

JENNIFER PINSOFF (SBN 350418)
ELIZABETH FEMIA (SBN 356193)
ANDREW CROCKER (SBN 291596)
ADAM SCHWARTZ (SBN 309491)
SAIRA HUSSAIN (SBN 300326)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: jpinsoff@eff.org

CHESSIE THACHER (SBN 296767)
NICOLAS HIDALGO (SBN 339177)
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 621-2493
Email: nhidalgo@aclunc.org

Attorneys for Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SANTA CLARA

SERVICES, IMMIGRANT RIGHTS &
EDUCATION NETWORK; COUNCIL ON
AMERICAN-ISLAMIC RELATIONS,
CALIFORNIA,

Plaintiffs,

v.

CITY OF SAN JOSE; PAUL JOSEPH, in his
official capacity as Chief of Police of the City of
San Jose Police Department; and MATT
MAHAN, in his official capacity as Mayor of the
City of San Jose,

Defendants.

**Electronically Filed
by Superior Court of CA,
County of Santa Clara,
on 7/24/2026 12:19 PM
Reviewed By: R. Fleming
Env. #24567708**

Case #25CV480254

Case No.: 25CV480254

**PLAINTIFFS' OPPOSITION TO
DEMURRER**

Date: August 6, 2026
Time: 9:00 a.m.
Dept.: 10
Judge: Hon. Jeffrey El-Hajj

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

TABLE OF CONTENTS.....2

TABLE OF AUTHORITIES3

INTRODUCTION6

STATEMENT OF FACTS7

 I. Defendants Operate a Vast ALPR System That Effortlessly Collects and Stores Precise
 Location Information About Millions of Innocent Drivers.7

 II. SJPD Conducts Warrantless Searches of ALPR Data Thousands of Times a Month.....7

 III. Plaintiffs Pay City Taxes, and Defendants Spend Public Funds on the ALPR System.8

LEGAL STANDARD.....8

ARGUMENT9

 I. SJPD’s Retrospective Searches of ALPR Information Violate Article I, Section 13 of the
 California Constitution.9

 A. Article I, Section 13 of the California Constitution Is More Protective of Privacy Than
 the Fourth Amendment of the U.S. Constitution.9

 B. People Have a Reasonable Expectation of Privacy in Their Movements Over Time,
 Including in Public.....10

 C. Defendants Violate the Reasonable Expectation of Privacy in Movements Over Time by
 Allowing Warrantless Searches of SJPD’s ALPR database.13

 1. Detailed13

 2. Effortless15

 3. Indiscriminate.....16

 4. Retrospective17

 II. SJPD’s Retrospective Searches of ALPR Information Violate Article I, Section 1 of the
 California Constitution.17

 A. Defendants Violate Legally Protected Privacy Interests..18

 B. Defendants Violate Reasonable Expectations of Privacy.....19

 C. Defendants’ Conduct Is a Serious Privacy Invasion.....19

 III. SJPD’s Retrospective Searches of ALPR Information Violate CCP Section 526a.....20

CONCLUSION.....20

PROOF OF SERVICE.....22

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Am. Academy of Pediatrics v. Lungren</i> , (1997) 16 Cal.4th 307	9, 18
<i>Burrows v. Superior Court</i> , (1974) 13 Cal.3d 238	10
<i>C.A. v. Hart Union High Sch. Dist.</i> , (2012) 53 Cal.4th 861	9
<i>California DUI Lawyers Ass’n v. California DMV</i> , (2018) 20 Cal.App.5th 1247	20
<i>California v. Ciraolo</i> , (1986) 476 U.S. 207	10
<i>California v. Greenwood</i> , (1988) 486 U.S. 35	10
<i>Carpenter v. United States</i> , (2018) 585 U.S. 310	<i>passim</i>
<i>Chatrue v. United States</i> , (2026) 609 U.S. ---, 2026 WL 1855568	<i>passim</i>
<i>Fremont Indemn. Co. v. Fremont Gen. Corp.</i> , (2007) 148 Cal.App.4th 97	8
<i>Hill v. NCAA</i> , (1994) 7 Cal.4th 1	18, 19
<i>In re Carmen M.</i> , (2006) 141 Cal.App.4th 478	18
<i>Katz v. United States</i> , (1967) 389 U.S. 347	9, 11, 12
<i>Kyllo v. United States</i> , (2001) 533 U.S. 27	11, 15
<i>Leaders of a Beautiful Struggle v. Baltimore Police Dept.</i> , (4th Cir. 2021) 2 F.4th 330	<i>passim</i>
<i>Loder v. City of Glendale</i> , (1997) 14 Cal.4th 846	18
<i>People v. Blair</i> , (1979) 25 Cal.3d 640	10

1	<i>People v. Buza,</i>	
2	(2018) 4 Cal.5th 658	9
3	<i>People v. Camacho,</i>	
4	(2000) 23 Cal.4th 824	9
5	<i>People v. Cartwright,</i>	
6	(2024) 99 Cal.App.5th 98	12
7	<i>People v. Krivda,</i>	
8	(1971) 5 Cal.3d 357, affd. (1973) 8 Cal.3d 623.....	10
9	<i>People v. Laiwa,</i>	
10	(1983) 34 Cal.3d 711	17
11	<i>People v. Lovelace,</i>	
12	(1981) 116 Cal.App.3d 541	12
13	<i>People v. Mayoff,</i>	
14	(1986) 42 Cal.3d 1302	9, 10
15	<i>People v. Sheridan,</i>	
16	(1965) 236 Cal.App.2d 667	12
17	<i>People v. Superior Court,</i>	
18	(2006) 143 Cal.App.4th 1183	17
19	<i>Perez v. Golden Empire Transit Dist.,</i>	
20	(2012) 209 Cal.App.4th 1228	9
21	<i>Sheehan v. San Francisco 49ers, Ltd.,</i>	
22	(2009) 45 Cal.4th 992	8
23	<i>Smith v. Maryland,</i>	
24	(1979) 442 U.S. 735.....	10
25	<i>United States v. Carpenter,</i>	
26	(6th Cir. 2016) 819 F.3d 880	14
27	<i>United States v. Jones,</i>	
28	(2012) 565 U.S. 400.....	<i>passim</i>
	<i>United States v. Karo,</i>	
	(1984) 468 U.S. 705.....	11
	<i>United States v. Knotts,</i>	
	(1983) 460 U.S. 276.....	12, 16
	<i>United States v. Miller,</i>	
	(1976) 425 U.S. 435.....	10

