

1 David M. Berger (SBN 277526)
Jane Farrell (SBN 333779)
2 Jennifer Sun (SBN 354276)
Kate Walford (SBN 362658)
3 **GIBBS MURA LLP**
4 1111 Broadway, Suite 2100
Oakland, CA 94607
5 Telephone: (510) 350-9700
Fax: (510) 350-9701
6 dmb@classlawgroup.com
7 jgf@classawgroup.com
jsun@classlawgroup.com
8 kgw@classlawgroup.com

9 Gary M. Klinger*
Mike Acciavatti*
10 Heather M. Lopez (SBN 354022)
11 **MILBERG PLLC**
280 S. Beverly Drive
12 Beverly Hills, CA 90212
Telephone: (331) 240-3015
13 gklinger@milberg.com
macciavatti@milberg.com
14 hmlopez@milberg.com

15 **pro hac vice forthcoming*
16 *Attorneys for Plaintiffs*

**ELECTRONICALLY
FILED**
*Superior Court of California,
County of San Francisco*
02/26/2026
Clerk of the Court
BY: ERNALYN BURA
Deputy Clerk

CGC-26-634334

17 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
18 **COUNTY OF SAN FRANCISCO**

19 DANIEL JAVORSKY and ANTHONY
20 MAYOR, individually and on behalf of all
others similarly situated,

21 Plaintiffs,

22 v.

23 FLOCK GROUP, INC., d/b/a Flock Safety,
24
25 Defendant.
26

Case No. _____

CLASS ACTION

COMPLAINT FOR DAMAGES:

- 27 **(1) Violation of California's ALPR Privacy Act, Cal. Civ. Code §§ 1798.90.5 et seq.**
- (2) Negligence**
- (3) Invasion of Privacy Under California Constitution, Art. 1, Sec. 1**
- (4) Intrusion Upon Seclusion**
- (5) Violations of Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, et seq.**

JURY TRIAL DEMANDED

COMPLEX

1 **TABLE OF CONTENTS**

2 NATURE OF THE CASE..... 2

3 PARTIES 6

4 JURISDICTION AND VENUE..... 6

5 FACTUAL ALLEGATIONS..... 7

6 I. ALPR Cameras and California’s ALPR Privacy Act..... 7

7 II. Flock’s ALPR Cameras and Software Amass, Analyze, and Interpret Massive

8 Amounts of Data, Creating Detailed Vehicle Profiles and Histories in

9 Violation of California Law 11

10 III. Flock Violates California Law by Sharing California ALPR Data with

11 Out-of-State and Federal Agencies 18

12 IV. Flock Violates California Law by Failing to Implement an Adequate Policy

13 or Reasonable Security Procedures to Prevent Unlawful Information Sharing . 26

14 V. Flock’s Security Measures Fall Far Below Reasonable Procedures and

15 Practices..... 29

16 VI. Flock’s Facilitation of California Law Enforcement Agencies’ Unlawful

17 Information Sharing Is Highly Offensive..... 32

18 A. Flock’s Network Amplifies Discriminatory Policing Practices 32

19 B. Cross-Jurisdictional Data Sharing Threatens Access to Abortion and

20 Gender-Affirming Care in California..... 34

21 C. Flock’s ALPR System Threatens Protected First Amendment

22 Activity..... 35

23 PLAINTIFFS’ EXPERIENCES..... 36

24 I. Plaintiff Javorsky’s Experience 36

25 II. Plaintiff Mayor’s Experience 37

26 III. Plaintiffs’ Data from Flock Cameras Has Economic Value..... 39

27 CLASS ACTION ALLEGATIONS..... 40

28 COUNT I: Violation of California’s ALPR Privacy Act 43

COUNT II: Negligence 45

COUNT III: Invasion of Privacy Under California’s Constitution 46

COUNT IV: Intrusion upon Seclusion 49

COUNT V: Violations of California’s Unfair Competition Law (“UCL”) 51

1 PRAYER FOR RELIEF 53
2 DEMAND FOR JURY TRIAL 53

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

1 Throughout California, drivers are tracked by a network of automated license plate
2 recognition (“ALPR”) cameras and software—tens of thousands of high-definition cameras
3 combined with artificial intelligence (“AI”) and sophisticated communications networks—
4 forming a vast, interconnected surveillance dragnet. Defendant Flock Group, Inc. d/b/a Flock
5 Safety (“Defendant” or “Flock”) owns and operates these cameras, oversees the data warehouse
6 that holds the billions of images and data points they capture, and controls the software and AI
7 architecture that facilitates nationwide surveillance through Flock.

8 Though this problem extends far beyond California’s borders, it implicates California law
9 and public policy interests in particularly pressing ways. The California Legislature has balanced
10 the benefits of ALPR technology against the dire threat to privacy rights and civil liberties Flock’s
11 mass surveillance poses. In 2015, California enacted Senate Bill 34 (the “ALPR Privacy Act”),
12 which places clear limits on the ability to legally capture, use, store, and share ALPR data. For
13 example, Flock and other ALPR operators are barred from sharing California ALPR data with
14 federal or out-of-state law enforcement agencies. For years, Flock has blatantly violated these
15 rules, imposing minimal restrictions on nationwide access to California ALPR data. More
16 recently, Flock has taken steps to mimic compliance with California law, which it violated on a
17 massive scale—sometimes with its clients’ assistance, and sometimes without their knowledge.
18 Flock could easily implement policies and design its system to comply with the ALPR Privacy
19 Act; indeed, it is legally required to do so. But it has instead pressed its customers to illegally
20 share information about California drivers’ daily movements. Meanwhile, Flock has openly
21 disclaimed its duty to prevent unlawful information sharing. Flock has repeatedly and publicly
22 disclaimed any responsibility for violations of the ALPR Privacy Act, instead blaming its
23 customers for any violations. In so doing, Flock has ignored its duties under California law.

24 Plaintiffs Daniel Javorsky and Anthony Mayor bring this Class Action Complaint against
25 Flock individually and on behalf of all others similarly situated, and allege upon personal
26 knowledge and their counsel’s investigations as follows:
27
28

1 NATURE OF THE CASE

2 1. Flock has created an Orwellian mass-surveillance infrastructure that is practically
3 impossible to avoid, particularly for anyone operating a vehicle in the towns and cities across this
4 country where Flock has installed its cameras. Flock violates California law by amassing and
5 sharing data on California drivers with out-of-state and federal law enforcement agencies. Flock
6 attempts to evade responsibility and shift liability for its violations by pointing fingers at its own
7 customers.¹ But Flock cannot rely on weaponized incompetence when its obligations under
8 California law are crystal clear.

9 2. ALPR technology captures, analyzes, and shares vehicle data, including a vehicle’s
10 license plate number, often paired with any distinguishing features. Flock aggregates and permits
11 its customers to search this data, which reveals the vehicle’s location and movements over time.
12 Flock markets itself as an end-to-end “safety-as-a-service” business.² It manufactures, owns, and
13 operates ALPR cameras. And Flock also creates, maintains, and controls data warehouses, web
14 interfaces, and applications that enable its customers to access and analyze ALPR data gathered
15 by other customers.

16 3. Flock operates ALPRs nationwide, including thousands of devices across cities
17 throughout California.³ More than 200 California law enforcement agencies use Flock’s ALPR
18 data.⁴

19
20
21 _____
22 ¹ Aaron Mak, *The CEO of Flock downloads on his surveillance cameras*, POLITICO (Dec. 22,
23 2025), <https://www.politico.com/newsletters/digital-future-daily/2025/12/22/the-ceo-of-flock-downloads-on-his-surveillance-cameras-00703165> (In an interview, Flock’s CEO is reported to have said, “[Flock] built a product that allows communities to put safeguards into the product.”)

24 ² Frequently Asked Questions: Why can’t I buy Flock Safety cameras?, FLOCK SAFETY,
25 <https://www.flocksafety.com/faq> [<https://perma.cc/L4MU-CVPW>] (last visited Feb. 22, 2026).

26 ³ See *ALPR Map*, DEFLOCK, <https://deflock.me/map> (last visited Feb. 9, 2026).

27 ⁴ Rachel Myrow, *California Cities Double Down on License-Plate Readers as Federal Surveillance Grows*, KQED (Dec. 18, 2025), [hereinafter Rachel Myrow, *California Cities Double Down*], <https://www.kqed.org/news/12066989/california-cities-double-down-on-license-plate-readers-as-federal-surveillance-grows> (last updated Dec. 18, 2025, at 12:30 PT).

1 4. Flock places high-definition cameras in fixed, high-traffic locations, creating a
2 “digital neighborhood watch” that records the time and location of any vehicle that passes by,
3 including the license plate number, along with vehicle characteristics such as make, color, and
4 distinguishing features.

5 5. While the California Legislature recognizes the benefits that ALPR technology can
6 provide to law enforcement agencies, it also recognizes that ALPR technology can invade
7 personal privacy and harm civil liberties.

8 6. California’s ALPR Privacy Act⁵ explicitly prohibits California law enforcement
9 agencies and Flock from sharing California ALPR data with federal agencies or out-of-state law
10 enforcement agencies. It also requires Flock to ensure its California customers use ALPR
11 information only for authorized purposes, and maintain reasonable security measures to prevent
12 unauthorized access and use. Flock has blatantly violated these requirements for the California
13 entities using its products and services.

14 7. Flock’s business practices flout California law. These practices include the
15 maintenance of a “national network” which aggregates data from Flock databases across the
16 country and makes this information available to state and federal law enforcement nationwide.

17 8. In fact, Flock explicitly advertises its interconnected, nationwide network of ALPR
18 data as a coveted product feature to potential customers. Its website invites agencies to tap into
19 “the nation’s largest crime-solving LPR network,” which collects more than 20 billion license
20 plate reads from across the country every month.⁶

21
22 _____
23 ⁵ Throughout this Complaint, the ALPR Privacy Act will refer to the laws codified in Cal. Civ.
24 Code §§1798.90.5 *et seq.*

25 ⁶ License Plate Readers (LPR): Stop Crime in Its Tracks with Evidence That Drives Action,
26 FLOCK SAFETY [hereinafter Flock License Plate Readers],
27 <https://www.flocksafety.com/products/license-plate-readers> [<https://perma.cc/RZU8-K5HG>]
28 (last visited Feb. 20, 2026); National LPR Network: Real-Time Vehicle Leads, Nationwide,
FLOCK SAFETY [hereinafter Flock National LPR Network],
<https://www.flocksafety.com/products/national-lpr-network> [<https://perma.cc/PL36-XJVM>] (last
visited Feb 20, 2026).

1 9. Flock has violated the ALPR Privacy Act—and Californian drivers’ privacy
2 rights—an untold number of times by facilitating federal agencies’ and out-of-state law
3 enforcement’s access to and use of its California ALPR databases and failing to implement
4 reasonable security measures to prevent such unauthorized access.

5 10. Flock’s illegal data sharing of California ALPR information is pervasive, blatant,
6 and often occurs unbeknownst to and against the wishes of its own customers.

7 11. Across California, out-of-state and federal agency sharing is pervasive. For
8 example, Flock allowed law enforcement agencies from outside of California to search the San
9 Francisco Police Department’s ALPR database more than 1.6 million times between August 2024
10 and February 2025.⁷ Likewise, Flock allowed agencies from 48 other states to search the Los
11 Altos, California database over a million times in 2024 and 2025.⁸ And Flock shares El Cajon’s
12 ALPR network data with over 300 out-of-state law enforcement agencies, including those in
13 Alabama, Minnesota, Ohio, and Texas.⁹

14 12. Flock blatantly ignores the ALPR Privacy Act and its intentional restrictions on
15 ALPR data, so much so that its own customers are often unaware that their data is being shared
16 with out-of-state and federal agencies. The Mountain View Police Department, for example, only
17 recently discovered, after being prompted to respond to ALPR Privacy Act-enabled public records
18 requests, that federal agencies accessed its cameras’ data through a nationwide search tool and
19 that this feature was “enabled without MVPD’s permission or knowledge.”¹⁰

22 ⁷ Tomo Chien, *SFPD let Georgia, Texas cops illegally search city surveillance data on behalf of*
23 *ICE*, S.F. STANDARD (Sept. 8, 2025, at 6:00 AM PT) [hereinafter Chien, *Georgia, Texas cops*
24 *illegally search*], <https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing>.

25 ⁸ *ALPR Updated Analysis Sept. 2025*, LOS ALTOS FOR REPRESENTATION AND EQUITY
(Sept. 2025), <https://www.lare.org/alpr-updated-analysis>.

26 ⁹ El Cajon CA PD Transparency Portal, FLOCK SAFETY, [hereinafter El Cajon Transparency
27 Portal], <https://transparency.flocksafety.com/-el-cajon-pd-ca> (last accessed Feb. 20, 2026).

28 ¹⁰ Katie Debenedetti, *As California Cities Grow Wary of Flock Safety Cameras, Mountain View*
Shuts Its Off, KQED [hereinafter Debenedetti, *California Cities Grow Wary*] (Feb 3, 2026),

1 13. Sometimes, Flock persists in sharing ALPR data in violation of the ALPR Privacy
2 Act, even when an agency has explicitly requested otherwise. The Los Altos Police Department,
3 for example, found that Flock somehow allowed at least one federal agency to search its database
4 even after specifically configuring Flock system settings to prohibit out-of-state and federal
5 sharing.¹¹

6 14. As Flock continued to violate the ALPR Privacy Act, some California cities are
7 rethinking their partnerships with Flock.¹² Numerous others have begun to opt out of using Flock
8 and its services altogether. In recent months, the cities of Santa Cruz, Richmond, Mountain View,
9 and Los Altos Hills all shut down Flock cameras or terminated their contracts.¹³

10 15. As part of a lawsuit to stop Flock’s sharing information from the El Cajon,
11 California Police Department, the California Attorney General stated: “When information about
12 Californians leaves the state, we no longer have any say over how it is used or shared. That’s why
13 the California Legislature passed the ALPR Privacy Act — to ensure information about
14 Californians remains here in California.” “California law prohibits the sharing of license plate
15 data with federal and out-of-state agencies” and doing so “jeopardizes the privacy and safety of
16 individuals in its community.”¹⁴

17
18
19 [https://www.kqed.org/news/12072077/as-california-cities-grow-wary-of-flock-safety-cameras-
mountain-views-shuts-its-off](https://www.kqed.org/news/12072077/as-california-cities-grow-wary-of-flock-safety-cameras-mountain-views-shuts-its-off).

