/.

capabilities. Michael De Yoanna, *Colorado Police Cautiously Eager about Body Cameras That Recognize Faces*, Colo. Pub. Radio (July 19, 2015).[32] Police body camera records, like license plate records, will need to be released to the public to provide the necessary oversight of their use.

Similar to the BWCs, police dashboard cameras were implemented as a tool of police oversight after numerous allegations of racial profiling by police conducting traffic stops. *Caught on Camera: The History of the Police Dashcam*, NBC News Digital (Oct. 22, 2015).[33] Like with BWCs, ALPRs, and other tools of surveillance, public record access is essential to ensure proper oversight.

Recent events surrounding public access to police dashcam footage demonstrate how important public record access is for oversight and accountability. In October 2014 Chicago Police Office Jason Van Dyke shot and killed 17-year-old Laquan McDonald. Daily Southtown, *Freelance Write Exposes Police Shooting Cover-up*, Chicago Tribune (Dec. 2, 2015).[34] The Chicago Police claimed that

---

[32] http://www.cpr.org/news/story/colorado-police-cautiously-eager-about-body-cameras-recognize-faces.
[33] http://www.nbcnews.com/feature/long-story-short/video/caught-on-camera-the-history-of-the-police-dashcam-548708419951.
[34] http://www.chicagotribune.com/suburbs/daily-southtown/opinion/ct-sta-reeder-mcdonald-shooting-st-1203-20151202-story.html.

the teenager had lunged at an officer with a knife. *Id.* It was only after freelance reporter, Brandon Smith, filed a request under the Illinois freedom of information law for the video and subsequently sued to get it did the truth come out. *Id.* Laquan McDonald never lunged at police and he was shot 16 times by a single officer while walking away from the police. *Id.* The video was released 13 months after the incident and only when its release became imminent did the officer who shot Mr. McDonald get charged with murder. *Id.*

For BWCs to be an effective tool for police accountability, the public will need access to the record of police conduct. Civil Rights, Privacy, Media Rights, and Open Government groups all agree that public access to BWC footage is essential for police accountability. The Leadership Conference on Civil and Human Rights Press Release, *Civil Rights, Privacy, and Media Rights Groups Release Principles for Law Enforcement Body Worn Cameras* (May 15, 2015);[35] D.C. Open Government Coalition, *Coalition Presents State-by-State Police Body Cam Research.*[36] Where the government has sought to restrict or exempt public access to BWC footage there has been push back. *See, e.g.*, Kelly Swanson, *Advocates Push Back Against FOIA Exemptions for Bodycam Footage*, Reporters Comm.

---

[35] http://www.civilrights.org/press/2015/body-camera-principles.html.
[36] http://www.dcogc.org/printpdf/content/coalition-presents-state-state-police-body-cam-research-0.

for Freedom of the Press (June 9, 2015).[37] Transparency through public access is essential to legitimizing BWCs as a tool of police accountability. *See* Media Freedom & Information Access Clinic, *Police Body Cam Footage: Just Another Public Record* (Dec. 2015).[38]

Indeed, even EPIC, which does not support the adoption of BWCs because of the privacy risks, advocates for public access to the agency records of BWC systems. *Body Cameras: Can Technology Increase Protection for Law Enforcement Officers and the Public: Hearing Before the Subcomm. on Crime and Terrorism of the S. Judiciary Comm.*, 113th Cong., 4-5 (2015) (statement of the Electronic Privacy Information Center).[39]

Attorney General Loretta Lynch has stated, "Body-worn cameras hold tremendous promise for *enhancing transparency*, *promoting accountability*, and advancing public safety for law enforcement officers and the communities they serve." DOJ Press Release, *Justice Department Announces $20 Million in Funding to*

---

[37] http://www.rcfp.org/browse-media-law-resources/news/advocates-push-back-against-foia-exemptions-bodycam-footage.
[38] http://isp.yale.edu/sites/default/files/publications/police_body_camera_footage-_just_another_public_record.pdf.
[39] https://epic.org/privacy/testimony/EPIC-Body-Camera-Statement-05-19-15.pdf.

Support Body-Worn Camera Pilot Program (May 1, 2015) (emphasis added).[40]

A broad interpretation of the investigative record exemption will not only undermine public oversight of ALPR programs, but it will threaten the police accountability promised by BWCs.