1	<i>United States v. Yang,</i>	
2	(9th Cir. 2020) 958 F.3d 851	15
3	<i>Van Atta v. Scott,</i>	
4	(1980) 27 Cal.3d 424	20
5	<i>White v. Davis,</i>	
6	(1975) 13 Cal.3d 757	18
7	Statutes	Page(s)
8	Cal. Const., art. I, § 1	6, 17, 18
9	Cal. Const., art. I, § 13	6, 9, 10
10	Code Civ. Proc., § 526a	20
11	Other Authorities	Page(s)
12	Ballot Pamp., Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11	18, 20
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

INTRODUCTION

California’s Constitution doubly protects against dragnet police surveillance: Article I, § 13 prohibits unreasonable searches and seizures, and Article I, § 1 guarantees privacy. These state constitutional protections are even stronger than the Fourth Amendment.

Plaintiffs seek to enforce these protections against the City of San Jose’s (“City”) policy of allowing police officers, without a warrant, to search the City’s massive database of the physical movements of anyone driving in San Jose. The City created this database by blanketing its roads with nearly 500 automated license plate readers (“ALPRs”) that indiscriminately capture and record the precise time and location a car passes. Every year, this dragnet records hundreds of millions of people’s movements, and officers query this data tens of thousands of times. This exposes when people are driving home or to a hospital, a legal clinic, or a protest.

Each police query of this database is a “search” that triggers the California Constitution’s warrant requirement. People have a reasonable expectation of privacy in the sum of their movements over time, so surveillance that reveals these movements is a search. (*Chatrue v. United States* (2026) 609 U.S. ---, 2026 WL 1855568; *Carpenter v. United States* (2018) 585 U.S. 310; *United States v. Jones* (2012) 565 U.S. 400.) The City’s vast ALPR database is such surveillance. It is pervasive in space, collecting precise information about a car’s exact whereabouts at hundreds of locations. It is pervasive in time, collecting data 24/7/365. It is automated, effortless, and inexpensive. It is indiscriminate, though only a tiny fraction of passing cars are of any previous interest to the police. It reveals previously unknowable intimate details of the lives of these drivers. It is unavoidable to the vast majority of City residents who must drive.

Plaintiffs do not challenge the City’s collection or storage of this data. Rather, they challenge only the City’s policy of allowing warrantless police searches of this data. The allegations in Plaintiffs’ Complaint clearly state a cause of action under California’s twin constitutional bans on dragnet police surveillance. Thus, Defendants’ demurrer must be denied.

STATEMENT OF FACTS

I. Defendants Operate a Vast ALPR System That Effortlessly Collects and Stores Precise Location Information About Millions of Innocent Drivers.

The San Jose Police Department (“SJPД”) operates a sprawling network of at least 474 high-tech ALPR cameras throughout San Jose, three times as many as were operational in 2023. (Plaintiffs’ Complaint (“Compl.”) ¶ 24.) SJPД has deployed them in residential areas and near highly sensitive locations, such as places of worship, immigration centers, and clinics. (Compl. ¶¶ 52, 55.) SJPД’s ALPR system consists of these cameras, software that converts images into data, and a cloud-based, searchable database (together, the “ALPR System”). (Compl. ¶ 15.)

The ALPR cameras automatically capture images of every passing vehicle, without suspicion that any given driver has violated the law. (Compl. ¶ 16.) They operate nonstop. (Compl. ¶ 18.) Once an image is captured, software extracts vehicle data, including the license plate number. (Compl. ¶ 16.) This data, and the precise date, time, and Global Positioning System (“GPS”) coordinates, are stored in the central ALPR database. (*Ibid.*) The images often capture people visible within the vehicle, bumper stickers, and vehicle features. (Compl. ¶ 17.) SJPД’s vendor, Flock Safety (“Flock”), extracts and stores such vehicle details. (Compl. ¶¶ 17, 35.)

A person who regularly drives through San Jose can have their location captured multiple times a day, providing an intimate window into their life. (Compl. ¶ 46.) A single ALPR camera can capture the locations of thousands of vehicles in minutes, and in 2024 alone, SJPД collected over 361 million scans. (Compl. ¶¶ 18, 26.) SJPД’s ALPR System also uses artificial intelligence (“AI”) to associate drivers, track vehicles frequently seen together, detect patterns, and purportedly predict “suspicious” movements. (Compl. ¶ 36.)

II. SJPД Conducts Warrantless Searches of ALPR Data Thousands of Times a Month.

SJPД stores all this ALPR information in a searchable database that officers use for retrospective investigations. (Compl. ¶ 20.) When the Complaint was filed, SJPД retained ALPR information in this database for a full year, (Compl. ¶ 31), though it may have since reduced this to 30 days. Whether measured in a year or a month, the ALPR System lets police search extensive and revealing information about drivers’ exact whereabouts at precise times. (Compl. ¶ 38.)