20 ¹¹ *ALPR Updated Analysis Sept. 2025, supra* note 8.

21 ¹² Brandon Pho, *Santa Clara County cities weigh ending Flock Safety contracts over ICE*
22 *access*, LOCAL NEWS MATTERS (Feb. 3, 2026),
23 <https://localnewsmatters.org/2026/02/03/silicon-valley-flock-safety-license-plate-readers-ice/>.

24 ¹³ Rachel Myrow, *Santa Cruz the First in California to Terminate Its Contract With Flock*
25 *Safety*, KQED (Jan. 14, 2026), [https://www.kqed.org/news/12069705/santa-cruz-the-first-in-
california-to-terminate-its-contract-with-flock-safety](https://www.kqed.org/news/12069705/santa-cruz-the-first-in-california-to-terminate-its-contract-with-flock-safety); Drew Penner, *Los Gatos officials debate*
26 *license plate readers, after Santa Cruz, Los Altos Hills jettison Flock Safety service*, LOS
27 *GATAN* (Jan. 28, 2026), [https://losgatan.com/los-gatos-officials-debate-license-plate-readers-
after-santa-cruz-los-altos-hills-jettison-flock-safety-service/](https://losgatan.com/los-gatos-officials-debate-license-plate-readers-after-santa-cruz-los-altos-hills-jettison-flock-safety-service/); Debenedetti, *California Cities*
Grow Wary, *supra* note 10.

28 ¹⁴ Press Release, Off. of the Att’y Gen., Cal. Dep’t of Just., Attorney General Bonta Sues El
Cajon for Illegally Sharing License Plate Data with Out-of-State Law Enforcement (Oct. 3,

1 16. Flock has shown a complete and continued disregard for California law. Plaintiffs
2 now seek to bring this class action lawsuit alleging violations of the ALPR Privacy Act,
3 California’s Unfair Competition Law, and California Constitutional and common law, and
4 requesting damages and injunctive relief.

5 **PARTIES**

6 17. Plaintiff Daniel Javorsky is a natural person and a citizen of the State of California.
7 Plaintiff Javorsky resides in San Francisco, California.

8 18. Plaintiff Anthony Mayor is a natural person and a citizen of the State of California.
9 Plaintiff Mayor resides in San Rafael, California.

10 19. Defendant Flock Group, Inc. d/b/a Flock Safety is a corporation formed under the
11 laws of Delaware. It is headquartered at 1160 Howell Mill Road NW, Suite 210 in Atlanta,
12 Georgia.

13 **JURISDICTION AND VENUE**

14 20. This Court has original jurisdiction over the matters alleged in this Complaint
15 pursuant to California Constitution, Article VI, § 10.

16 21. This Court has personal jurisdiction over Flock pursuant to California Code of
17 Civil Procedure §§ 410.10, 335, 337, 338 *et. seq.*, because Flock has purposefully availed itself
18 of the benefits and burdens of doing business in California and under California law. Flock has
19 sufficient minimum contacts such that exercising personal jurisdiction over it comports with
20 traditional notions of fair play and substantial justice. Indeed, Flock has numerous contracts with
21 California law enforcement agencies (and other entities in California, including municipalities and
22 private organizations like malls and homeowners’ associations). Additionally, Flock has
23 thousands of cameras located in California, which it uses to take billions of license plate scans of
24 California vehicles, and regularly interacts with California law enforcement agencies. Plaintiffs’
25 claims arise out of and relate to Flock’s California contacts.

26 _____
27
28 2025), <https://oag.ca.gov/news/press-releases/attorney-general-bonta-sues-el-cajon-illegally-sharing-license-plate-data-out>.

1 25. ALPR surveillance occurs almost exclusively without drivers’ knowledge as it
2 targets both active drivers and stationary vehicles parked on public streets in view of Flock
3 technology. Flock has specifically ignored the ALPR Privacy Act’s strict operator requirements.

4 26. The ALPR Privacy Act mandates that *both* the “operators” of commercial ALPR
5 technology like Flock and its California “end-users” and customers (e.g., law enforcement
6 departments and private businesses) adhere to five fundamental requirements:¹⁷

7 a. **The Security Requirement:** Both ALPR operators and end-users must “maintain
8 reasonable security procedures and practices, including operational,
9 administrative, technical, and physical safeguards, to protect ALPR information
10 from unauthorized access, destruction, use, modification, or disclosure.” Cal Civ.
11 Code § 1798.90.51(a); *id.* § 1798.90.53(a).

12 b. **The Privacy Requirement:** Both ALPR operators and end-users must “implement
13 a usage and privacy policy in order to ensure that the collection, use, maintenance,
14 sharing, and dissemination of ALPR information is consistent with respect for
15 individuals’ privacy and civil liberties.” *Id.* § 1798.90.51(b)(1); *id.* §
16 1798.90.53(b)(1).

17 c. **The Notice Requirement:** Both ALPR operators and end-users must post the
18 usage and privacy policy “conspicuously” on their website and include the
19 following information:

20 i. The authorized purposes for using the ALPR system and collecting ALPR
21 information.

22 ii. A description of the job title or other designation of the employees and
23 independent contractors who are authorized to use or access the ALPR
24 system, or to collect ALPR information. The policy shall identify the training
25 requirements necessary for those authorized employees and independent
26 contractors.

27 _____
28 ¹⁷ Cal. Civ. Code § 1798.90.5.

- 1 iii. A description of how the ALPR system will be monitored to ensure the
2 security of the information and compliance with applicable privacy laws.
- 3 iv. The purposes of, process for, and restrictions on, the sale, sharing, or transfer
4 of ALPR information to other persons.
- 5 v. The title of the official custodian, or owner, of the ALPR system responsible
6 for implementing this section.
- 7 vi. A description of the reasonable measures that will be used to ensure the
8 accuracy of ALPR information and correct data errors.
- 9 vii. The length of time ALPR information will be retained, and the process the
10 ALPR operator will utilize to determine if and when to destroy retained
11 ALPR information.

12 *Id.* §§ 1798.90.51(b), 1798.90.53(b).

13 27. Crucially, ALPR operators like Flock must also comply with two additional
14 requirements to ensure consumer privacy and protect against unauthorized access:

15 a. **The Audit Requirement.** ALPR operators must maintain a record of the times
16 their ALPR system is accessed, whether by the operators, its employees, or an end-
17 user. *Id.* § 1798.90.52(a). The audit trail must note the date and time of the query,
18 the data that was queried, who queried it, and the purpose of the query. *Id.*
19 § 1798.90.52(a).

20 b. **The Proper Use Requirement.** ALPR operators must also “require that ALPR
21 information only be used for the authorized purposes described in the usage and
22 privacy policy” *Id.* §1798.90.52(b).

23 28. California public agencies collecting ALPR data may not share ALPR data with
24 federal agencies or out-of-state law enforcement agencies. “A public agency shall not sell, share,
25 or transfer ALPR information, except to another public agency, and only as otherwise permitted
26 by law.” *Id.* § 1798.90.55(b).

1 29. “Public agency” for purposes of the ALPR Privacy Act means “the state, any city,
2 county, or city and county, or any agency or political subdivision of the state or a city, county, or
3 city and county, including, but not limited to, a law enforcement agency.” *Id.* § 1798.90.5(f).

4 30. The California AG has interpreted this plain text of the ALPR Privacy Act
5 (including, crucially, §§ 1798.90.5(f) & 1798.90.55(b)) as permitting sharing of ALPR data only
6 with other California state and local agencies.

7 31. The California AG emphasized:¹⁸

8 Importantly, the definition of ‘public agency’ is limited to state or local agencies,
9 including law enforcement agencies, and does not include out-of-state or federal
10 law enforcement agencies. (See Civ. Code, § 1798.90.5, subd. (f).) Accordingly,
11 [the ALPR Privacy Act] does not permit California LEAs [Law Enforcement
12 Agencies] to share ALPR information with private entities or out-of-state or federal
13 agencies, including out-of-state and federal law enforcement agencies. This
14 prohibition applies to ALPR database(s) that LEAs access through private or
15 public vendors who maintain ALPR information collected from multiple databases
16 and/or public agencies.¹⁹

17 32. Likewise, the California AG has clarified that, under the ALPR Privacy Act,
18 “ALPR operators [like Flock] . . . must develop a usage and privacy policy, which must be
19 conspicuously posted on their website, and must contain provisions designed to ‘protect ALPR
20 information from unauthorized access, destruction, use, modification, or disclosure.’”²⁰

21 33. The ALPR Privacy Act contains no exceptions that would permit sharing ALPR
22 data collected in California with federal or out-of-state agencies for any purpose. Consistent with
23 the California AG’s interpretation of the ALPR Privacy Act, any such sharing is clearly prohibited
24 by the Act’s plain text.

25 _____
26 ¹⁸ John D. Marsh, Div. of L. Enf’t, Cal. Dep’t of Just., Info Bull. 2023-DLE-06, California
Automated License Plate Reader Data Guidance (Oct. 27, 2023),
<https://oag.ca.gov/system/files/media/2023-dle-06.pdf>.

27 ¹⁹ *Id.*

28 ²⁰ *Id.*

1 34. An individual harmed by a violation of the ALPR Privacy Act—“including, but
2 not limited to, unauthorized access or use of ALPR information or a breach of security of an ALPR
3 system”—may bring a civil suit “against a person who knowingly caused the harm” and recover
4 (1) actual damages, but not less than liquidated damages in the amount of \$2,500, (2) punitive
5 damages upon proof of willful or reckless disregard of the law, (3) reasonable attorney’s fees and
6 other litigation costs reasonably incurred, and (4) other preliminary and equitable relief as the
7 court determines to be appropriate. *Id.* § 1798.90.54.

8 35. Here, Flock has knowingly been in violation of the ALPR Privacy Act since its
9 enactment in 2015, and its violations are made more egregious by its proprietary technologies
10 described below.

11 **II. Flock’s ALPR Cameras and Software Amass, Analyze, and Interpret Massive**
12 **Amounts of Data, Creating Detailed Vehicle Profiles and Histories in Violation of**
13 **California Law**

14 36. In the decade since the ALPR Privacy Act was enacted, ALPR camera technology
15 has become more sophisticated, as has the software and algorithms that companies like Flock use
16 to analyze and organize that data. One of the primary shifts between past and present ALPR
17 technology is the transition from capturing images to doing a real-time analysis and extensive
18 tracking of license plates and vehicles.

19 37. Flock captures vehicle data and identifies automobiles through an integrated
20 system of hardware, artificial intelligence, and cloud computing that goes far beyond just
21 collecting license plates.

22 38. Advancements in camera technology have allowed for the widespread proliferation
23 of ALPR cameras. Flock’s ALPR system alone now includes tens of thousands of cameras
24 nationwide.

25 39. Flock’s most popular products, the “Falcon” and the “Sparrow,” are ALPR
26 cameras that monitor driving activity and photograph all passing vehicles.

1 40. The below images from Flock’s website show typical examples of Flock ALPR
2 cameras mounted on existing traffic poles or on their own freestanding poles with their solar
3 power sources.



11 41. When a Flock ALPR camera identifies a vehicle, it snaps pictures of the license
12 plate and the rest of the vehicle, each time stamped and tagged with precise GPS coordinates.
13 Flock cameras even capture images of bicyclists, even though bicycles don’t have license plates.²¹

14 42. Flock uses OCR software to isolate the license plate from the close-framed image
15 and convert the image into machine-readable text, i.e., the plate number. Flock ALPR cameras
16 capture at least the following information:²²

- 17 a. License plate image;
18 b. Vehicle image;
19 c. Vehicle characteristics (e.g., color, make, other vehicle attributes);
20 d. License plate number;
21 e. License plate state;

22
23
24 ²¹ Frequently Asked Questions: What kind of vehicles can a Flock Safety camera identify?,
25 FLOCK SAFETY, <https://www.flocksafety.com/faq> [<https://perma.cc/L4MU-CVPW>] (last
26 visited Feb. 21, 2026); Here’s the Data Police Actually Get from Traditional License Plate
Reading Systems, FLOCK SAFETY (Mar. 28, 2019), [https://www.flocksafety.com/blog/heres-
the-data-police-actually-get-from-traditional](https://www.flocksafety.com/blog/heres-the-data-police-actually-get-from-traditional) [<https://perma.cc/HT32-3JXD>].

27 ²² License Plate Reader Policy, FLOCK SAFETY [hereinafter Flock LPR Policy],
28 <https://www.flocksafety.com/legal/lpr-policy> [<https://perma.cc/8CPY-TADR>] (last updated Nov.
13, 2025).

- f. Date;
- g. Time; and
- h. Camera location.

43. Other vehicle attributes may include bumper damage or a roof rack, as seen in the following image on Flock’s website.²³



44. Flock transmits these images and extracted information to its cloud servers. Once in the cloud, Flock then cross-checks the plate number against official state and law enforcement databases and feeds the ALPR data into a myriad of algorithms and tools to provide its customers with an ever-growing trove of information.