C. Freedom of information laws have also enabled oversight of "fusion centers."

Over the past ten years, the Department of Homeland Security has facilitated the "receipt, analysis, gathering, and sharing" of information about individuals through the "fusion center" program. DHS, *National Network of Fusion Centers Fact Sheet* (2016).[41] Given the broad scope of data collected about everyday Americans, these programs require intense public scrutiny and oversight to ensure strong privacy protections. *See* EPIC, *Information Fusion Centers and Privacy* (2016).[42] The Department of Homeland Security has recognized that it cannot simply conduct these programs in secret without public knowledge, and has provided resources to learn about their development. DHS, *Resources for Fusion Centers* (2016).[43] The

---

[40] https://www.justice.gov/opa/pr/justice-department-announces-20-million-funding-support-body-worn-camera-pilot-program.
[41] https://www.dhs.gov/national-network-fusion-centers-fact-sheet.
[42] https://epic.org/privacy/fusion/.
[43] https://www.dhs.gov/resources-fusion-centers.

agency has never suggested that providing information about these programs impacts individual investigations.

But even where the government has provided the public with information about programs, there is still a need for additional accountability through public records requests. Even though the government acknowledged its increasing reliance on fusion centers nationwide—*see* DHS, *2014 National Network of Fusion Centers Final Report* 9 (Jan. 2015);[44] DHS, *Fusion Center Locations and Contact Information* (Apr. 21, 2016)[45]—freedom of information requests are still necessary to ensure that the public understands what data is being collected and prevents abuse.

Prior to the creation of the Department of Homeland Security and the rollout of fusion centers nationwide, the Defense Advanced Research Projects Agency created a program aimed at achieving "total information awareness." DARPA, *Report to Congress Regarding the Terrorism Information Awareness Program* (2003).[46] EPIC was able to obtain documents about the program under the federal Freedom of

---

[44] https://www.dhs.gov/sites/default/files/publications/2014%20National%20Network%20of%20Fusion%20Centers%20Final%20Report_1.pdf.

[45] https://www.dhs.gov/fusion-center-locations-and-contact-information.

[46] https://epic.org/privacy/profiling/tia/may03_report.pdf.

Information Act. EPIC, *"Terrorism" Information Awareness* (2016).[47] Soon after this and other information was uncovered about the program, lawmakers held hearings and reacted to the government's overreach. *Senate Rebuffs Domestic Spy Plan*, Wired (Jan. 23, 2002).[48] Following these developments, former officials acknowledged the need for greater privacy protections to prevent misuse. *See* Steve Lohr, *Data Expert Is Cautious About Misuse of Information*, N.Y. Times (Mar. 25, 2003).[49] These public oversight efforts played a key role in underscoring the need for limits on broad scale data collection—collection that would subsequently be taken on by fusion centers.

Fusion centers, which operate at the local level, combine records from federal and state agencies, and government and private record systems. They are the "local arm" of the intelligence community, the 17 federal agencies administered by the Office of the Director of National Intelligence and coordinated by the National Counterterrorism Center. Nat'l Counterterrorism Ctr., *Overview*;[50] Office of the Dir. of Nat'l Intelligence, *Members of the IC.*[51]

---

[47] https://epic.org/privacy/profiling/tia/#foia.
[48] http://archive.wired.com/politics/law/news/2003/01/57386.
[49] http://www.nytimes.com/2003/03/25/technology/25DATA.html.
[50] https://www.nctc.gov/overview.html (last visited May 1, 2016).
[51] https://www.dni.gov/index.php/intelligence-community/members-of-the-ic (last visited May 1, 2016).

The term "fusion center"—first coined by the Department of Defense—refers to the "fusing" of information from public and private sources for analysis. See EPIC, *Information Fusion Centers and Privacy* (2016). Today there are two types of fusion centers: (1) primary fusion centers, which provide "information sharing and analysis for an entire state," and (2) recognized fusion centers, which provide "information sharing and analysis for a major urban area." DHS, *Fusion Center Locations and Contact Information*, *supra*.[52] Primary fusion centers receive "the highest priority for the allocation of federal resources to centers" because they are "the focus points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information," in addition to having "responsibilities related to the coordination of critical operational capabilities across the statewide fusion process with recognized fusion centers and nodes." Info. Sharing Env't, *Information Sharing Environment Guidance: Federal Resource Allocation Criteria (RAC)*, ISE-G-112, at 3 (June 3, 2011).[53]

California has six fusion centers: one primary (California State Threat Assessment Center) and five recognized (Central California Intelligence Center; Sacramento, CA; Los Angeles Joint Regional

---

[52] https://www.dhs.gov/fusion-center-locations-and-contact-information.