1 SJPd officers, and law enforcement officials across California, routinely search SJPd’s
2 ALPR database. (Compl. ¶ 38.)¹ Officers can search for a full or partial license plate number, all
3 vehicles at a particular location at specific times, all vehicles that have been to multiple specified
4 locations, or all vehicles with certain features, including make, model, color, bumper stickers, or
5 vehicle alterations. (Compl. ¶¶ 21, 35.)

6 SJPd does not require officers to seek a warrant or other judicial authorization before
7 conducting these searches. (Compl. ¶¶ 42, 45.) As a result, officers search SJPd’s ALPR database a
8 staggering number of times. For example, published audits show that, between June 5, 2024 and
9 June 17, 2025, SJPd officers logged 261,711 searches, averaging about 692 searches a day.
10 (Compl. ¶ 41.) Counting searches of the database by other California law enforcement agencies, this
11 balloons to 3.9 million in this period. (Compl. ¶ 42.)

12 **III. Plaintiffs Pay City Taxes, and Defendants Spend Public Funds on the ALPR System.**

13 Plaintiffs Services, Immigrant Rights & Education Network (“SIREN”) and Council on
14 American-Islamic Relations, California (“CAIR-CA”) are nonprofits serving, respectively, the
15 immigrant community and American Muslim community in San Jose and the broader region.
16 (Compl. ¶¶ 8–9.) Each has paid taxes that fund San Jose within the last year, including sales taxes.
17 (*Ibid.*) Defendants expend taxpayer funds, personnel time, and other resources to purchase and
18 operate the ALPR System. (Compl. ¶ 57.) Without an order from this Court, Defendants will
19 continue to do so. (Compl. ¶ 58.)

20 **LEGAL STANDARD**

21 The only issue a court may resolve on demurrer is whether the complaint, standing alone,
22 states a cause of action under any possible legal theory. (*Sheehan v. San Francisco 49ers, Ltd.*
23 (2009) 45 Cal.4th 992, 998.) The Court must accept factual allegations as true, including any “facts
24 that reasonably can be inferred.” (*Fremont Indemn. Co. v. Fremont Gen. Corp.* (2007) 148
25 Cal.App.4th 97, 111.) The complaint “need only allege facts sufficient to state a cause of action,”

26
27 ¹ Flock allows agencies to automatically share their ALPR data with other agencies. (Compl. ¶ 34.)
28 This creates a vast, interconnected network that tracks drivers across the country. (*Ibid.*) SJPd grants
other California law enforcement agencies direct and continuous access. (Compl. ¶ 42.)

1 and need not provide every “evidentiary fact that might eventually form part of the plaintiff’s proof
2” (*C.A. v. Hart Union High Sch. Dist.* (2012) 53 Cal.4th 861, 872.) When allegations are
3 subject to different reasonable interpretations, the Court must draw inferences that are favorable to
4 the plaintiff. (*Perez v. Golden Empire Transit Dist.* (2012) 209 Cal.App.4th 1228, 1238.)

5 **ARGUMENT**

6 **I. SJPD’s Retrospective Searches of ALPR Information Violate Article I, Section 13 of 7 the California Constitution.**

8 Article I, § 13 of the California Constitution protects individuals against unreasonable
9 searches and seizures. A search occurs when the government infringes a person’s reasonable
10 expectation of privacy. (*People v. Camacho* (2000) 23 Cal.4th 824, 830; see also *Katz v. United*
11 *States* (1967) 389 U.S. 347, 360 (Harlan, J., concurring) [“electronic . . . intrusion” on a “reasonable
12 expectation of privacy” can violate the Fourth Amendment].)

13 Drivers in San Jose have a reasonable expectation of privacy in the precise location
14 information collected and stored by SJPD’s ALPR System. Defendants violate that expectation by
15 allowing SJPD and other California officers to search this ALPR information without a warrant.
16 Because a search is presumptively unreasonable if it is done without a warrant, the challenged
17 dragnet surveillance program violates Plaintiffs’ rights under Article I, § 13.

18 **A. Article I, Section 13 of the California Constitution Is More Protective of Privacy 19 Than the Fourth Amendment of the U.S. Constitution.**

20 Although Article I, § 13 and the Fourth Amendment “ordinarily” are construed “in tandem,”
21 California courts will rule “solely” under the former where, as here, the U.S. Supreme Court has not
22 yet reached the issue. (*People v. Buza* (2018) 4 Cal.5th 658, 686.) The California Constitution is “a
23 document of independent force” (*Am. Academy of Pediatrics v. Lungren* (1997) 16 Cal.4th
24 307, 325, citation omitted.) While California courts give “respectful consideration” to constitutional
25 interpretations of the U.S. Supreme Court, they need only follow them “where they provide no less
26 individual protection than is guaranteed by California law.” (*People v. Mayoff* (1986) 42 Cal.3d
27 1302, 1312, citation omitted.)

28 In the context of technology-based surveillance, the California Supreme Court has held that
people have a reasonable expectation of privacy against police aerial surveillance of their

1 backyards, whereas the U.S. Supreme Court held the opposite. (Compare *Mayoff*, 42 Cal.3d at
2 1312, with *California v. Ciraolo* (1986) 476 U.S. 207, 214.) California cases addressing other forms
3 of police searches also demonstrate Article I, § 13’s broader privacy protections. (Compare *People*
4 *v. Krivda* (1971) 5 Cal.3d 357, 367 [finding a reasonable expectation of privacy against police
5 scrutiny of garbage] *affd.*, *People v. Krivda* (1973) 8 Cal.3d 623, with *California v. Greenwood*
6 (1988) 486 U.S. 35, 40 [holding the opposite]; Compare *Burrows v. Superior Court* (1974) 13
7 Cal.3d 238; *People v. Blair* (1979) 25 Cal.3d 640, 652, 654–655) [requiring court order for bank
8 and phone records], with *United States v. Miller* (1976) 425 U.S. 435; *Smith v. Maryland* (1979)
9 442 U.S. 735, 749 [no expectation of privacy in these records due to “third-party” doctrine].)