45. Flock uses images of a vehicle’s rear to generate its “Vehicle Fingerprint,”²⁴ which creates a unique profile for the vehicle so it can be quickly identified if it is captured on camera

²³ The image is taken from Flock’s website. (“roof rack” as an example is from the 27 Flock Evidence Policy. *See* Flock Evidence Policy, FLOCK SAFETY, <https://www.flocksafety.com/legal/flock-evidence-policy> [<https://perma.cc/74YF-XNYN>] (last updated January 9, 2026)).

²⁴ 6 Myths About License Plate Readers and Security Systems, FLOCK SAFETY (May 31, 2023), <https://www.flocksafety.com/blog/6-myths-license-plate-readers-security-systems> [<https://perma.cc/Q9WN-HJQC>] (Last visited Feb. 20, 2026).

1 in the future. Relying solely on this Vehicle Fingerprint, Flock can even identify vehicles with no
2 license plate or temporary paper tags.²⁵

3 46. Flock also uses the images captured by its cameras to train the AI models and
4 software systems that power many of its products.²⁶

5 47. Flock’s FreeForm product allows customers to search for vehicles using natural
6 language if they don’t have a license plate number to search. For example, a user could search for
7 “red pickup truck with a dog in the bed,” to find a red pickup truck carrying a dog.²⁷ Flock’s
8 powerful tools allow its customers to search for cars and people using granular details.

9 48. Flock’s “Investigations Manager” tool²⁸ proactively analyzes movement patterns
10 and related data to flag potentially “suspicious” vehicles. It identifies vehicles that tend to move
11 together and labels the cars and affiliated individuals as “suspect networks.” In marketing
12 materials for Investigations Manager, Flock “urges police departments to ‘Maximize [their] LPR
13 data to detect patterns of suspicious activity across cities and states.’”²⁹

14 49. Flock also touts its AI-powered [1] “Multi-State Insights feature,” which alerts law
15 enforcement “when suspect vehicles have been detected in multiple states”; [2] “Linked Vehicles”
16 or “Convoy Search,” which allows law enforcement to “uncover vehicles frequently seen
17
18

19 ²⁵ *Id.*; Flock License Plate Readers, *supra* note 6 (“No Plate? No Problem. Turn images into
20 actionable evidence – no plate required.”).

21 ²⁶ Privacy Policy, FLOCK SAFETY, <https://www.flocksafety.com/legal/privacy-policy>
22 [<https://perma.cc/7T8D-AALC>] (last updated Aug. 1, 2025).

23 ²⁷ Flock License Plate Readers, *supra* note 6.

24 ²⁸ Investigations Manager: Connect the Dots. Close More Cases., FLOCK SAFETY,
25 <https://www.flocksafety.com/products/investigations-manager> [<https://perma.cc/YTP9-AVER>]
(last visited Feb. 20, 2026).

26 ²⁹ Jay Stanley, *Surveillance Company Flock Now Using AI to Report Us to Police if It Thinks*
27 *Our Movement Patterns Are “Suspicious”*, ACLU: NEWS & COMMENTARY (Aug. 7, 2025),
28 [hereinafter Jay Stanley, “*Suspicious” Movement Patterns*] <https://www.aclu.org/news/national-security/surveillance-company-flock-now-using-ai-to-report-us-to-police-if-it-thinks-our-movement-patterns-are-suspicious>.

1 together,” thus tracking people’s associations; and [3] a “Multiple locations search,” which aims
2 to “Uncover vehicles seen in multiple locations.”³⁰

3 50. From a single set of vehicle images, Flock thus creates detailed, searchable, and
4 dangerously actionable data records that extend far beyond just a license plate number.

5 51. The below image from a Flock presentation shows the type of information Flock
6 records and deduces, including that the SUV belongs to a “non resident” and was “[s]een three
7 times in the last 30 days.”



8
9
10
11
12
13
14
15
16
17
18 52. The use of Flock’s high-end but inexpensive tools and the associated databases that
19 Flock has created allow law enforcement agencies across the country to have instant access to
20 shared data from tens of thousands of cameras—exactly the kind of practice that the ALPR Privacy
21 Act regulates.

22 53. An individual Flock camera can photograph thousands of cars per day; for
23 example, Oak Park, Illinois’ eight Flock cameras took over 300,000 scans monthly in the 2022 to
24 2023 timeframe.³¹

25
26
27 ³⁰ *Id.*

28 ³¹ *84% of drivers stopped by Oak Park police in Flock traffic stops were Black*, FREEDOM TO THRIVE OAK PARK: BLOG (Apr. 16), <https://www.freedomtothriveop.com/blog/84-of-the->

1 54. The Los Angeles County Sheriff’s Department alone operates 476 Flock ALPR
2 cameras.³²

3 55. Collectively, the San Francisco and Oakland Police Departments also operate
4 hundreds of Flock cameras.³³

5 56. More than 200 California law enforcement agencies collect and use images
6 captured by Flock ALPR cameras.³⁴

7 57. Flock boasts that over 4,800 law enforcement agencies nationwide use its cameras
8 and it claims to collect 20 billion plate reads per month.³⁵ It prides itself on having the nation’s
9 largest fixed ALPR network. “With billions of monthly plate reads, Flock connects communities,
10 businesses and law enforcement in a shared network[.]”³⁶

11 58. Likewise, Flock’s investors recognize the value of Flock achieving such
12 widespread adoption:

13 What magnifies the power of Flock Safety even more is that the digital evidence
14 can be pooled across different law enforcement agencies for a short period of time,
15 making it more powerful as adoption scales within a community and across the U.S.
16 more broadly. The power of Flock Safety is in its network. The more devices
17 deployed, the more evidence there is to solve crimes.³⁷

18 _____
19 drivers-stopped-by-oak-park-police-in-a-flock-traffic-stops-were-black (last visited Jan. 2,
20 2026).

21 ³² Rebecca Ellis, *L.A. County moves to keep ICE away from data that show where people drive*,
22 L.A. TIMES (Sept. 17, 2025, at 3:00 PT), <https://www.latimes.com/california/story/2025-09-17/la-county-ice-license-plate-data>.

23 ³³ Tomo Chien, *SF, Oakland cops illegally funneled license plate data to feds*, S.F.
24 STANDARD (July 14, 2025, at 6:00 PT) [hereinafter Chien, *SF/Oakland ICE LPRs*],
25 <https://sfstandard.com/2025/07/14/oakland-san-francisco-ice-license-plate-readers/>.

26 ³⁴ Rachel Myrow, *California Cities Double Down*, *supra* note 4.

27 ³⁵ Flock National LPR Network, *supra* note 6.

28 ³⁶ *Id.*

³⁷ David Ulevitch & David George, *Announcement: Investing in Flock Safety*, ANDREESSEN
HOROWITZ (July 13, 2021), <https://a16z.com/announcement/investing-in-flock-safety>.

1 59. Consequently, Flock’s ALPR system reveals “sensitive details about where
2 individuals work, live, associate, worship, seek medical care, and travel.”³⁸ Bypassing warrants
3 and laws designed to protect personal liberties, Flock’s ALPR system tracks, catalogues, and
4 analyzes every turn of every driver’s route, looking for “suspicious activity” to generate new
5 business—not safer communities. As noted in recent reporting by the ACLU, each of Flock’s
6 advanced analytics and AI-powered features “are variants on the same theme: using the camera
7 network not just to investigate based on suspicion, but to generate suspicion itself.”³⁹

8 60. In May 2025, Flock announced the development of a new people search product
9 (“Nova”) that would integrate its ALPR systems with data broker lookups, credit-related
10 information from Equifax and TransUnion, and other external sources—even including stolen
11 personal information from data breaches found on the dark web—to give its customers even more
12 invasive ways to conduct warrantless surveillance.⁴⁰

13 61. At an internal meeting, a Flock employee explained “You’re going to be able to
14 access data and jump from LPR to person and understand what that context is, link to other people
15 that are related to that person [...] marriage or through gang affiliation, et cetera,” demonstrating
16 that Flock is willing to enable even greater (and even more highly offensive) invasions of privacy
17 in its pursuit of profit.

18
19
20 ³⁸ Letter from Jennifer Pinsof, Staff Att’y, Elec. Frontier Found.; Matt Cagle, Senior 18 Staff
21 Att’y, ACLU Found. of N. Cal.; Mohammad Tasjar, Senior Staff Att’y, ACLU Found. of S.
22 Cal.; & David Trujillo, Chief Program & Strategy Officer, to Att’y Gen. Rob Bonta, Off. of the
23 Att’y Gen., Cal. Dep’t of Just., at 2 (Jan. 31, 2024) [hereinafter EFF–ACLU Joint Letter],
24 https://www.eff.org/files/2024/01/30/2024-01-31_letter_to_ag_bonta_re_sb_34_final.pdf (citing
25 *Automatic License Plate Readers*, ELEC. FRONTIER FOUND. (Mar 29, 2023),
<https://sls.eff.org/technologies/automated-license-plate-readers-alprs>; *You Are Being Tracked:
How License Plate Readers Are Being Used to Record Americans’ Movements*, ACLU (July
2013), <https://www.aclu.org/you-are-being-tracked>).

26 ³⁹ Jay Stanley, “*Suspicious*” *Movement Patterns*, supra note 29.

27 ⁴⁰ Joseph Cox, *License Plate Reader Company Flock Is Building a Massive People Lookup Tool,*
28 *Leak Shows*, 404 MEDIA (May 14, 2025), [https://www.404media.co/license-plate-reader-
company-flock-is-building-a-massive-people-lookup-tool-leak-shows/](https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/).

1 62. ALPR technology’s potential as a crime-fighting tool must be weighed against the
2 increasingly invasive—and highly offensive to a reasonable person—widespread domestic
3 surveillance⁴¹ and profiling of California drivers.

4 **III. Flock Violates California Law by Sharing California ALPR Data with Out-of-State**
5 **and Federal Agencies**

6 63. Flock’s amassment of ALPR camera data, its proprietary surveillance tools, and its
7 ability to profile and track vehicles all raise serious privacy concerns. Of equal concern is that
8 Flock shares this sensitive information with agencies outside of California’s jurisdiction, robbing
9 California drivers of the protections due under their state’s ALPR Privacy Act.

10 64. While the ALPR Privacy Act explicitly prohibits state and local agencies from
11 sharing ALPR data with federal or out-of-state law enforcement, Flock’s infrastructure and
12 business model do just that. Flock’s national network and permissive sharing tools enable and
13 encourage out-of-state state and federal law enforcement like ICE and CBP to track California
14 drivers.

15 65. **The National Lookup Network:** Flock operates a national, interconnected
16 database comprising of over 80,000 cameras across the United States. A core feature of this system
17 for subscribers is the “National Lookup” tool. This function, which Flock or its end-users can turn
18 on, allows anyone with access to query license plate reads from any participating agency.

19 66. Flock’s August 2023 User Guide instructed law enforcement users that their
20 agency could enable National Lookup, which allowed all law enforcement agencies in the country
21 with the same feature enabled to search data obtained through that agency’s Flock cameras as
22 well, with no limitation on California law enforcement agencies.⁴²

23 _____
24 ⁴¹ Flock itself admits that whether its technology can be accurately characterized as “mass
25 surveillance” “depends on several factual questions”. *See Is Flock Mass Surveillance? Here’s*
26 *What 30 Courts Decided* (Feb. 26, 2026) FLOCK SAFETY,
27 <https://www.flocksafety.com/blog/does-flock-enable-mass-surveillance> [[https://perma.cc/Q72R-
HR5C](https://perma.cc/Q72R-HR5C)].

28 ⁴² Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404 MEDIA (May 27, 2025) [hereinafter Koebler & Cox, *ICE Taps into Nationwide Network*], <https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data->

1 67. For example, Flock enabled federal law enforcement agencies, including the
2 Department of Homeland Security (“DHS”) and DHS’s Customs and Border Control (“CBP”)⁴³
3 to access Flock’s National Lookup utility. Flock never even alerted its customers that federal
4 agencies would have access.⁴⁴

5 68. Because Flock did not restrict out-of-state law enforcement agencies’ access to
6 California ALPR data, a sheriff’s department in Georgia and police departments in Illinois and
7 Massachusetts were able to search the San Francisco Police Department’s ALPR data to aid ICE
8 investigations.⁴⁵ After reporting on Flock’s widespread violations gained traction, Flock
9 announced and implemented a series of technical changes, tacitly conceding that its previous
10 practices violated the ALPR Privacy Act.⁴⁶

11 69. Extensive investigations have concluded that Flock connected California
12 customers’ networks to the National Lookup tool, and that some California agencies were
13 themselves unaware that Flock was allowing their ALPR databases to be used in violation of the
14 ALPR Privacy Act. For example, Bernie Escalante, Police Chief of the Santa Cruz Police
15 Department, “said the department learned only recently that Flock’s ‘national search tool’ had
16 been activated in a way that improperly allowed out-of-state law enforcement agencies to search
17

18 _____
19 shows (citing FLOCK SAFETY USER GUIDE AUGUST 2023, FLOCK SAFETY at 3 (2023),
20 <https://www.documentcloud.org/documents/24172417-flocksafetyuserguideaug2023>).

21 ⁴³ Byron Tau and Garance Burke, *Border Patrol is monitoring US drivers and detaining those*
22 *with ‘suspicious’ travel patterns*, THE ASSOCIATED PRESS (Nov. 20, 2025),
<https://www.ap.org/news-highlights/spotlights/2025/border-patrol-is-monitoring-us-drivers-and-detaining-those-with-suspicious-travel-patterns/>.

23 ⁴⁴ Garrett Langley, *Ensuring Local Compliance: A statement from Flock Safety*, FLOCK
24 SAFETY [hereinafter *Ensuring Local Compliance*] (Aug. 25, 2025),
<https://www.flocksafety.com/blog/ensuring-local-compliance> [<https://perma.cc/AR88-U768>].