[53] http://www.ise.gov/sites/default/files/RAC_final.pdf.

Intelligence Center; Los Angeles, CA; Northern California Regional Intelligence Center; San Francisco, CA; Orange County Intelligence Assessment Center; Orange County, CA; San Diego Law Enforcement Coordination Center; San Diego, CA). DHS, *Fusion Center Locations and Contact Information*, *supra*.

Serious problems with fusion centers remain, underscoring the ongoing need for public oversight. *E.g.*, Permanent Subcomm. on Investigations, Investigative Report Criticizes Counterterrorism Reporting, *Waste at State & Local Intelligence Fusion Centers* (Oct. 3, 2012)[54] (finding that DHS intelligence officers at state and local fusion centers "produced intelligence of uneven quality—oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism." (internal quotation marks omitted)).

Fusion centers have also spearheaded the Nationwide Suspicious Activity Reporting Initiative ("NSI"), which poses serious threats to fundamental civil liberties. EPIC, *Suspicious Activity Reporting* (2016)[55]; *see* Nationwide SAR Initiative, *Nationwide SAR*

---

[54] https://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.

[55] https://epic.org/privacy/suspicious-activity-reporting/.

Initiative (2016).[56] The NSI is a "joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, and territorial law enforcement partners" to identify and report suspicious activity across the country, as well as to centrally share suspicious activity reporting ("SAR") information. *Nationwide SAR Initiative*, *supra*.

For the purposes of the NSI, "suspicious activity" is "[o]bserved behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." Info. Sharing Env't, *Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5.5*, ISE-FS-200, at 4 (Feb. 23, 2015)[57] [hereinafter *FS SAR*]. Individuals, state, and federal officials can all report suspicious activity. *Id.* at 4, 58. Federal guidance mandates that a state, federal, local, tribal, or territorial official investigate all suspicious activity observations to determine whether the activity is innocent or worthy of escalation to a SAR. *Id.* at 53. Investigative techniques include personal observations, interviews with the subject, or accessing a number of information databases. *Id.*

Once a SAR has been created, the information undergoes additional analysis before becoming an Information Sharing

---

[56] https://nsi.ncirc.gov/?AspxAutoDetectCookieSupport=1.
[57] https://www.ise.gov/sites/default/files/SAR_FS_1.5.5_IssuedFeb2015.pdf.

Environment SAR ("ISE-SAR"): a SAR "that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism)." *FS SAR*, *supra*, at 3. Yet federal agency guidance suggests that lawful or constitutionally protected behavior—such as "[l]earning how to operate, or operating an aircraft," "[q]uestioning individuals or otherwise soliciting information at a level beyond mere curiosity," "[t]aking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner," or "[a]ttempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities"—can justify creation of an ISE-SAR. *Id.* at 41–50. Once information becomes an ISE-SAR, it can be shared with the FBI, homeland security personnel, and state and local law enforcement agencies.

Following the rollout of NSI suspicious activity reporting systems, there has been a strong opposition in California and across the country based on the "lack of a reasonable suspicion threshold" and the fact that innocent activities such as "taking photos of public buildings, using binoculars and taking notes about building measurements" could provide the basis for a report. Kelly Goff, *Los*

Angeles Panel to Gauge Concern Over LAPD Surveillance Programs, L.A. Daily News (Mar. 5, 2014).[58] Public outcry over the use of these reports has also led the LAPD to prohibit reports "taken on the basis of race, creed or religion," and continued public pressure has led to oversight hearings by the city's Human Relations Commission. *Id.* Public records requests are necessary to ensure that agencies continue to follow these new rules.

II. Transparency is necessary to ensure accountability for indiscriminate public surveillance.

It is critically important that open government laws enable public access to information about law enforcement surveillance programs. "[T]he essential problem raised by secret bulk collection of telephone metadata records [was] the fact that the public was denied any opportunity to grant—or withhold—its consent to this practice." Steven Aftergood, *Privacy and the Imperative of Open Government, in Privacy in the Modern Age: The Search for Solutions* 19, 20 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015). First, these programs are surreptitious by nature; individuals have no other way of learning how much data is collected or how it is used. Second, the use of indiscriminate surveillance without public oversight will have a chilling effect on lawful activities. And third, such broad-scale

---

[58] http://www.dailynews.com/government-and-politics/20140305/los-angeles-panel-to-gauge-concern-over-lapd-surveillance-programs.

surveillance systems present opportunities for abuse. "Transparency is a prerequisite of accountability, and where it is not mission-critical, the cloak of secrecy that covers entire electronic surveillance programs by national intelligence should be lifted." Kristina Irion, *Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection, in Privacy in the Modern Age* 78, 83–84.