10 **B. People Have a Reasonable Expectation of Privacy in Their Movements Over**
11 **Time, Including in Public.**

12 Drivers in San Jose have a reasonable expectation of privacy in their movements throughout
13 the City, including as captured by SJPD’s ALPR System.

14 In *Carpenter v. United States*, the U.S. Supreme Court held that individuals have a
15 reasonable expectation of privacy in the sum of their physical movements over time, and
16 surveillance that reveals these movements can be so intrusive as to constitute a Fourth Amendment-
17 violative search. (585 U.S. at 310 [reaffd. by *Chatrre*, 2026 WL 1855568].) The Court reasoned that
18 technology that “attempts to reconstruct a person’s movements” presents a particularly acute risk of
19 “erod[ing] Fourth Amendment protections” given its capacity to reveal the “privacies of life.” (*Id.*
20 at 310–311, 320.) Five Justices reached a similar conclusion in *United States v. Jones*. (565 U.S. at
21 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment).) Justice Alito
22 explained, “[i]n the precomputer age, the greatest protections of privacy were neither constitutional
23 nor statutory, but practical.” (*Id.* at 429.) But today, “technology has enhanced the Government’s
24 capacity to encroach upon areas normally guarded from inquisitive eyes” (*Carpenter*, 585 U.S.
25 at 305.) Technologically aided surveillance “provides an intimate window into a person’s life,
26 revealing not only his particular movements, but through them his ‘familial, political, professional,
27 religious, and sexual associations.’” (*Id.* at 311 [quoting *Jones*, 565 U.S. at 415 (Sotomayor, J.,
28 concurring)].) Accordingly, technology’s use to collect “otherwise unknowable” information

1 triggers constitutional protections. (*Id.* at 312; see also *Leaders of a Beautiful Struggle v. Baltimore*
2 *Police Dept.* (4th Cir. 2021) 2 F.4th 330, 341 (en banc); *Chatrue*, 2026 WL 1855568 at *10 [“A new
3 technology should not transform what individuals had reasonably thought they could withhold from
4 the Government.”].)²

5 Though *Carpenter* specifically addressed cell site location information (“CSLI”), its
6 reasoning applies in full force to other technology that “attempts to reconstruct a person’s
7 movements,” like ALPRs. (585 U.S. at 310, 312 [Fourth Amendment search occurred when the
8 government tracked an individual’s movements by accessing days of CSLI held by a cell service
9 provider].) The pattern of where a person travels—including when, how often, and in what
10 sequence—exposes the most intimate details of life: where they live, work, worship, seek medical
11 care, and spend their nights. For this reason, the federal Court of Appeals for the Fourth Circuit held
12 that Baltimore police violated the Fourth Amendment by operating an aerial surveillance program
13 (“AIR”) that captured wide-area, low-resolution photographs allowing indiscriminate tracking of
14 people’s movements throughout the city. (*Leaders of a Beautiful Struggle*, 2 F.4th at 333.) The
15 court explained: “*Carpenter* solidified the line between short-term tracking of public movements—
16 akin to what law enforcement could do prior to the digital age—and prolonged tracking that can
17 reveal intimate details through habits and patterns.”³ (*Id.* at 341 [cleaned up].)

18 People indisputably retain this reasonable expectation of privacy in their movements in
19

20
21 ² The U.S. Supreme Court has a longstanding approach of looking to historical expectations of
22 privacy to determine current Fourth Amendment safeguards. (See *United States v. Karo* (1984)
23 468 U.S. 705, 715) [using beeper to monitor object’s location inside a traditionally protected space
24 was a search, because police could not obtain this information by manual observation alone]; *Kyllo*
25 *v. United States* (2001) 533 U.S. 27, 36–37, 40 [using thermal imaging device was a search, because
26 police could not otherwise obtain equivalent information without physically entering the home];
27 *Katz*, 389 U.S. at 352 [electronic eavesdropping in closed phonebooth was a search, because police
28 could not have otherwise overheard the call].)

25 ³ The court squarely held that the AIR program was a search even though it did not continuously
26 collect location information. (*Id.* at 342 [“We do not suggest that the AIR program allows perfect
27 tracking of all individuals it captures across all the time it covers. Though data is collected in 12-
28 hour increments, the tracks are often shorter snippets of several hours or less. Still, the program
enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive
days, with a month and a half of daytimes for analysts to work with. That is enough to yield a wealth
of detail, greater than the sum of the individual trips.”] [cleaned up].)

1 public. The U.S. Supreme Court has held that a person “does not surrender all Fourth Amendment
2 protection by venturing into the public sphere.” (*Carpenter*, 585 U.S. at 310.) To the contrary,
3 because the Fourth Amendment “protects people, not places,” its protections apply “even in an area
4 accessible to the public.” (*Ibid.*; *Katz*, 389 U.S. at 351–352.)