25 ⁴⁵ Chien, *Georgia, Texas cops illegally search*, *supra* note 7.

26 ⁴⁶ *Why Are Some Flock Cameras Being Removed by Cities?*, FLOCK SAFETY (Feb. 26, 2025),
27 <https://www.flocksafety.com/blog/why-are-some-flock-cameras-being-removed-by-cities>
28 [<https://perma.cc/PA5Z-8E6N>] (detailing data privacy and control practices “[a]s of early 2026...”).

1 camera data from across the entire Flock network—including California agencies legally barred
2 from sharing such information” and that “[t]hese violations were not known to the Santa Cruz
3 Police Department and were not the result of any deliberate attempt by city staff to circumvent
4 California law[.]”⁴⁷

5 70. Flock admits that California was included in the National Lookup service. On
6 February 11, 2025, “Flock . . . notified agencies statewide that a flaw in its system architecture
7 inadvertently allowed law enforcement agencies outside California to conduct broad searches of
8 license-plate data that “violated two laws,” including the ALPR Privacy Act.⁴⁸

9 71. Sometime between March and June 2025, Flock updated its product feature and,
10 in one fell swoop, purported to remove all California agencies and their ALPR information from
11 the National Lookup service.

12 72. In a June 19, 2025 blog post, Flock CEO and Co-Founder Garrett Langley wrote,
13 “Some states, like California, do not allow any sharing across state borders. For those states, Flock
14 has disabled National Lookup to make compliance easier.”⁴⁹ This makes clear that Flock was
15 always capable of complying with California law, including the ALPR Privacy Act.

16 73. But the damage was already done. This violation of trust and others like it have led
17 multiple localities to cut ties with Flock.⁵⁰ In January 2026, the Santa Cruz City Council voted
18
19
20

21 ⁴⁷ Joan Hammel, *Eyes in the Sky: Santa Cruz discloses violations involving ALPRs, launches*
22 *review of camera use*, GOODTIMES (Nov. 26, 2025) [hereinafter Joan Hammel, *Eyes in the*
23 *Sky*], <https://www.goodtimes.sc/santa-cruz-alpr-violations-review-flock-safety>; ACLU of
24 Massachusetts, *Network Sharing Overview* (Youtube, Oct. 7, 2025),
25 https://www.youtube.com/watch?v=S34n0_TBFgo.

26 ⁴⁸ Joan Hammel, *Eyes in the Sky*, *supra* note 47.

27 ⁴⁹ Garrett Langley, *Setting the Record Straight: Statement on Flock Network Sharing, Use*
28 *Cases, and Federal Cooperation*, FLOCK SAFETY: BLOG (June 19, 2025) [hereinafter
Langley, *Setting the Record Straight*], <https://www.flocksafety.com/blog/statement-network-sharing-use-cases-federal-cooperation>.

⁵⁰ *See supra*, note 13.

1 near-unanimously to terminate its contract with Flock, “citing rising tensions with ICE, and weak
2 trust in the company following Flock’s lackluster response to the data breaches.”⁵¹

3 74. Santa Cruz City Councilmember Susie O’Hara stated: “Flock has made too many
4 mistakes and Flock’s leadership has too often dismissed real, valid concern instead of responding
5 with transparency and accountability We need a partner who can take criticism seriously and
6 redirect course.”⁵²

7 75. More recently, leaders in Santa Clara County, California effectively cut ties with
8 Flock, with one Supervisor stating “Flock is a problematic company, and their reported conduct
9 and sharing of private data is incompatible with our county’s values, my personal values and the
10 values that I promised the voters of District 2 that I would uphold”⁵³

11 76. Flock’s technical changes still do not bring Flock into compliance though: Flock’s
12 systems still permit California ALPR data to be shared and accessed by out-of-state and federal
13 law enforcement in many different ways, some of which are detailed in the following paragraphs.

14 77. **1:1 Sharing:** Law enforcement agencies using Flock can enter into 1:1 agreements
15 with other agencies to share ALPR data. Flock makes this possible by allowing any law
16 enforcement agency to “request” access from another agency. An agency may grant the individual
17 or bulk requests through the click of a button, and sometimes even automatically.⁵⁴ Flock’s
18
19
20

21 ⁵¹ B. Sakura Cannestra, *Santa Cruz leaders vote to terminate contract with Flock*, SANTA
22 CRUZ LOCAL (Jan. 13, 2026), <https://santacruzlocal.org/2026/01/13/santa-cruz-leaders-vote-to-terminate-contract-with-flock/>.

23 ⁵² *Id.*

24 ⁵³ Joseph Geha, *Santa Clara County Leaders Cut Out Flock Safety in New Surveillance Policy*,
25 KQED (Feb. 25, 2026), <https://www.kqed.org/news/12074467/santa-clara-county-leaders-cut-out-flock-safety-in-new-surveillance-policy>.

26 ⁵⁴ Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*,
27 ACLU of Massachusetts (October 7, 2025), <https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/>.
28

1 software has thus resulted in both intentional *and* inadvertent sharing in violation of the ALPR
2 Privacy Act.⁵⁵

3 78. Flock claims that it does not allow California agencies to initiate out-of-state
4 sharing relationships, but data from Flock-maintained customer transparency portals say
5 otherwise.⁵⁶ El Cajon, for example, currently maintains 1:1 sharing agreement with hundreds of
6 out-of-state law enforcement agencies.⁵⁷

7 79. Based on public reports, Flock deceives many California law enforcement agencies
8 into sharing their data far more broadly than they intend. This is because Flock’s “1:1” sharing
9 agreements do not function as simple bilateral arrangements between two agencies. Instead, Flock
10 structures its system so that when Agency A enters into a 1:1 agreement with Agency B, Agency
11 A’s data becomes accessible not just to Agency B, but to every agency that Agency B has also
12 agreed to share with—including out-of-state and federal law enforcement. The result is that
13 California agencies are unknowingly feeding Flock ALPR data into a vast, multi-agency
14 surveillance network.

15 80. “Once a department allows another agency to access its system, the outside agency
16 can search the data without needing approval each time.”⁵⁸ Likewise, users can query multiple
17
18

19 ⁵⁵ Spencer Soicher, *Flock admits federal immigration agents have direct access to tracking data,*
20 *despite previous claims*, 9NEWS (August 19, 2025),
21 [https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-](https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8ace742-56d4-4a57-b5bb-0373286dfef8?)
22 [data/73-a8ace742-56d4-4a57-b5bb-0373286dfef8?;](https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8ace742-56d4-4a57-b5bb-0373286dfef8?) Jason Koebler, *CBP Had Access to More*
than 80,000 Flock AI Cameras Nationwide, 404 Media (August 25, 2025),
<https://www.404media.co/cbp-had-access-to-more-than-80-000-flock-ai-cameras-nationwide/>

23 ⁵⁶ Henry Lee and Kayla Galloway, *CHP warns Flock over sharing of surveillance data with*
24 *federal government*, FOX KTVU (Nov. 24, 2025, at 2:12 PT), [https://www.ktvu.com/news/chp-](https://www.ktvu.com/news/chp-warns-flock-over-sharing-surveillance-data-federal-government)
[warns-flock-over-sharing-surveillance-data-federal-government.](https://www.ktvu.com/news/chp-warns-flock-over-sharing-surveillance-data-federal-government)

25 ⁵⁷ El Cajon Transparency Portal, *supra* note 9.

26 ⁵⁸ Tomo Chien, *California cops are breaking surveillance laws. Who’s going to stop them?*, S.F.
27 STANDARD (July 23, 2025, at 6:00 PT) [hereinafter Chien, *California cops are breaking*
28 *surveillance laws*], [https://sfstandard.com/2025/07/23/california-police-sharing-flock-license-](https://sfstandard.com/2025/07/23/california-police-sharing-flock-license-plate-data)
[plate-data.](https://sfstandard.com/2025/07/23/california-police-sharing-flock-license-plate-data)

1 networks simultaneously—searches of Oakland’s ALPR data, for example, were found to reach
2 hundreds of other networks at once.⁵⁹

3 81. As another example, Flock allowed Alameda County to set up 1:1 agreements with
4 more than 300 out-of-state agencies in the 287(g) program, which deputizes local law enforcement
5 to assist federal agents with immigration enforcement and deportation.⁶⁰ California legislation
6 prohibits police from participating in this program.⁶¹ Yet through these 1:1 agreements, these
7 agencies have searched Alameda County’s data tens of thousands of times, effectively dragging
8 Alameda County into the 287(g) program in violation of California law. Flock continues to allow
9 programs like 287(g) access to its database for California agencies.

10 82. **“Fusion” Agreements:** Flock also permits and facilitates multi-agency “fusion”
11 agreements and data pooling. Regional fusion centers aggregate data, including ALPR
12 information collected by Flock cameras, and share insights from the aggregated data back to the
13 agencies.⁶² Flock allows these fusion centers to maintain their own accounts and multiple agencies
14 may agree to share their ALPR data with these in-state centers. However, Flock does not restrict
15 the centers from sharing this aggregated information—including the data from all California
16 member agencies—with out-of-state and federal agencies. This violates the ALPR Privacy Act.

17 83. Through these permissive 1:1, fusion, and other ALPR sharing practices, Flock
18 grants out-of-state and federal agencies access to ALPR data collected in California.

19
20
21 ⁵⁹ *Id.*

22 ⁶⁰ Eli Wolfe, “*Flock license plate scanner contract postponed by Alameda County Leaders*”,
23 The Oaklandside (Feb. 11, 2026) [hereinafter Wolfe, *Flock Contract Postponed*],
<https://oaklandside.org/2026/02/11/flock-contract-alameda-county-ice-federal/>

24 ⁶¹ California Values Act, Cal. Gov. Code §§ 7284–7284.12.

25 ⁶² Agenda Report, CITY OF RICHMOND POLICE DEPARTMENT (Jan. 21, 2025),
26 <https://pub-richmond.escribemeetings.com/filestream.ashx?DocumentId=56204>; Dave Maass,
27 *San Francisco Police Must End Irresponsible Relationship with the Northern California Fusion*
28 *Center*, ELEC. FRONTIER FOUND. (Sep. 15, 2022),
<https://www.eff.org/deeplinks/2022/09/san-francisco-police-must-end-irresponsible-relationship-northern-california>.

1 84. **“Side-Door” Access:** Audit logs provided by Flock reveal that federal agencies
2 have accessed Flock data from California police departments.⁶³ This often occurs through side-
3 door methods that bypass formal data-sharing agreements that are prohibited by the ALPR Privacy
4 Act. A common example of this side-door method is a police officer with system access running
5 plates on behalf of a federal agent or federal agents being given login credentials for a local
6 agency’s Flock portal.

7 85. This is only possible because Flock designed its product to allow local police to
8 perform lookups in Flock’s ALPR system on behalf of unauthorized external users.⁶⁴ This
9 contravenes guidance from the California AG regarding the permissible uses of ALPR under the
10 ALPR Privacy Act.

11 86. In addition to direct sharing discussed above, Flock’s system also permits ICE and
12 CBP to frequently use California ALPR data in contravention of the ALPR Privacy Act through
13 side-door access.

14 87. In April 2025, the California Highway Patrol conducted a search on behalf of ICE
15 across 845 different California agency databases with which it had sharing agreements.⁶⁵ Given
16 the expansive nature of Flock’s settings for 1:1 agreements, this meant ICE effectively searched
17 not just one, but 845 localities’ databases in a single query.

18 88. The Riverside County Sheriff’s Office, which has 1:1 sharing agreements with
19 more than 300 other California Flock customers, often runs searches for “HSI,” ICE’s Homeland
20 Security Investigations unit, and “CBP.”⁶⁶ It continues to run ALPR searches on behalf of federal
21

22 ⁶³ Chien, *California cops are breaking surveillance laws*, supra note 58; Wolfe, *Flock Contract*
23 *Postponed*, supra note 60.

24 ⁶⁴ Koebler & Cox, *ICE Taps into Nationwide Network*, supra note 42.

25 ⁶⁵ Chien, *California cops are breaking surveillance laws*, supra note 58.

26 ⁶⁶ Khari Johnson and Mohamed Al Elew, *California police are illegally sharing license plate*
27 *data with ICE and Border Patrol*, CAL MATTERS (June 13, 2025) [hereinafter Johnson & Al
28 Elew, *California police illegally sharing*],
<https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/>.

1 agencies despite knowing that its practice of sharing ALPR with federal agencies “violates state
2 law.”⁶⁷ Flock’s 1:1 agreement sharing settings means that any one of these searches exposed
3 hundreds of California agencies—and millions of California drivers—to CBP and ICE
4 surveillance against California law.

5 89. An investigation by the San Francisco Standard found that San Francisco and
6 Oakland police officers also repeatedly violated the ALPR Privacy Act both by running searches
7 on behalf of the FBI and other federal agencies, as well as maintaining 1:1 sharing agreements
8 with other California agencies acting on behalf of federal agencies.⁶⁸

9 90. Likewise, the Los Angeles Police Department, as well as Sheriff’s Departments in
10 Los Angeles, San Diego, and Orange Counties, all have searched license plate readings contained
11 in Flock’s database on behalf of ICE and CBP.⁶⁹

12 91. **Ineffective, Faulty Settings:** Even when Flock’s customers have explicitly
13 requested that Flock prevent California ALPR information from being shared out-of-state or with
14 federal agencies, Flock lacks effective, reliable guardrails. When the City of Los Altos turned off
15 sharing with federal agencies, it found that Flock nevertheless shared its information with a federal
16 agency, despite its settings.⁷⁰ Researchers suspected that, to turn off sharing with non-California
17 agencies, Flock programmed its system to filter and allow sharing only with agencies that contain
18 “CA” in their name. But in this case, its faulty system allowed “Loma Linda Healthcare System
19 CA Veterans Affairs PD [Federal]” (emphasis added) to conduct searches. Of course, “[w]ithout
20 insight into Flock’s security mechanisms, it is impossible to be sure.” Flock perpetrates
21 unauthorized sharing through its faulty design and deficient, misleading end user settings.