A. Indiscriminate surveillance programs pose a unique threat to privacy.

Unlike traditional and targeted investigatory techniques, indiscriminate surveillance systems pose unique threats to privacy that require a greater degree of transparency and oversight. "[T]hese new technologies raise concerns about the privacy of those who are—rightly or wrongly—the targets of the new technologies." Comm. on Privacy in the Info. Age, Nat'l Research Council, *Engaging Privacy and Information Technology in the Digital Age* 254 (James Waldo et al. eds. 2007). This is especially true as government agencies seek to compile large data sets to be analyzed in a way that can reveal much more about individuals' traits and behaviors that initially expected. *See* Exec. Office of the Pres., *Big Data and Privacy: A Technological Perspective* ix (May 2014)[59] (noting that "big data" is big "in the

[59] https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

quantity and variety of data that are available to be processed," and also big "in the scale of analytics . . . that can be applied to those data, ultimately to make inferences and draw conclusions").

For example, a recent study showed that telephone call data, when collected indiscriminately and subject to close analysis, revealed "unambiguously sensitive, even in a small population and over a short time window," Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, Web Policy (Mar. 12, 2014).[60] This discovery contradicted numerous statements by government officials dismissing privacy concerns about the Section 215 telephone metadata surveillance program. Remarks on Health Insurance Reform and an Exchange With Reporters in San Jose, California, 2013 Daily Comp. Pres. Doc. 397, at 4–5 (June 7, 2013)[61] (stating that the Section 215 telephone metadata surveillance program is not looking at content); Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program*, Wash. Post (June 6,

---

[60] http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

[61] https://www.gpo.gov/fdsys/pkg/DCPD-201300397/pdf/DCPD-201300397.pdf.

2013)[62] ("As you know, this is just metadata. There is no content involved.").

Instead, Mayer found that just matching called phone numbers to public phone directors on Yelp and Google Places allowed for a number of sensitive inferences. Mayer & Mutchler, *supra.* Participants called "Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more," allowing for direct inferences of purpose. *Id.* Calls to specialty medical practice areas allow an inference that the caller is seeking specialty medical care (e.g., sexual and reproductive health; cardiology; neurology). *Id.* In addition, a pattern of calls can be even more revealing. *Id.* For example, one participant "spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmia"—and later corroborated the participant's medical condition. *Id.* Another participant "had a long, early morning call with her sister. Two days later, she placed a series of calls to the local

[62] https://www.washingtonpost.com/news/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/.

Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after." *Id.*

Research has also shown that large data sets collected for other purposes can reveal sensitive—and unexpected—facts about individuals. A 2016 report revealed that insurance claims, credit histories, and voter histories can predict precise individual health needs, such as who is at risk for diabetes or a heart attack, who is considering costly medical procedures, and who is pregnant. Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, Wall St. J. (Feb. 17, 2016).[63] Retailer Target discovered that women who purchased larger quantities of unscented lotion, cotton balls, and vitamin supplements were likely pregnant, and could predict their due date to the month. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2012).[64] FICO, a credit score generation company, discovered that publicly available data such as home ownership and job status can "predict which patients are at highest risk for skipping or incorrectly using prescription medications." Tara Parker-Pope, *Keeping Score on How You Take Your Medicine*, N.Y.

---

[63] http://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940#:Tt2bneJzyT0qGA.
[64] http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#5c4246cd34c6.

Times (June 20, 2011).[65] And researchers recently discovered that analysis of Twitter user posts can clearly signal prescription medication abuse. Abeed Sarker et al., *Social Media Mining for Toxicovigilance: Automatic Monitoring of Prescription Medication Abuse from Twitter*, 39 Drug Safety 231, 231 (2016).[66]

Large sets of data, even innocuous data, can now be analyzed to reveal sensitive information about individuals. Consequently, the privacy risks are heightened and thus indiscriminate surveillance programs, like the ALPR program, require greater transparency and oversight of the data collected.