5 Thus, Defendants err by denying that drivers on public roads have a reasonable expectation
6 of privacy. (Memorandum of Points and Authorities in Support of Defendants’ Demurrer to
7 Complaint (“Demurrer”) at 4, 7.) The U.S. Supreme Court in *Carpenter*, and a majority of Justices
8 in *Jones*, expressly found privacy interests in public movements, as did the Fourth Circuit in
9 *Leaders of a Beautiful Struggle*. (585 U.S. at 310; 565 U.S. at 415, 430; 2 F.4th at 340.) The privacy
10 interest does not turn on whether any single movement is in public or observable to a passerby;
11 rather, it turns on what the aggregation of movements, recorded and retained over time, can reveal
12 about the person making them. (*Carpenter*, 585 U.S. at 311.) Likewise, Defendants are not assisted
13 by *United States v. Knotts* (1983) 460 U.S. 276. (Cf. Demurrer at 3.) *Knotts* “was careful to
14 distinguish between the rudimentary tracking facilitated by [a] beeper and more sweeping modes of
15 surveillance.” (*Carpenter*, 585 U.S. at 306.) The beeper in *Knotts* was used only during a “discrete
16 automotive journey,” and the Court there expressly reserved whether “different constitutional
17 principles may be applicable” if “twenty-four hour surveillance of any citizen of this country [were]
18 possible.” (*Id.* at 306–307 [quoting *Knotts*, 460 U.S. at 284–285].) Further, the references in *Knotts*
19 to information “voluntarily conveyed,” (460 U.S. at 281), and in *Katz* to information “knowingly
20 expose[d],” (389 U.S. at 351), must be read through the lens of *Carpenter* and *Jones*, and the
21 permeating, round-the-clock digital surveillance that has become a reality in San Jose and other
22 cities across America. (Cf. Demurrer at 7.)

23 Finally, SJPD’s ALPR System is far more privacy invasive than the surveillance in three
24 inapposite cases Defendants cite. (Demurrer at 7–8.) *People v. Cartwright* concerned a small
25 number of conventional security cameras which could “only capture ‘short term’ movements” and
26 could not “create ‘a retrospective database of everyone’s movements across the city.’” ((2024) 99
27 Cal.App.5th 98, 104–05, citation omitted.) *People v. Sheridan* and *People v. Lovelace* concerned
28 direct observations of individual people unassisted by technology. ((1965) 236 Cal.App.2d 667,

1 669; (1981) 116 Cal.App.3d 541, 548.) SJPd’s ALPR System is categorically different. Its nearly
2 500 cameras blanket the city’s roadways, automatically capturing and storing the time, location, and
3 identifying details of every passing vehicle. It is designed to create a retrospective database that
4 reveals where individuals come and go over extended periods.

5 **C. Defendants Violate the Reasonable Expectation of Privacy in Movements Over**
6 **Time by Allowing Warrantless Searches of SJPd’s ALPR database.**

7 SJPd’s ALPR System infringes on individuals’ reasonable expectations of privacy in their
8 movements for the same reason as the tracking of cell phones in *Carpenter* and the aerial
9 surveillance in *Leaders of a Beautiful Struggle*: it facilitates prolonged tracking of all drivers in the
10 city, before SJPd has any possible justification to surveil them, revealing previously unknowable
11 intimate details of their lives. And it does so through the preemptive collection of vast repositories
12 of searchable data. All of these pervasive surveillance technologies are “qualitatively different”
13 from traditional police surveillance, (*Carpenter*, 585 U.S. at 309), and it is “impossible to think of
14 late-18th-century situations that are analogous.” (*Jones*, 565 U.S. at 420 (Alito, J., concurring in
15 judgment).)

16 The *Carpenter* Court listed several factors identifying why police acquisition of CSLI
17 interfered with reasonable expectations of privacy in movements and thus constituted a search.
18 Each applies equally to police queries of SJPd’s ALPR database.

19 1. Detailed

20 *Carpenter* reasoned that “like GPS tracking of a vehicle, cell phone location information is
21 detailed, encyclopedic, and effortlessly compiled.” (585 U.S. at 309.)

22 SJPd’s ALPR database shares these characteristics. GPS coordinates associated with ALPR
23 records can place vehicles right next to a particular camera, (Compl. ¶ 16), locating an individual’s
24 car with even more precision than the cell phone data at issue in *Carpenter*, which ranged in
25 accuracy from one-eighth of a mile to four miles. (*Id.* at 312.)

26 SJPd’s ALPR network is pervasive in space. SJPd operates at least 474 ALPR cameras.
27 (Compl. ¶ 24.) They are strategically installed across the entire city, including near highly sensitive
28 locations, such as healthcare clinics, immigration centers, and places of worship, and in residential

1 areas, tracking people going to and from their homes. (Compl. ¶¶ 52–55.) With multiple captures
2 over a short time, police can infer a driver’s route using the location, timestamp, and direction of
3 travel. (Compl. ¶¶ 46–47.) Likewise, the absence of captures can exclude places a driver could not
4 have reached without passing a camera. (Compl. ¶¶ 32, 46–47.) SJPd officers can even track a
5 driver after they leave San Jose and enter a neighboring city, through Flock’s data sharing system.
6 (Compl. ¶¶ 34, 42; cf. Demurrer at 6.)

7 SJPd’s ALPR System is also pervasive in time. Unlike police officers, ALPR cameras
8 engage in constant, around-the-clock surveillance—collecting data 24 hours a day, seven days a
9 week, 365 days a year. (Compl. ¶ 18.) This continuous collection is more comprehensive than the
10 CSLI in *Carpenter* or the AIR data in *Leaders of a Beautiful Struggle*. (See *United States v.*
11 *Carpenter* (6th Cir. 2016) 819 F.3d 880, 885 [CSLI only recorded at the start and end of calls];
12 *Leaders of a Beautiful Struggle*, 2 F.4th at 334, 342 [aerial images captured only in daylight and
13 good weather, often yielding “shorter snippets of several hours or less”].) And because SJPd retains
14 ALPR data for a year or at least a month, it is a “detailed, encyclopedic” record of drivers’
15 movements over an extended period. (*Carpenter* 585 U.S. at 309.)