22
23
24
25 ⁶⁷ Chien, *California cops are breaking surveillance laws*, *supra* note 58.

26 ⁶⁸ Chien, *SF/Oakland ICE LPRs*, *supra* note 33.

27 ⁶⁹ Johnson & Al Elew, *California police illegally sharing*, *supra* note 66.

28 ⁷⁰ *ALPR Updated Analysis Sept. 2025*, *supra* note 8.

1 92. **Flock Investigative Tools:** The investigative tools that Flock developed and offers
2 to its customers have also flouted agencies’ sharing settings and agreements. Features like “Multi-
3 State Insights” let an investigator in one state see that a vehicle of interest has traveled through
4 other states, including California.⁷¹ Additionally, if a California vehicle is added to a national
5 hotlist, a Flock camera detecting it in California will generate a real-time alert⁷² that is visible to
6 any agency nationwide monitoring that hotlist.

7 93. Flock could design its system to abide by California law such that the ALPR
8 interface it provides to agencies precludes the sharing of California ALPR data with out-of-state
9 and federal agencies everywhere. But it has not. Instead, it has taken performative steps—and
10 only when faced with public pressure. Meanwhile, it continues to unfairly profit from the ALPR
11 data its pervasive surveillance system collects.

12 **IV. Flock Violates California Law by Failing to Implement an Adequate Policy or**
13 **Reasonable Security Procedures to Prevent Unlawful Information Sharing**

14 94. The ALPR Privacy Act requires ALPR operators like Flock to implement and
15 maintain a policy sufficient to ensure their ALPR system will be used exclusively for permissible
16 purposes. Cal. Civ. Code § 1798.90.52(b).

17 95. Flock has an ALPR policy, which was last updated on November 13, 2025.⁷³

18 96. In its Terms and Conditions, Flock defines its authorized or “permitted” purpose
19 as “legitimate public safety and/or business purpose, including but not limited to the awareness,
20
21
22

23
24 ⁷¹ *The Future of Investigations: How Flock’s New AI-Powered Tools Are Transforming*
25 *Vehicular Evidence*, Flock Safety Blog, (Feb. 14, 2025), [https://www.flocksafety.com/blog/the-
26 future-of-investigations-how-flocks-new-ai-powered-tools-are-transforming-vehicular-evidence](https://www.flocksafety.com/blog/the-future-of-investigations-how-flocks-new-ai-powered-tools-are-transforming-vehicular-evidence)
27 [<https://perma.cc/S6NY-CP37>].

28 ⁷² Oakland CA PD Transparency Portal, FLOCK SAFETY
<https://transparency.flocksafety.com/oakland-ca-pd> (last visited Feb. 25, 2026).

⁷³ Flock LPR Policy, *supra* note 22.

1 prevention, and prosecution of crime; investigations; and prevention of commercial harm, *to the*
2 *extent permitted by law.*”⁷⁴

3 97. But by designing its ALPR system to allow out-of-state and federal agency sharing
4 of California ALPR data, Flock violates its own authorized purpose and its own promise to abide
5 by the laws of the states in which it operates.

6 98. The ALPR Privacy Act requires Flock to maintain reasonable security procedures
7 and practices to protect ALPR information from unauthorized access. Cal. Civ. Code
8 § 1798.90.51(a). Flock’s practices, including those listed above, all allow out-of-state and federal
9 law enforcement to access California ALPR data. But for Flock’s policies, design, and
10 infrastructure technology, California law enforcement agencies could not and would not violate
11 the ALPR Privacy Act.

12 99. Flock’s policies regarding whether it needs to do something as plain and self-
13 evident as obeying the ALPR Privacy Act are, at best, incoherent.

14 100. On the one hand, Flock disavows its responsibilities and insists that its
15 customers—not Flock—are the ones who bear the onus for obeying the law. In the section of a
16 blog post titled “Local Autonomy in working with Federal Agencies,” Flock CEO Garrett Langley
17 attempted to disclaim all responsibility for compliance with privacy laws, claiming that working
18 with federal authorities “is a local decision. Not my decision, and not Flock’s decision.”

19 101. But Langley mischaracterizes what California law requires: The burden of
20 compliance rests not just on law enforcement agencies but on Flock and other ALPR operators,
21 too. The ALPR Privacy Act obligates Flock to “*ensure* . . . compliance with applicable privacy
22 laws,” see Cal. Civ. Code. § 1798.90.51(b)(2)(C) (emphasis added)—not just, as Langley put it,
23 “to make compliance easier.”

24
25
26
27
28 ⁷⁴ Terms and Conditions, FLOCK SAFETY, <https://www.flocksafety.com/legal/terms-and-conditions> [<https://perma.cc/H6L4-VK3V>] (last updated Feb. 16, 2026) (emphasis added).

1 102. Flock says as much in another blog post, stating that at the company, “compliance
2 is not an afterthought. It is foundational to how our products are built, deployed, and supported.”⁷⁵

3 103. In fact, on August 25, 2025, Langley wrote that Flock’s new Chief Legal Officer,
4 Dan Haley, would lead the company’s new effort “to ensure users are able to determine, in
5 compliance with local laws, regulations, and community norms, whether and when to share their
6 data.”⁷⁶

7 104. This statement followed closely after Flock updated its ALPR system and placed
8 “restrictions directly within the platform” to prevent California ALPR data from being shared with
9 out-of-state or federal agencies pursuant to the ALPR Privacy Act.⁷⁷

10 105. Flock’s recent actions illustrate two important points regarding its obligations and
11 liability under California law: First, its August 25 statement is an admission that, at the time the
12 blog post was written, users could not ensure their compliance with local laws, and Flock was
13 therefore not in compliance with the ALPR Privacy Act. Second, Flock’s recent system updates
14 make clear that it was *always* feasible for Flock to place reasonable limitations on use of its
15 database in order to comply with California law, including the ALPR Privacy Act. It simply *chose*
16 not to.

17 106. Flock still disclaims its obligation to ensure compliance with the ALPR Privacy
18 Act, maintaining that its “[c]ustomers choose whether to share LPR data with other customers in
19 accordance with their laws and policies.”⁷⁸ But it fails to acknowledge that its customers’ choices
20
21

22
23 ⁷⁵ Flock Aligns License Plate Reader Technology with State-Specific Legal Frameworks,
24 FLOCK SAFETY (Feb. 16, 2026), <https://www.flocksafety.com/blog/flock-aligns-license-plate-reader-technology-with-state-specific-legal-frameworks> [<https://perma.cc/6YAL-D7ZQ>].

25 ⁷⁶ Langley, *Ensuring Local Compliance*, *supra* note 44.

26 ⁷⁷ Does Flock Share Data With ICE?, FLOCK SAFETY (Jan. 6, 2026),
27 <https://www.flocksafety.com/blog/does-flock-share-data-with-ice> [<https://perma.cc/AG84-9AQV>].

28 ⁷⁸ Flock LPR Policy, *supra* note 22.

1 are inextricable from its products and its own compliance with the law. Flock can and must build
2 its ALPR system to abide by California law.

3 107. California law enforcement agencies’ continued routine violations of the ALPR
4 Privacy Act, even with interpretative guidance from and enforcement actions by the California
5 AG, were foreseeable and preventable. Law enforcement agencies (in California and elsewhere)
6 have flouted other bans (under California law) relating to, for example, the use of facial
7 recognition technology and the use of drones.

8 108. Had Flock implemented required and reasonable measures to prevent out-of-state
9 and federal sharing of California ALPR data, it would have complied with the ALPR Privacy Act
10 itself as well as prevented California law enforcement agencies from violating the ALPR Privacy
11 Act. This is well within Flock’s capabilities.

12 109. Allowing this kind of information-sharing is not merely a statutory violation; it is
13 a legal and ethical concern.

14 110. Federal and out-of-state law enforcement agencies have different legal and ethical
15 standards and rules than California law enforcement agencies. They also have different policy
16 priorities. California residents can shape local and state law enforcement policies, including how
17 ALPR data is used, as constituents of their elected officials; the same cannot be said for out-of-
18 state jurisdictions.

19 **V. Flock’s Security Measures Fall Far Below Reasonable Procedures and Practices**

20 111. Flock is in further violation of the ALPR Privacy Act by failing to implement and
21 maintain reasonable security procedures and practices.

22 112. Flock’s lax approach to data security has further enabled illegal information-
23 sharing in violation of the ALPR Privacy Act and intrusion of privacy standards.

24 113. For example, Flock does not require multifactor authentication (“MFA”) when law
25 enforcement end-users access its ALPR database. In this context, MFA— “an everyday, familiar
26 technology”—would help prevent unauthorized sharing of credentials with federal agencies and
27 out-of-state law enforcement agencies. Only after negative press coverage of a federal agency’s
28

1 use of a police officer’s unsecured account did Flock make MFA its default setting—and even
2 then, Flock still failed to require MFA.

3 114. Predictably, failing to mandate MFA has led to “the leak of numerous police logins
4 to Flock systems”; Flock police logins have even been found “for sale by Russian hackers in a
5 dark web forum.

6 115. A security analyst known as Jon “GainSec” Gains published a formal white paper
7 exposing “dozens of security vulnerabilities”—many of which the white paper describes
8 as “critical” in Flock’s cameras, including its ALPR readers.⁷⁹

9 116. Recent media reports have also revealed major vulnerabilities in how video
10 feeds from some models of Flock cameras were configured vulnerabilities that made at least
11 dozens of video feeds from certain types of Flock cameras available on the internet for anyone,
12 without any password or login information required. These models of Flock cameras, known as
13 “Condor” and specifically designed to track people, operate in conjunction with Flock’s ALPR
14 cameras to provide information to law enforcement.⁸⁰

15 117. A recent article provides “a sampling of some of Flock’s most preposterous
16 hardware and software issues” outlined in the GainSec white paper, noting that “[t]he porous
17 security system of these camera systems approaches the comical”.⁸¹

21 ⁷⁹ Jon Gains, *Examining the security posture of an Anti-Crime Ecosystem*, GAINSEC, (Nov. 11,
22 2025) [hereinafter Gains, *Examining the security posture of an Anti-Crime Ecosystem*],
accessible at <https://gainsec.com/2025/11/05/formalizing-my-flock-safety-security-research/>.

23 ⁸⁰ Jason Koebler, *Flock Exposed Its AI-Powered Cameras to the Internet. We Tracked*
24 *Ourselves.*, 404 MEDIA (Dec. 22, 2025), [https://www.404media.co/flock-exposed-its-ai-
powered-cameras-to-the-internet-we-tracked-ourselves](https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves).

25 ⁸¹ Tyler Walicek, *A Vast Camera System Now Feeds Information to Police on Drivers Across*
26 *the US*, TRUTHOUT (Nov. 26, 2025) [hereinafter Tyler Walicek, *Vast Camera System Feeds*
27 *Information*], [https://truthout.org/articles/a-vast-camera-system-now-feeds-information-to-
police-on-drivers-across-the-us](https://truthout.org/articles/a-vast-camera-system-now-feeds-information-to-police-on-drivers-across-the-us).

- 1 i. **Physical vulnerabilities:** “Pressing an easily accessible button on the back of
2 Flock cameras (which, you may recall, are mounted in public across the country)
3 a handful of times in an extremely simple sequence will open a wireless access
4 point, which is easily hijacked to grant root access to the camera’s systems; once
5 you have ‘root,’ you can connect to the device, access its video data, and install
6 whatever you’d like. Flock cameras’ exposed USB ports offer another avenue to
7 gain control of the device to scrape data, insert fake camera feeds or anything else,
8 obtain police information, and generally perform an endless variety of
9 manipulations.”
- 10 ii. **Unsupported operating system:** “Flock cameras still run on Android Things
11 8.1— an outdated mobile system that, crucially, has been discontinued and is no
12 longer supported by Google with security patches. Unsupported operating systems
13 are essentially undefended, riddled with known exploits.”
- 14 iii. **Unprotected testing data:** “Flock . . . left its internal testing data accessible
15 online: a trove that included police names and phone numbers, patrol areas, suspect
16 hotlists, full license plates and even geographic information systems (GIS) data
17 showing the live location of patrol cars.”

18 118. In response to the GainSec white paper, Flock released a statement attempting to
19 reassure customers, reading: “Overall, none of the vulnerabilities detailed in the report have an
20 impact on our customers’ ability to carry out their public safety objectives. Exploitation of these
21 vulnerabilities would not only require physical access to a device but also require intimate
22 knowledge of internal device hardware. No customer action is required in response to this
23 disclosure.”⁸²

24 119. This statement is misleading at best. As noted in the article, “[t]he failings are
25 farcical for a purported ‘security’ company.” As above, to the extent these exploits require
26

27 ⁸² *Response to Compiled Security Research on Flock Safety Devices*, FLOCK SAFETY: BLOG
28 (Nov. 6, 2025), <https://www.flocksafety.com/blog/response-to-compiled-security-research-on-flock-safety-devices> [<https://perma.cc/L3K6-6C79>].

1 physical access to Flock cameras, that is easy to obtain because most are mounted in public areas.
2 And in general, Flock’s statement is patently misleading: The “basic vulnerabilities” in its systems
3 “would be all too easy for even less experienced hackers to exploit. Any competent state or non-
4 state actors, infiltrators of criminal or foreign intelligence origin, could have a field day.”⁸³

5 120. In reality, a popular YouTuber, Benn Jordan, posted a detailed video showing how
6 a lay person could easily hack a Flock Safety Camera in under 30 seconds.⁸⁴ In the video he goes
7 over six of the vulnerabilities detailed in the GainSec White Paper.