B. Public access to state records is necessary to assess the impact of programs of indiscriminate surveillance.

Public disclosure of ALPR data is necessary to understand the scope and impact of the massive data collection program. Information collected from the general public to identify stolen cars might eventually be used to build profiles of individuals based on travel patterns, the places they visit, and the people they know. But the public and lawmakers cannot meaningfully limit the government's use of that data if they are not aware of the scope of the program, the data

---

[65] http://well.blogs.nytimes.com/2011/06/20/keeping-score-on-how-you-take-your-medicine/.

[66] http://link.springer.com/article/10.1007/s40264-015-0379-4.

that is collected, or how it is used. That is the reason for open records laws, such as the California Public Records Act.

Public disclosure has played a key role in facilitating oversight of government surveillance programs. A FOIA lawsuit pursued by EPIC about the DHS monitoring of social network and media organizations produced 285 pages of documents. *EPIC v. DHS*, 999 F. Supp. 2d 6, 75 (D.D.C. 2013). These documents revealed that DHS was monitoring for media reports and social media that reflected negatively against the agency. EPIC, *EPIC v. Department of Homeland Security: Media Monitoring* (2016).[67] The documents led to a Congressional hearing on DHS's social media monitoring program. *See DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H. Comm. on Homeland Security*, 112th Cong. (2012).

The purpose of freedom of information laws is to promote government transparency. The federal Freedom of Information Act, 5 U.S.C. § 552, is "the law that keeps citizens in the know about their government." DOJ, *What is FOIA?*[68] The California Public Records Act "declares that access to information concerning the conduct of the

---

[67] http://epic.org/foia/epic-v-dhs-media-monitoring/.
[68] http://www.foia.gov/about.html (last visited May 2, 2016).

people's business is a fundamental and necessary right of every person in this state." Cal. Gov't Code § 6250 (West 2016). And thanks to the overwhelming approval of Proposition 59 by California voters in 2004, the California Constitution enshrines the people's "right of access to information concerning the conduct of the people's business." Cal. Const. art. I, § 3(b)(1).

CONCLUSION

Amicus Curiae EPIC respectfully requests that this Court rule in favor of the Petitioners and reverse the decision of the lower court.

Dated: May 5, 2016

Respectfully submitted,

/s/ Alan Butler

MARC ROTENBERG
ALAN BUTLER
JERAMIE SCOTT
AIMEE THOMSON
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave. N.W.,
Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
Counsel for Amicus Curiae

CERTIFICATION OF WORD COUNT

I certify pursuant to California Rule of Court 8.520 that this Application For Leave To File Amicus Curiae Brief And Amicus Curiae Brief Of Electronic Privacy Information Center (EPIC) In Support Of Petitioners is proportionally spaced, has a typeface of 13 points or more, contains 4,867 words, excluding the cover, the tables, the signature block, the 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-procession program used to prepare this brief.

Dated: May 5, 2016

ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I, Alan Butler, do hereby affirm that I am a citizen of the United States and employed in the City of Washington, District of Columbia. I am over the age of 18 years and not a party to the within action. My business address is 1718 Connecticut Ave., N.W., Suite 200, Washington, D.C. 20009.

On May 5, 2016, I served the following document: **Application For Leave To File Amicus Curiae Brief And Amicus Curiae Brief of Electronic Privacy Information Center (EPIC) In Support Of Petitioners** upon each of the parties by placing a true and correct copy of the document, enclosed in a sealed envelope, on the persons below as follows:

Peter Bibring
ACLU Foundation of Southern California
1313 West Eighth Street
Los Angeles, CA
Counsel for Petitioner American Civil Liberties Union Foundation of Southern California

Jennifer Ann Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA
Counsel for Petitioner Electronic Frontier Foundation

James Christopher Jardin
Collins Collins Muir & Stewart, LLP
1100 El Centro Street
South Pasadena, CA
Counsel for Real Party in Interest County of Los Angeles and Los Angeles County Sheriff's Department

Lisa S. Berger
Los Angeles City Attorney's Office
600 City Hall East
200 North Main Street
Los Angeles, CA
Counsel for Real Party in Interest City of Los Angeles and Los Angeles Police Department

Clerk of the Court of Appeal of California
Second Appellate District
Division Three
Ronald Reagan State Building
300 S. Spring Street
2nd Floor, North Tower
Los Angeles, CA 90013

Clerk of the Los Angeles County Superior Court
111 North Hill St.
Los Angeles, CA 90012

I deposited the sealed envelopes with the United States Postal Service, with postage thereon fully prepaid. The envelopes were placed in the mail in Washington, D.C.

I declare under 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 5, 2016.

_____
ALAN BUTLER