16 Such precise, pervasive tracking of people’s locations over time reveals intimate
17 information about their lives. (Compl. ¶¶ 32, 46.) Among other reasons, people’s movements are
18 predictable and unique. “[M]any people start and end most days at home, following a relatively
19 habitual pattern in between.” (*Leaders of a Beautiful Struggle*, 2 F.4th at 343.) As the *Carpenter*
20 Court explained, “time-stamped [location] data provides an intimate window into a person’s life,
21 revealing not only his particular movements, but through them his familial, political, professional,
22 religious, and sexual associations.” (565 U.S. at 311, quotations omitted.) “These location records
23 hold for many Americans the privacies of life.” (*Ibid.*)

24 SJPd’s ALPR System raises identical concerns—even for drivers who pass relatively few
25 cameras on a given day. (Compl. ¶ 47.) Just a few ALPR data points are enough to identify
26 someone and make inferences about their associations and habits, including the homes, businesses,
27 and neighborhoods they frequent. (*Ibid.*) As *Leaders of a Beautiful Struggle* explained, “it is almost
28 always possible to identify people by observing even just a few points of their location history.” (2

1 F.4th at 343; see also *Chatrie*, 2026 WL 1855568 at *20 [recognizing the capacity “of short-term
2 location information to reveal private matters.”].) Indeed, identifying specific people is the entire
3 point of deploying a system like this one. Likewise, the Supreme Court “has already rejected the
4 proposition that ‘inference insulates a search.’” (*Carpenter*, 585 U.S. at 312 [quoting *Kyllo*, 533
5 U.S. at 36]; cf. *Demurrer* at 3 [implausibly insisting ALPR cameras “captur[e] the activities of
6 vehicles, not persons.”].)

7 SJPD’s ALPR System need not capture the literal “whole” of people’s movements to be a
8 search. (Cf. *Demurrer* at 6 [quoting *Carpenter*, 585 U.S. at 310].) After all, “[t]he datasets in *Jones*
9 and *Carpenter* [and *Leaders of a Beautiful Struggle*] had gaps in their coverage, too,” but “in [all
10 three] cases, the surveillance still surpassed ordinary expectations of law enforcement’s capacity
11 and provided enough information to deduce details from the whole of the individuals’ movements.”
12 (*Leaders of a Beautiful Struggle*, 2 F.4th at 342–343; see *id.* at 343 [even where location data has
13 gaps, the sensitivity of certain locations will often allow police to “deduce identity”].) As to *United*
14 *States v. Yang* (9th Cir. 2020) 958 F.3d 851, 863–864 (Bea, J., concurring), the lone judge
15 Defendants cite explicitly reserved the issue of more extensive ALPR searches than those at issue in
16 that case. (Cf. *Demurrer* at 6.)

17 2. Effortless

18 *Carpenter* reasoned that “cell phone tracking is remarkably easy, cheap, and efficient
19 compared to traditional investigative tools.” (585 U.S. at 311.)

20 SJPD’s ALPR System is also, by leaps and bounds, easier, cheaper, and more efficient than
21 any traditional investigative technique. Unlike an officer posted at a street corner, ALPRs do not
22 blink, take breaks, or sleep, and a single ALPR camera can capture the locations of thousands of
23 drivers in minutes, all without any human involvement. (Compl. ¶18.) Even officers stationed at
24 474 locations, and working 24/7 without breaks, could not take note of the license plate, direction,
25 time, and surrounding detail of every single passing car. And if they could, they would not be able
26 to instantaneously relay all this information back to a central hub where, “[w]ith just the click of a
27 button, [SJPD] can access [this] deep repository of historical location information at practically no
28 expense.” (*Carpenter*, 585 U.S. at 311.) No “traditional” surveillance method could realistically

1 come close to duplicating this ALPR dragnet.

2 3. Indiscriminate

3 *Carpenter* reasoned that “this newfound [CSLI] tracking capacity runs against everyone,”
4 and “[o]nly the few without cell phones could escape this tireless and absolute surveillance.” (585
5 U.S. at 312.)

6 The same is true of SJPD’s ALPR System. For the vast majority of people living and
7 working in San Jose, the choice to drive is “indispensable to participation in modern society.” (*Id.* at
8 298.) San Jose is a car-dependent city, too large to traverse by foot and often lacking meaningful
9 public transportation alternatives. (Compl. ¶ 49.) For many, it would be difficult to get to work, pick
10 up kids, or obtain medical care without driving. (Compl. ¶ 3.)⁴

11 Yet, once people get behind the wheel, there is little they can do to avoid SJPD’s ALPR
12 System. It automatically captures images of every vehicle that comes into view, even though there
13 is no suspicion that any given driver has violated the law. (Compl. ¶ 16.)⁵ This dragnet surveillance
14 is indiscriminate. As in *Carpenter*, where the “newfound tracking capacity r[an] against everyone,”
15 (585 U.S. at 312), SJPD is collecting all drivers’ location data because some tiny fraction of them
16 might later be accused of crimes.

17 Whereas ALPRs are indiscriminate, surveillance systems such as the beeper placed on a
18 single truck are targeted. (Cf. Demurrer at 3 [citing *United States v. Knotts* (1983) 460 U.S. 276].)
19 Because it targets *all* drivers on San Jose’s roads regardless of suspicion, the ALPR dragnet here is
20 governed squarely by *Carpenter*.

21
22
23 ⁴ Defendants’ emphasis of alternative forms of travel is both legally irrelevant and factually dubious.
24 (See Demurrer at 5.) Legally, people do not voluntarily expose themselves to long-term surveillance
25 as a condition of driving any more than they do as a condition of using a cell phone. (See *Carpenter*,
26 585 U.S. at 314.) Factually, many people have good reasons to drive their own cars rather than rely
27 on Defendants’ proffered alternatives. Mass transit does not serve every part of the city and can take
28 much longer. Fee-per-ride (Waymo, Uber, Lyft, taxi, Zipcar, and car rental) can cost more than car
ownership. Active transit (bikes, pedicabs, e-scooters, and e-bikes) is not an option for many
disabled people and can only be used for limited distances. And carpooling or borrowing a car is
often impractical.