8 121. Flock claims to be setting the standard for public safety technology and
9 cybersecurity,⁸⁵ yet continues to be in blatant violation of the ALPR Privacy Act and intrusion of
10 privacy standards.

11 **VI. Flock’s Facilitation of California Law Enforcement Agencies’ Unlawful**
12 **Information Sharing Is Highly Offensive**

13 **A. Flock’s Network Amplifies Discriminatory Policing Practices**

14 122. The ALPR Privacy Act is necessary because ALPR systems are not neutral public-
15 safety tools. On paper they are used to solve crime and make people feel safer, but in practice they
16 frequently aid discriminatory policing, and disproportionately target low-income neighborhoods
17 and communities. These tools embed and amplify longstanding policing bias by converting them
18 into scalable surveillance.

19 123. As noted by several privacy advocates and the ACLU, “police often
20 disproportionately deploy license plate readers in communities experiencing poverty and
21 historically overpoliced communities of color, regardless of crime rates.”⁸⁶

22 _____
23 ⁸³ Tyler Walicek, *Vast Camera System Feeds Information*, *supra* note 81.

24 ⁸⁴ Benn Jordan, *We hacked Flock Safety Cameras in under 30 Seconds.*, Youtube (Nov. 16,
25 2025), <https://www.youtube.com/watch?v=uB0gr7Fh6lY>.

26 ⁸⁵ Chris Castaldo, *Holding Ourselves to the Highest Standard to Protect Community Data*,
27 FLOCK SAFETY: BLOG (Feb. 9, 2026), <https://www.flocksafety.com/blog/flock-security-testing-bishop-fox-privacy> [<https://perma.cc/Y8EX-368U>].

28 ⁸⁶ EFF–ACLU Joint Letter, *supra* note 38, at 2 (citing Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland’s Raw ALPR Data*, ELEC. FRONTIER FOUND. (Jan. 21, 2015),

1 124. Flock’s nationwide network expands the reach and impact of these practices. While
2 the system prompts officers to provide a reason for each search, audit logs reveal that these tools
3 are used to enact prejudice on an unprecedented geographic scale. For instance, the Electronic
4 Frontier Foundation has documented that more than 80 law enforcement agencies used pejorative
5 terms for Romani people in Flock search logs.

6 125. Specific examples include the Sacramento Police Department, which in May 2025
7 ran at least six searches using a racial slur against Romani people, scanning across 468 networks
8 and 12,885 cameras. Similarly, the Irvine Police Department ran eight searches using the term
9 “roma” in early 2025, querying data from 29,364 devices.⁸⁷

10 126. These searches represent a trend that creates tangibly discriminatory outcomes. For
11 example, data from Oak Park, Illinois, shows that 84% of drivers stopped in Flock-related traffic
12 incidents are Black—despite Black people making up only 19% of Oak Park residents.⁸⁸

13 127. As above, the ALPR Privacy Act prohibits all unauthorized ALPR data sharing
14 with federal agencies and out-of-state law enforcement agencies, not simply data sharing
15 conducted for an illicit, discriminatory purpose. The use and sharing of ALPR data for
16 discriminatory purposes heightens the highly offensive nature of the widespread collection,
17 storage, use, and sharing of ALPR data.

18
19
20 <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>; Barton Gellman
21 & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21,
22 2017), [https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-](https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf)
23 [surveillance.pdf](https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf)); *see also, e.g.*, Kaveh Waddell, *How License-Plate Readers Have Helped*
24 *Police and Lenders Target the Poor*, THE ATLANTIC (Apr. 22, 2016),
25 [https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-](https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436)
26 [helped-police-and-lenders-target-the-poor/479436](https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436) (summarizing data indicating that Oakland
27 Police Department deployed ALPRs disproportionately, often in low-income areas and in
28 neighborhoods with high concentrations of African-American and Latino residents”).

87 Rindala Alajaji & Dave Maass, *License Plate Surveillance Logs Reveal Racist Policing Against Romani People*, ELEC. FRONTIER FOUND. (Nov. 3, 2025), <https://www.eff.org/deeplinks/2025/11/license-plate-surveillance-logs-reveal-racist-policing-against-romani-people>.

88 84% of drivers stopped by Oak Park police in Flock traffic stops were Black, *supra* note 31.

1 **B. Cross-Jurisdictional Data Sharing Threatens Access to Abortion and Gender-**
2 **Affirming Care in California**

3 128. The weaponization of ALPR data extends beyond racial profiling, directly
4 threatening individuals seeking constitutionally protected healthcare in California. Location
5 information from California-based Flock cameras can be used by agencies in restrictive states to
6 monitor clinics, track vehicles, and survey the movements of patients and providers.⁸⁹

7 129. Indeed, the Electronic Frontier Foundation has reported that at least one Texas law
8 enforcement officer searched Flock’s national database, which at the time would have included
9 results in California, for an investigation into a woman who had self-administered an abortion.⁹⁰

10 130. Given that multiple states have moved to criminalize obtaining or facilitating out-
11 of-state abortions, sharing Flock data with their law enforcement agencies threatens anyone

14 ⁸⁹ See, e.g., Caroline Kitchener & Devlin Barrett, *Antiabortion lawmakers want to block patients*
15 *from crossing state lines*, WASH. POST (June 29, 2022, at 18:17 ET),
16 <https://www.washingtonpost.com/politics/2022/06/29/abortion-state-lines> (last updated June 30,
17 2022, at 8:30 ET); *Idaho governor signs ‘abortion trafficking’ bill into law*, AP NEWS (Apr. 6,
18 2023), [https://apnews.com/article/idaho-abortion-minors-criminalization-](https://apnews.com/article/idaho-abortion-minors-criminalization-b8fb4b6feb9b520d63f75432a1219588)
19 [b8fb4b6feb9b520d63f75432a1219588](https://apnews.com/article/idaho-abortion-minors-criminalization-b8fb4b6feb9b520d63f75432a1219588); Josh Moon, *Alabama AG: state may prosecute those who*
20 *assist in out-of-state abortions*, ALA. POL. REP. (Sep. 15, 2022, at 6:30 CT),
21 [https://www.alreporter.com/2022/09/15/alabama-ag-state-may-prosecute-those-who-assist-in-out-](https://www.alreporter.com/2022/09/15/alabama-ag-state-may-prosecute-those-who-assist-in-out-of-state-abortions)
22 [of-state-abortions](https://www.alreporter.com/2022/09/15/alabama-ag-state-may-prosecute-those-who-assist-in-out-of-state-abortions).

23 ⁹⁰ Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras*
24 *Nationwide for a Woman Who Got an Abortion*, 404 MEDIA (May 29, 2025),
25 [https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-](https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion)
26 [woman-who-got-an-abortion](https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion). Flock and the Johnson County, Texas, Sheriff initially
27 insisted that the search was not “related to enforcing Texas’s abortion ban” and that “media
28 accounts” were “‘false,’ ‘misleading,’ and ‘clickbait.’” These claims were proven false. See
29 Dave Maass & Rindala Alajaji, *Flock Safety and Texas Sheriff Claimed License Plate*
30 *Search Was for a Missing Person. It Was an Abortion Investigation.*, ELEC.
31 FRONTIER FOUND. (Oct. 7, 2025), [https://www.eff.org/deeplinks/2025/10/flock-safety-and-](https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it)
32 [texas-sheriff-claimed-license-plate-search-was-missing-person-it](https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it) (“New documents and
33 court records obtained by EFF show that Texas deputies queried Flock Safety’s
34 surveillance data in an abortion investigation. The new information shows that deputies
35 had initiated a ‘death investigation’ of a ‘non-viable fetus,’ logged evidence of a
36 woman’s self-managed abortion, and consulted prosecutors about possibly charging her.”);
37 Jason Koebler & Joseph Cox, *Police Said They Surveilled Woman Who Had an Abortion for*
38 *Her ‘Safety.’ Court Records Show They Considered Charging Her With a Crime*, 404 MEDIA
39 (Oct. 7, 2025), [https://www.404media.co/police-said-they-surveilled-woman-who-had-an-](https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/)
40 [abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/](https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/).

1 involved in abortion care within California.⁹¹ Parallel efforts to criminalize out-of-state travel for
2 gender-affirming care expose another vulnerable population to the same risks. The use of ALPR
3 data to enable such extraterritorial prosecutions profoundly intensifies the highly offensive nature
4 of the unauthorized data sharing Flock facilitates.

5 **C. Flock’s ALPR System Threatens Protected First Amendment Activity**

6 131. “Aggregated location data allows law enforcement and private companies to create
7 detailed profiles of a person's daily life. When considered in bulk, ALPR data can form an intimate
8 picture of a driver’s activities and even deter First Amendment-protected activities. This kind of
9 targeted tracking threatens to erode fundamental freedoms of speech.”⁹²

10 132. Law enforcement have used Flock ALPR data to track individuals exercising their
11 First Amendment rights, including engaging in peaceful protest. Through an analysis of Flock’s
12 nationwide searches, Electronic Frontier Foundation found that “more than 50 federal, state, and
13 local agencies ran hundreds of searches through Flock’s national network of surveillance data in
14 connection with protest activity.”⁹³

15 133. Recent reports indicate law enforcement agencies logged hundreds of searches
16 related to political demonstrations over the ten months of logs analyzed, including No Kings
17 protests, 50501 protests, Hands Off protests, and protests against deportation raids and in support
18 of pro-Palestinian activist Mahmoud Khalil.⁹⁴

20 ⁹¹ Dave Maass, *Automated License Plate Readers Threaten Abortion Access. Here's How*
21 *Policymakers Can Mitigate the Risk*, ELEC. FRONTIER FOUND. (Sept. 28, 2022),
22 [https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-
access-heres-how-policymakers](https://www.eff.org/deeplinks/2022/09/automated-license-plate-readers-threaten-abortion-access-heres-how-policymakers).

23 ⁹² SB274 Analysis, CALIFORNIA STATE ASSEMBLY COMMITTEE ON PRIVACY AND
24 CONSUMER PROTECTION, [https://apcp.assembly.ca.gov/system/files/2025-07/sb-274-
cervantes-apcp-analysis.pdf](https://apcp.assembly.ca.gov/system/files/2025-07/sb-274-cervantes-apcp-analysis.pdf), at 4 (last visited Feb. 22, 2026).

25 ⁹³ Dave Maass and Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to*
26 *Surveil Protesters and Activists*, ELEC. FRONTIER FOUND. (Nov. 20, 2025),
27 [https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-
protesters-and-activists](https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists).

28 ⁹⁴ *Id.*

1 134. Audit logs compiled by the website “Have I Been Flocked” show searches on the
2 national network which appear to relate to protected activity, such as a search in North Carolina
3 with the stated reason as “Mosque,” a search in Iowa for a “protester” and a search from Akron,
4 Ohio for “activist recording.”⁹⁵

5 135. Because of Flock’s vast network of ALPR data sharing, many of these searches
6 had nationwide reach. For example, a Texas police department ran two vehicle searches listing
7 “KINGS DAY PROTEST” as the reason, which together reached 1,774 networks.⁹⁶

8 136. As above, the ALPR Privacy Act prohibits all unauthorized ALPR data sharing
9 with federal agencies and out-of-state law enforcement agencies, not just data sharing which
10 appears to be investigating protected First Amendment activity. The use and sharing of ALPR
11 data for tracking those engaging in protected First Amendment activity heightens the highly
12 offensive nature of the widespread collection, storage, use, and sharing of ALPR data.

PLAINTIFFS’ EXPERIENCES

I. Plaintiff Javorsky’s Experience

13
14
15 137. Plaintiff Daniel Javorsky is a resident of San Francisco, California.

16 138. Plaintiff Javorsky currently owns and drives a white Audi A5 convertible.

17 139. Plaintiff Javorsky regularly drives in San Francisco for day-to-day activities such
18 as running errands, going to the gym, and visiting friends, including along routes with Flock
19 cameras installed. Plaintiff Javorsky also regularly drives to Oakland, California, to visit friends,
20 including along routes where Flock cameras are installed.

21 140. Plaintiff Javorsky has regularly driven along these routes from 2022 until present.

22 141. Because Flock cameras scan and collect the license plate, vehicle, and location
23 information of every car passing by, Plaintiff Javorsky’s license plate, vehicle, and location data
24 has been and continues to be collected and stored by Flock.

25
26 _____
27 ⁹⁵ *First Amendment Report, Have I Been Flocked?*, https://haveibeenflocked.com/first-amendment-records?sort=date_desc (last visited Feb. 19, 2026).

28 ⁹⁶ *Id.*

1 142. The Flock cameras in San Francisco and Oakland are situated such that Plaintiff
2 Javorsky cannot drive for his regular activities without passing a camera. If Plaintiff Javorsky
3 could avoid routes where Flock cameras are installed, he would, but he cannot.

4 143. The location data collected by Flock from its sprawling network of cameras in San
5 Francisco and Oakland also allows those with access to Flock's systems to ascertain Plaintiff
6 Javorsky's movement data.

7 144. The San Francisco and Oakland ALPR data collected and stored by Flock has been
8 shared with and is accessible by out-of-state and/or federal law enforcement agencies.⁹⁷

9 145. Given the pervasive nature of Flock's broad data sharing agreements, Plaintiff
10 Javorsky's vehicle and location information data has been accessed by out-of-state and/or federal
11 law enforcement agencies.

12 146. Plaintiff Javorsky is concerned about the continuous collection, aggregation, and
13 sharing of his vehicle and location data, including with out-of-state and federal law enforcement
14 agencies. Plaintiff Javorsky believes that continuous collection, aggregation, and sharing violates
15 his privacy.

16 147. Plaintiff Javorsky finds the unauthorized sharing of their vehicle, location, and
17 movement data with out-of-state and federal law enforcement agencies highly offensive.

18 **II. Plaintiff Mayor's Experience**

19 148. Plaintiff Anthony Mayor lives in Marin County, specifically, San Rafael,
20 California.

21 149. Plaintiff Mayor currently owns and drives a red Kia Niro.

22 150. Plaintiff Mayor regularly drives in San Francisco County, Marin County, and Napa
23 County, including along routes where Flock cameras are installed.

24 _____
25 ⁹⁷ Chien, Tomo, *Oakland police illegally shared license plate data: lawsuit*, S.F. STANDARD
26 (Nov. 18, 2025), [https://sfstandard.com/2025/11/18/oakland-police-opd-lawsuit-flock-](https://sfstandard.com/2025/11/18/oakland-police-opd-lawsuit-flock-surveillance/)
27 *surveillance/*; Chien, *Georgia, Texas cops illegally search*, supra note 7; *Why Are The Alameda*
28 *County Sheriff And SFPD Sharing So Much Data With 287(g) agencies?* SECURE JUSTICE
(Dec. 7, 2025), [https://secure-justice.org/blog/why-are-the-alameda-county-sheriff-and-sfpd-](https://secure-justice.org/blog/why-are-the-alameda-county-sheriff-and-sfpd-sharing-so-much-data-with-287g-agencies)
sharing-so-much-data-with-287g-agencies.

1 151. Plaintiff Mayor has regularly driven along these routes since May 2024.

2 152. From 2022 to May 2024, Plaintiff Mayor regularly drove in San Mateo County and
3 San Francisco County, also passing in front of Flock cameras.

4 153. Because Flock cameras scan and collect the license plate, vehicle, and location
5 information of every car passing by, Plaintiff Mayor's license plate, vehicle, and location data has
6 been and continues to be collected and stored by Flock.

7 154. The Flock cameras in Marin County, San Francisco County, and Napa County are
8 situated such that Plaintiff Mayor cannot drive to and from work without passing a camera.
9 Specifically, Plaintiff Mayor passes by 12 cameras on his daily commute to his job in San
10 Francisco as a music teacher.

11 155. Plaintiff Mayor passes by dozens more Flock cameras driving to and from Napa
12 County and San Francisco's Castro District for a part-time job and his weekly commitments as
13 part of the San Francisco Gay Men's Chorus. This does not include any of the cameras he would
14 pass by while running errands, like grocery shopping, or adjusting for heavy traffic days, which
15 are common throughout the Bay Area. If Plaintiff Mayor could avoid routes where Flock cameras
16 are installed, he would, but he cannot.

17 156. The location data collected by Flock from its sprawling network of cameras in San
18 Francisco, Marin, and Napa counties also allows those with access to Flock's systems to ascertain
19 Plaintiff Mayor's movement data.

20 157. The San Francisco ALPR data collected and stored by Flock has been shared with
21 and is accessible by out-of-state and/or federal law enforcement agencies.⁹⁸

22 158. Given the pervasive nature of Flock's broad data sharing agreements, Plaintiff
23 Mayor's vehicle and location information data has been accessed by out-of-state and/or federal
24 law enforcement agencies.

25 159. Plaintiff Mayor is concerned about the continuous collection, aggregation, and
26 sharing of his vehicle and location data, including with out-of-state and federal law enforcement
27

28 ⁹⁸ Chien, *Georgia, Texas cops illegally search*, supra note 7.

1 agencies. Plaintiff Mayor believes that continuous collection, aggregation, and sharing violates
2 his privacy.

3 160. Plaintiff Mayor finds the unauthorized sharing of their vehicle, location, and
4 movement data with out-of-state and federal law enforcement agencies highly offensive.

5 **III. Plaintiffs’ Data from Flock Cameras Has Economic Value**

6 161. Every day, commercial entities purchase data about individuals—including their
7 location history—from data brokers⁹⁹ and other sources to run advertisements and target their
8 services.¹⁰⁰

9 162. For the past decade, data brokers have sought out and combined data from private
10 and public sources. While individual data sources “may provide only a few elements about a
11 person’s activities, data brokers combine these elements to form a detailed, composite view of the
12 consumer’s life.”¹⁰¹

13 163. Fusing Flock’s ALPR data, including historical data about an individual’s
14 movements, with other data taken from ad tech and other companies enhances the economic value
15 of any of the millions of existing datasets on California drivers.

16 164. Moreover, it is easy to see how information regarding someone’s daily commute
17 or vehicle alone could be valuable to advertisers. For example, where a vehicle travels reveals an
18 astonishing amount about the purchasing decisions, lifestyles, and interests of its occupants.

21 ⁹⁹ California law defines a “data broker” as “a business that knowingly collects and sells to third
22 parties the personal information of a consumer with whom the business does not have a direct
23 relationship,” subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

24 ¹⁰⁰ Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American*
25 *Civil Rights, National Security, and Democracy*, at 2 (2021), Duke Sanford Cyber Policy
26 Program, [https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-](https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/)
27 [individuals/](https://techpolicy.sanford.duke.edu/report-data-brokers-and-sensitive-data-on-u-s-individuals/) (last visited Feb. 26, 2026).

28 ¹⁰¹ Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records*
29 *for Detailed Profiles of Adults and Children*, COSN ’15: PROCEEDINGS OF THE 2015 ACM
30 ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015),
31 <https://dl.acm.org/doi/10.1145/2817946.2817957> (last visited Feb. 26, 2026).

1 165. Indeed, Flock itself developed its “Nova” product to fuse—and thus enhance the
2 value of—both third-party and Flock datasets.¹⁰²

3 166. The data Flock collects thus has economic value to its owners, including to
4 Plaintiff.

5 167. Both Plaintiffs Javorsky and Mayor find the unauthorized sharing of his vehicle,
6 location, and movement data, and the fusing of such data with sensitive information from third-
7 party sources to generate even more detailed insights about Plaintiffs highly offensive.

8 **CLASS ACTION ALLEGATIONS**

9 168. Pursuant to California Code of Civil Procedure § 382, Plaintiffs seeks certification
10 of the following classes (hereinafter referred to as “the Class”):

- 11 a. All individuals whose license plate data was collected in California by the
12 Flock ALPR system and was accessible by, and thus disclosed to, federal law
13 enforcement agencies, out-of-state agencies on or after February 26, 2022 (the
14 “Class Period”).
- 15 b. All individuals whose license plate data was collected in California by the
16 Flock ALPR system and was searched for by federal law enforcement agencies
17 and/or out-of-state agencies during the Class Period.

18 169. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries,
19 any entity in which Defendant has a controlling interest, any Defendant officer or director; any
20 Judge who adjudicates this case, including their staff and immediate family; persons who properly
21 execute and file a timely request for exclusion from the Class; persons whose claims in this matter
22 have been finally adjudicated on the merits or otherwise released; Plaintiffs’ counsel and
23 Defendant’s counsel; and the legal representatives, successors, and assigns of any such excluded
24 person.

25 170. Plaintiffs reserve the right to modify or amend the definition of the proposed class
26 before the Court determines whether certification is appropriate.

27 _____
28 ¹⁰² Joseph Cox, *License Plate Reader Company Flock Is Building a Massive People Lookup
Tool, Leak Shows*, *supra* note 40.

1 171. Ascertainability. Members of the Class (“Class Members”) are ascertainable
2 because the definition provides a definition which allows putative class members to identify
3 themselves as having a right to recover, and provides an objective, concrete basis for which to
4 determine who will be bound by a judgment.

5 172. Numerosity. The Class Members are so numerous that joinder of all members is
6 impracticable. There are millions of drivers throughout California whose license plates were
7 photographed, time stamped, and geolocation data collected by Flock and Flock’s policies have
8 permitted unauthorized sharing of this data with federal agencies, out-of-state agencies, and the
9 general public. Because of the sophisticated nature and detailed, ongoing collection, Flock will be
10 able to identify all these individuals through their amassed records.

11 173. Predominance. Questions of law and fact common to the Class exist and
12 predominate over any questions affecting only individual Class Members. These include:

- 13 (a) Whether Flock implemented and maintained a policy that complied with
14 California’s ALPR Privacy Act;
- 15 (b) Whether Flock complies with the Notice, Privacy, Security, Audit, and Proper-Use
16 Requirements set forth in California’s ALPR Privacy Act;
- 17 (c) Whether Flock gathered location data and license plan scans of Class Members;
- 18 (d) Whether Flock’s policies permit unauthorized access of Flock ALPR data owned
19 by California law enforcement agencies by federal agencies or out-of-state law
20 enforcement agencies;
- 21 (e) Whether Class Members’ data was shared with out-of-state or federal agencies;
- 22 (f) Whether Flock knew or should have known that its infrastructure and inadequate
23 policy facilitated unauthorized sharing of Class Members’ ALPR data with federal
24 and out-of-state agencies;
- 25 (g) Whether the unauthorized sharing of Class Members’ ALPR data has harmed the
26 Class;
- 27 (h) Whether Flock’s violations of California law have harmed the class; and
- 28 (i) Whether Flock is subject to punitive damages under California’s ALPR Privacy

1 Act and California common law.

2 174. Typicality. Plaintiffs' claims are typical of those of other Class Members because
3 all had their ALPR data compromised as a result of Flock's lax policy and infrastructure.

4 175. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests
5 of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be
6 antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic
7 or adverse to the Members of the Class and the infringement of the rights, and the damages
8 Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel
9 experienced in complex class action litigation, and Plaintiffs intend to prosecute this action
10 vigorously.

11 176. Superiority. Class litigation is an appropriate method for fair and efficient
12 adjudication of the claims involved. Class action treatment is superior to all other available
13 methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a
14 large number of Class Members to prosecute their common claims in a single forum
15 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
16 expense that hundreds of individual actions would require. Class action treatment will permit the
17 adjudication of relatively modest claims by certain Class Members, who could not individually
18 afford to litigate a complex claim against a large corporation like Defendant. Further, even for
19 those Class Members who could afford to litigate such a claim, it would still be economically
20 impractical and impose a burden on the courts.

21 177. Policies Generally Applicable to the Class. This class action is also appropriate for
22 certification because Defendant has acted or refused to act on grounds generally applicable to the
23 Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
24 of conduct toward the Class Members and making final injunctive relief appropriate with respect
25 to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members
26 uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect
27 to the Class as a whole, not on facts or law applicable only to Plaintiff.

28

1 178. Unless a class-wide injunction is issued, Defendant will continue disclosing Class
2 Member ALPR data, and Flock may continue to act unlawfully as set forth in this Complaint.

3 179. Further, Defendant has acted or refused to act on grounds generally applicable to
4 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the
5 Class Members as a whole is appropriate.

6 180. Issue Certification, Likewise, particular issues are appropriate for certification
7 because such claims present only particular, common issues, the resolution of which would
8 advance the disposition of this matter and the parties' interests therein.

9 Plaintiffs reserve the right to revise the foregoing "Class Allegations" and "Class Definition"
10 based on facts learned through additional investigation and/or the discovery process.

11 **COUNT I**
12 **Violation of California's ALPR Privacy Act**
13 **Cal. Civ. Code §§1798.90.5 *et seq.***
14 **(On behalf of Plaintiffs, the Class, and the Subclass)**

15 181. Plaintiffs incorporate all prior allegations as if fully set forth herein and brings this
16 Count individually and on behalf of the proposed Class.

17 182. Flock operates a nationwide ALPR system that captures photographs of license
18 plates, detailed physical characteristics of vehicles, together with the location, time, and date of
19 Plaintiffs' and the Class's travels, which can be searched via web interface or application.

20 183. Flock is both an ALPR operator under Cal. Civ. Code § 1798.90.5(c) and an ALPR
21 end-user under the ALPR Privacy Act because it operates an ALPR system and accesses or uses
22 an ALPR system to train its AI algorithms and build new product features.

23 184. As an ALPR operator and end-user in California, Flock is legally required to (1)
24 maintain reasonable security procedures to protect ALPR information; (2) implement and enforce
25 a usage and privacy policy ensuring collection and sharing respects individual privacy and civil
26 liberties; and (3) monitor its system to ensure security and compliance with law. Flock is
27 prohibited from allowing ALPR information to be used for any purpose not authorized by its own
28 policy and compliant with the ALPR Privacy Act.

1 185. The ALPR Privacy Act explicitly prohibits the sale, sharing, or transfer of ALPR
2 information except to another California “public agency.” Despite this, Flock designed and
3 maintained a system with inadequate security and privacy controls that facilitated the unlawful
4 sharing of California residents’ ALPR data.

5 186. Flock failed to implement basic technological safeguards that would have
6 prevented California law enforcement data from being accessed by federal agencies (including
7 ICE and CBP) and out-of-state law enforcement agencies.

8 187. Among other security failures, Flock did not require MFA for access to or searches
9 of its ALPR database, allowing California ALPR data to be shared with out-of-state and federal
10 agencies. Flock’s unreasonable security practices were demonstrated by a researcher’s recent
11 exposure of fifty-one (51) distinct vulnerabilities in its hardware and software.

12 188. Flock knew or should have known that its failure to implement and maintain
13 adequate privacy and security measures would permit unauthorized information sharing with
14 federal agencies and out-of-state law enforcement agencies in violation of the ALPR Privacy Act.

15 189. Flock did not introduce measures that would have prevented California law
16 enforcement agencies’ ALPR data from being shared with federal agencies or out-of-state
17 agencies, such as blocking sharing of California ALPR data with federal agencies and out-of-state
18 law enforcement agencies or giving California law enforcement agencies the option to limit
19 sharing of their ALPR data to only “public agencies” as defined by the ALPR Privacy Act.