⁵ Only a tiny fraction of scanned plates are a “hit” on a hot list. (Compl. ¶ 28.) In 2024, there were
only 923,159 hits for 361,494,941 scans, for a hit rate of only 0.2%. (Compl. ¶ 29.)

1 4. Retrospective

2 *Carpenter* distinguished CSLI from traditional law enforcement surveillance because of “the
3 retrospective quality of the data” which “gives police access to a category of information otherwise
4 unknowable.” (585 U.S. at 312.) As the Court explained: “[i]n the past, attempts to reconstruct a
5 person’s movements were limited by a dearth of records and the frailties of recollection. With
6 access to CSLI, the Government can now travel back in time to retrace a person’s whereabouts,
7 subject only to the retention policies of the wireless carriers” (*Ibid.*)

8 Like CSLI, SJPD’s ALPR System allows police to “travel back in time” to “reconstruct a
9 person’s movements.” (*Ibid.*) SJPD retains ALPR data for a year, (Compl. ¶ 31), or at least a month.
10 Either way, this is far longer than the seven days in *Carpenter*, (585 U.S. at 302), and of a piece
11 with the 45 days in *Leaders of a Beautiful Struggle* (2 F.4th at 341–342). Indeed, accessing “even
12 two hours” of location information can be revealing enough to constitute a privacy invasion.
13 (*Chatrie*, 2026 WL 1855568 at *12.) SJPD’s ability to recreate individuals’ movements over time
14 thus infringes their reasonable expectations of privacy.

15 In sum, SJPD’s ALPR System embodies the same characteristics that led *Carpenter* to
16 conclude that police access to CSLI invaded reasonable expectations of privacy. It has the capacity
17 to “effortlessly compile[]” highly “detailed” information, (585 U.S. at 309), to record
18 indiscriminately in a way that “runs against everyone,” (*id.* at 312), and to generate “retrospective”
19 data that could be mined by law enforcement—granting “police access to a category of information
20 [that is] otherwise unknowable.” (*Ibid.*) Thus, queries of SJPD’s historical ALPR database burden
21 reasonable expectations of privacy and constitute a search.

22 Finally, because SJPD does not obtain warrants to conduct these searches, (Compl. ¶ 45),
23 they are “per se unreasonable.” (*People v. Laiwa* (1983) 34 Cal.3d 711, 725; *People v. Superior*
24 *Court* (2006) 143 Cal.App.4th 1183, 1196.) Defendants do not deny that if querying SJPD’s stored
25 ALPR data constitutes a search, then a warrant is required.

26 **II. SJPD’s Retrospective Searches of ALPR Information Violate Article I, Section 1 of**
27 **the California Constitution.**

28 Article I, § 1 of the California Constitution provides all people an inalienable right to

1 privacy, which—contrary to Defendants’ assertion, (Demurrer at 3)—is more protective than the
2 U.S. Constitution. (*In re Carmen M.* (2006) 141 Cal.App.4th 478, 490 n. 10, citation omitted; *Am.*
3 *Academy of Pediatrics*, 16 Cal.4th at 326.) It guarantees the right to be free from government
4 intrusion into private lives. (*Hill v. NCAA* (1994) 7 Cal.4th 1, 35–36.) Privacy “is a fundamental and
5 compelling interest” that prevents “government and business interests from collecting and
6 stockpiling unnecessary information about us”⁶

7 SJPD’s warrantless retrospective searches for driver location information violate Article I, §
8 1. A prima facie claim under Article I, § 1 requires a plaintiff to allege: “(1) a legally protected
9 privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by
10 the defendant constituting a serious invasion of privacy.” (*Hill*, 7 Cal.4th at 39–40.) Any “genuine,
11 nontrivial invasion of a protected privacy interest” shifts the burden to the government to provide
12 “justification for the conduct in question.” (*Loder v. City of Glendale* (1997) 14 Cal.4th 846, 893–
13 894.)⁷ Plaintiffs properly pled facts that satisfy the *Hill* prongs. (Compl. ¶¶ 73–78.)

14 **A. Defendants Violate Legally Protected Privacy Interests.**

15 Defendants violate drivers’ informational and autonomy privacy interests. (Compl. ¶ 76.)
16 People have a legitimate privacy interest in their location information, (see *Carpenter*, 585 U.S. at
17 311), and a privacy interest against government-compiled dossiers of information about them. (See
18 *White v. Davis* (1975) 13 Cal.3d 757, 761 [the “accumulation in ‘police dossiers’ of information . . .
19 presents one clear example of activity which the constitutional amendment envisions as a threat to
20 personal privacy and security.”].) SJPD’s compilation of location information is akin to such
21 dossiers: Warrantless retrospective searches of the ALPR database reveals intimate details about
22 drivers’ lives, including where they live, work, attend religious services, and obtain medical care.
23 (Compl. ¶¶ 36, 46, 48, 76.)

24 _____
25 ⁶ Ballot Pamp., Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27
26 <https://repository.uclawsf.edu/ca_ballot_props/762> (as of June 3, 2026).