20 190. Flock deliberately collected Plaintiffs’ and the Class’s ALPR information and
21 disclosed that information to its out-of-state and federal law enforcement customers, allowing
22 them to identify physical characteristics of, movement patterns of, and locations visited by
23 Plaintiffs’ and Class Members’ vehicles, as well as potentially other identifying information.

24 191. Flock’s failure to implement these required safeguards constitutes a willful and
25 reckless disregard for California law and resident privacy. Its conduct is highly offensive to a
26 reasonable person, amounts to willful and reckless disregard of the law, and has directly harmed
27 Plaintiffs and the Class by exposing their sensitive personal information, such as location and
28 movement information, to unauthorized entities.

1 192. Flock is liable for actual or statutory damages of not less than \$2,500 per violation,
2 as well as any punitive damages.

3 **COUNT II**
4 **Negligence**

5 **(On behalf of Plaintiffs, the Class, and the Subclass)**

6 193. Plaintiffs incorporate all prior allegations as if fully set forth herein and brings this
7 Count individually and on behalf of the proposed Class.

8 194. Flock owed Plaintiffs and Class members a duty to prevent unauthorized sharing
9 and to maintain reasonable and adequate information and data security practices.

10 195. Flock's duty is demonstrated by California's ALPR Privacy Act.

11 196. Flock breached that duty by violating the ALPR Privacy Act—allowing federal and
12 out-of-state agencies to access California ALPR data in direct violation of the ALPR Privacy Act
13 and against the repeated warnings from the California Attorney General's office.

14 197. Flock further breached its duty by failing to implement reasonable security
15 practices.

16 198. Plaintiffs and the Class have been injured by Flock's conduct because their ALPR
17 information has been improperly shared with federal and out-of-state law enforcement agencies
18 as well as, potentially, other unauthorized third parties. This has harmed Plaintiffs and the Class
19 in ways enumerated above. Flock's facilitation of unlawful ALPR data sharing with federal
20 agencies and out-of-state law enforcement agencies is highly offensive to a reasonable person.

21 199. As a direct and proximate cause of Flock's business practices, Plaintiffs and Class
22 members were damaged because their ALPR data has been improperly shared with federal and
23 out-of-state agencies as well as, potentially, other unauthorized third parties, and that data was not
24 properly safeguarded.

25 200. Flock's violation of the ALPR Privacy Act constitutes negligence per se, and its
26 willful and reckless conduct warrants an award of compensatory and punitive damages.

27 201. Flock's failure to limit ALPR information-sharing and maintain reasonable and
28 adequate information- and data-security practices was precisely the kind of conduct the ALPR
Privacy Act was designed to prevent.

1 210. By aggregating and analyzing Plaintiffs’ and Class Members’ vehicle
2 characteristics and movements over extended periods of time using its proprietary software,
3 Defendant intentionally invaded Plaintiffs’ and Class Members’ privacy rights, as well as intruded
4 upon Plaintiffs’ and Class Members’ seclusion.

5 211. By developing and deploying proprietary software capable of not just reading and
6 logging a license plate number, but creating detailed profiles of vehicles, reporting past
7 movements, and predicting future movements, Defendant intentionally invaded Plaintiffs’ and
8 Class Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class Members’ seclusion.

9 212. By developing and deploying proprietary software that allows Defendant to share
10 the aforementioned information about Plaintiffs and Class Members with any of its customers
11 across California and the United States, Defendant intentionally invaded Plaintiffs’ and Class
12 Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class Members’ seclusion.

13 213. By developing and deploying technology that allows Defendant to merge the
14 aforementioned data about Plaintiffs and Class Members with data from external sources,
15 including data brokers and credit reporting agencies, thus creating more detailed and
16 commercially valuable profiles of Plaintiffs and Class Members, Defendant intentionally invaded
17 Plaintiffs’ and Class Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class
18 Members’ seclusion.

19 214. Plaintiffs and Class Members do not anticipate that their daily travels be recorded
20 or that this information be fused with non-Flock data sources such as information compiled by
21 data brokers and credit reporting agencies, to generate detailed and highly personal profiles about
22 them, let alone profiles that local and out-of-state law enforcement agencies may easily search,
23 access, and act upon. Plaintiffs and Class Members do not and cannot know which categories of
24 information Defendant may or may not be fusing with the detailed digital profiles it is compiling
25 about them.

26 215. By sharing data on California drivers’ vehicles and movements with federal law
27 enforcement agencies who have amassed information on individuals and are able to merge these
28 datasets, Defendant further empowered the federal government to create detailed profiles of

1 Plaintiffs engaged in lawful activity that the federal government is criminalizing, including
2 participating in peaceful protests against the federal government. This has further intruded upon
3 and eroded Plaintiffs' privacy rights.

4 216. The nature and volume of the data collected is such that Defendant's practice of
5 compiling comprehensive profiles of Plaintiffs' and Class Members violates their reasonable
6 expectation of privacy.

7 217. The generation of detailed profiles on Plaintiffs and Class Members allow third
8 parties to learn intimate details about Plaintiffs and Class Members' lives, thus allowing them to
9 be targeted for advertising and political purposes and abrogating their autonomy and ability to
10 control the dissemination and use of information about them. This also violated their reasonable
11 expectation of privacy.

12 218. Plaintiffs and Class Members did not and could not authorize Defendants to
13 intercept data on their activities.

14 219. By engaging in the aforementioned actions, Flock intentionally invaded Plaintiffs'
15 and Class Members' privacy rights under the California Constitution.

16 220. This invasion of privacy is serious in nature, scope, and impact. Moreover, it
17 constitutes an egregious breach of the societal norms underlying the right of privacy.

18 221. As a result of Flock's actions, Plaintiffs and Class Members have suffered harm
19 and injury, including but not limited to an invasion of their privacy rights.

20 222. Plaintiffs and Class Members have been damaged as a direct and proximate result
21 of Flock's invasion of their privacy and are entitled to just compensation, including monetary
22 damages.

23 223. Plaintiffs and Class Members seek appropriate relief for this injury, including but
24 not limited to damages that will reasonably compensate them for the harm to their privacy
25 interests.

26 224. Plaintiffs and Class Members are also entitled to punitive damages resulting from
27 the malicious, willful, and intentional nature of Flock's actions, directed at injuring Plaintiffs and
28 Class Members in conscious disregard of their rights.

1 Defendant intentionally invaded Plaintiffs’ and Class Members’ privacy rights, as well as intruded
2 upon Plaintiffs’ and Class Members’ seclusion.

3 232. By developing and deploying proprietary software capable of not just reading and
4 logging a license plate number, but creating detailed profiles of vehicles, reporting past
5 movements, and predicting future movements, Defendant intentionally invaded Plaintiffs’ and
6 Class Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class Members’ seclusion.

7 233. By developing and deploying proprietary software that allows Defendant to share
8 the aforementioned information about Plaintiffs and Class Members with any of its customers
9 across California and the United States, Defendant intentionally invaded Plaintiffs’ and Class
10 Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class Members’ seclusion.

11 234. By developing and deploying technology that allows Defendant to merge the
12 aforementioned data about Plaintiffs and Class Members with data from external sources,
13 including data brokers and credit reporting agencies, thus creating more detailed and
14 commercially valuable profiles of Plaintiffs and Class Members, Defendant intentionally invaded
15 Plaintiffs’ and Class Members’ privacy rights, as well as intruded upon Plaintiffs’ and Class
16 Members’ seclusion.

17 235. Plaintiffs and Class Members do not anticipate that their daily travels be recorded
18 or that this information be fused with non-Flock data sources such as information compiled by
19 data brokers and credit reporting agencies, to generate detailed and highly personal profiles about
20 them, let alone profiles that local and out-of-state law enforcement agencies may easily search,
21 access, and act upon. Plaintiffs and Class Members do not and cannot know which categories of
22 information Defendant may or may not be fusing with the detailed digital profiles it is compiling
23 about them.

24 236. By sharing data on California divers’ vehicles and movements with federal law
25 enforcement agencies who have amassed information on individuals and are able to merge these
26 datasets, Defendant further empowered the federal government to create detailed profiles of
27 Plaintiffs engaged in lawful activity that the federal government is criminalizing, including
28

1 participating in peaceful protests against the federal government. This has further intruded upon
2 and eroded Plaintiffs' privacy rights.

3 237. The nature and volume of the data collected is such that Defendant's practice of
4 compiling comprehensive profiles of Plaintiffs' and Class Members violates their reasonable
5 expectation of privacy.

6 238. The generation of detailed profiles on Plaintiffs and Class Members allow third
7 parties to learn intimate details about Plaintiffs and Class Members' lives, thus allowing them to
8 be targeted for advertising and political purposes and abrogating their autonomy and ability to
9 control the dissemination and use of information about them. This also violated their reasonable
10 expectation of privacy.

11 239. Plaintiffs and Class Members did not and could not authorize Defendants to
12 intercept data on their activities.

13 240. The conduct as described herein is highly offensive to a reasonable person and
14 constitutes an egregious breach of social norms.

15 241. Plaintiffs and Class Members seek appropriate relief for this injury, including but
16 not limited to damages that will reasonably compensate them for the harm to their privacy
17 interests.

18 242. Accordingly, Plaintiffs and Class Members and California Subclass Members seek
19 all relief available for invasion of privacy claims under common law.

20 **COUNT V**

21 **Violations of California's Unfair Competition Law ("UCL")**

22 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

23 **(On behalf of Plaintiffs, the Class, and the Subclass)**

24 243. Plaintiffs incorporates all prior allegations as if fully set forth herein and brings
25 this Count individually and on behalf of the proposed Class.

26 244. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or
27 fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal.
28 Bus. & Prof. Code § 17200.

1 245. Flock engaged in unlawful business practices in connection with its disclosure of
2 ALPR data belonging to Plaintiffs and Class Members’ to federal and out-of-state law
3 enforcement agencies despite the legal, moral, ethical, and policy requirements against doing so.

4 246. Flock’s acts, omissions, and conduct, as alleged herein, constitute “business
5 practices” within the meaning of the UCL.

6 247. Flock violated the “unlawful” prong of the UCL by violating, *inter alia*, Plaintiffs
7 and Class Member’ constitutional rights to privacy, state privacy statutes, state consumer
8 protection statutes, and ALPR technology specific statutes.

9 248. Flock’s acts, omissions, and conduct also violate the unfair prong of the UCL
10 because those acts, omission, and conduct offend public policy (namely the ALPR Privacy Act)
11 and constitute immoral, unethical, oppressive, and unscrupulous activities that cause substantial
12 injury, including Plaintiffs and Class Members.

13 249. Flock’s conduct was unfair because it knew or should have known that it was
14 collecting and sharing sensitive personal information and continued to do so anyway despite
15 knowing about Californian’s privacy rights and the harms that could result by disseminating such
16 information to federal and out-of-state law enforcement agencies, as well as creating detailed
17 profiles of Plaintiffs and Class Members using third party data and its proprietary software.

18 250. The harm caused by Flock’s conduct outweighs any potential public safety benefits
19 attributable to such conduct, and there is reasonable alternative to further Flock’s legitimate
20 business interests other than Flock’s conduct described herein.

21 251. As a result of Flock’s violations of the UCL, Plaintiffs and Class Members are
22 entitled to injunctive relief. This is particularly true since the dissemination of Plaintiffs’ and Class
23 Members’ ALPR is ongoing.

24 252. Plaintiffs and Class Members have suffered an injury-in-fact as a proximate result
25 of the violations of law and wrongful conduct of Flock alleged herein, and they lack an adequate
26 remedy at law to address the unfair conduct at issue here.

27 253. Plaintiffs seek an injunction prohibiting Flock’s ongoing violations under the UCL.
28

1 **PRAYER FOR RELIEF**

2 Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that the
3 Court grant the following relief:

- 4 a. Certification of this action as a class action and appointment of Plaintiffs and
5 Plaintiffs’ counsel to represent the Class;
- 6 b. A declaratory judgement that Defendant violated Cal. Civ. Code §§1798.90.5 *et*
7 *seq.* and California common law;
- 8 c. An order enjoining Flock from engaging in the unlawful practices and illegal acts
9 described herein; and
- 10 d. An order awarding Plaintiffs and the Class: (1) actual or liquidated damages
11 (whichever is higher); (2) punitive damages—as warranted—in an amount to be
12 determined at trial; (3) injunctive relief as the Court may deem proper; (4)
13 reasonable attorneys’ fees and expenses and costs of suit pursuant to Cal. Code of
14 Civil Procedure § 1021.5 and/or other applicable law; (5) pre-judgment and post-
15 judgment interest as provided by law; and (6) such other and further relief as the
16 Court may deem appropriate.

17 **DEMAND FOR JURY TRIAL**

18 Plaintiff, individually and on behalf of the proposed Class, requests a trial by jury of all
19 claims that can be so tried.

20 Dated: February 26, 2026

GIBBS MURA LLP

21 By: 
 22 David M. Berger (SBN 277526)
 23 Jane Farrell (SBN 333779)
 24 Jennifer Sun (SBN 354276)
 25 Kate Walford (SBN 362658)

GIBBS MURA LLP
 1111 Broadway, Suite 2100
 Oakland, CA 94607
 Telephone: (510) 350-9700
 Fax: (510) 350-9701
 dmb@classlawgroup.com
 jgf@classlawgroup.com
 jsun@classlawgroup.com
 kgw@classlawgroup.com

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

Gary M. Klinger*
Mike Acciavatti*
Heather M. Lopez (SBN 354022)
Milberg PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (331) 240-3015
gklinger@milberg.com
macciavatti@milberg.com
hmlopez@milberg.com

**pro hac vice forthcoming*

Attorneys for Plaintiffs