27 ⁷ After a plaintiff establishes a prima facie violation, courts may consider a defendant’s
28 countervailing interests. (*Hill*, 7 Cal.4th at 40.) The *existence* of such interests may be “threshold
questions of law” at the demurrer stage, but Defendants do not even attempt to justify their privacy
invasions. (*Ibid.*) Even if they had, the balancing analysis “present[s] mixed questions of law and
fact” that are not considered at the demurrer stage. (*Ibid.*)

1 Defendants incorrectly claim that they do not violate any privacy interest because “at most,
2 the cameras are capturing the activities of vehicles, not persons.” (Demurrer at 3.) ALPR cameras
3 inherently capture information about *drivers*, often capturing images of individual drivers
4 themselves. (Compl. ¶¶ 14, 17, 22.) Even when the driver is not visibly photographed, SJPD can
5 and does easily identify the owner (and often other drivers) of a vehicle. (Compl. ¶ 37; see also
6 Demurrer at 4.) Officers take this identification step every time they act on ALPR information
7 because they investigate and charge individuals, not vehicles. (See *supra* Part I(C).)

8 **B. Defendants Violate Reasonable Expectations of Privacy.**

9 SJPD’s retrospective searches of ALPR information violate a reasonable expectation of
10 privacy. (*Supra* Parts I(B) and I(C); see also Compl. ¶¶ 61, 68, 76.) Customs and practices further
11 support this analysis. (*Hill*, 7 Cal. 4th at 36.) Society has not accepted that police can simply
12 “secretly monitor and catalogue every single movement of an individual’s car for a very long
13 period.” (*Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment).) Nor have Plaintiffs.

14 **C. Defendants’ Conduct Is a Serious Privacy Invasion.**

15 SJPD’s retrospective searches of the ALPR database constitute a *serious* privacy invasion.
16 The ALPR System gathers “intimate details and private facts about the lives of drivers in San Jose”
17 (Compl. ¶ 56) that “can reveal a map of a person’s private habits, movements, and associations and
18 other ‘privacies of life.’” (Compl. ¶ 32 [citing *Carpenter*, 585 U.S. at 311].)

19 SJPD’s ALPR network captures hundreds of millions of driver location datapoints every
20 year. (Compl. ¶¶ 18, 26.) These cameras are placed strategically and collect information on people
21 driving to their homes, clinics, immigration centers, and places of worship. (Compl. ¶¶ 52–55.)
22 Flock also advertises a feature to “uncover vehicles frequently seen together,” which could allow
23 SJPD to “flag people as suspicious in databases solely because they associate together, worship
24 together, or live together.” (Compl. ¶ 36.)

25 SJPD’s warrantless retrospective searches thus violate core privacy interests that the
26 California Constitution specifically protects, including privacy in “our homes, our families . . . our
27
28

1 freedom of communion, and our freedom to associate with the people we choose.”⁸ Plaintiffs
2 alleged Defendants’ violation of these core privacy interests is “serious.” (Compl. ¶ 51.)

3 **III. SJPD’s Retrospective Searches of ALPR Information Violate CCP Section 526a.**

4 Plaintiffs have properly alleged a taxpayer cause of action under Code of Civil Procedure §
5 526a. This “general citizen remedy for controlling illegal governmental activity” allows a taxpayer
6 to sue state or local officials to stop them from violating the Constitution. (*Van Atta v. Scott* (1980)
7 27 Cal.3d 424, 447, citation omitted, abrogated on other grounds, (1995) 9 Cal. 4th 1133;
8 *California DUI Lawyers Ass’n v. California DMV* (2018) 20 Cal.App.5th 1247, 1261 [“Cases that
9 challenge the legality or constitutionality of governmental actions fall squarely within the purview
10 of section 526a.”].) A taxpayer plaintiff need only allege (not prove) that the public expenditure was
11 illegal. (See *California DUI Lawyers Ass’n*, 20 Cal.App.5th at 1260–1261.)

12 Here, Plaintiffs pay taxes to San Jose, and ask the Court to stop Defendants’
13 unconstitutional violations described above. (Compl. ¶¶ 8–9.) Defendants do not dispute that the
14 City expends taxpayer funds, personnel time, and resources to purchase, operate, and maintain
15 SJPD’s ALPR System. (Compl. ¶ 57.) And contrary to Defendants’ claims, (Demurrer at 8),
16 Plaintiffs have adequately alleged that the City spends taxpayer funds to facilitate searches of its
17 ALPR System by external agencies. (Compl. ¶¶ 57, 60, 63.) Finally, as detailed in the Complaint,
18 Plaintiffs have adequately alleged that SJPD’s ALPR System violates the California Constitution.
19 (*Supra* Parts I & II.)

20 **CONCLUSION**

21 For these reasons, Plaintiffs respectfully ask this Court to deny Defendants’ demurrer.

22
23 DATED: July 24, 2026

Respectfully Submitted,

24 **ELECTRONIC FRONTIER**
25 **FOUNDATION**

26 /s/ Elizabeth Femia
27 JENNIFER PINSOFF (SBN 350418)
ELIZABETH FEMIA (SBN 356193)

28
⁸ *Supra* Ballot Pamp., argument in favor of Prop. 11 at 27.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ANDREW CROCKER (SBN 291596)
ADAM SCHWARTZ (SBN 309491)
SAIRA HUSSAIN (SBN 300326)

**ACLU FOUNDATION OF NORTHERN
CALIFORNIA, INC.**

/s/ Nicolas Hidalgo
CHESSIE THACHER (SBN 296767)
NICOLAS HIDALGO (SBN 339177)

Attorneys for Plaintiffs

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

I am employed in San Francisco, California. I am over the age of eighteen years and not a party to the within-entitled action. My business address is American Civil Liberties Union Foundation of Northern California, 39 Drumm Street, San Francisco, CA 94111. My electronic service address is aalas@aclunc.org. On July 24, 2026, I served a copy of the within document(s):

by transmitting via e-mail or electronic transmission the document(s) listed above to the person(s) at the e-mail address(es) set forth below.

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

/s/ Angelina Alas
ANGELINA ALAS