David M. Berger (SBN 277526)
Jane Farrell (SBN 333779)
Jennifer Sun (SBN 354276)
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@classawgroup.com
jsun@classlawgroup.com
kgw@classlawgroup.com

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

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SAN FRANCISCO

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

Plaintiffs,

v.

FLOCK GROUP, INC., d/b/a Flock Safety,

Defendant.

Case No. _____

CLASS ACTION

COMPLAINT FOR DAMAGES:

(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

TABLE OF CONTENTS

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

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

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

NATURE OF THE CASE

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

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

3. Flock operates ALPRs nationwide, including thousands of devices across cities throughout California.[3] More than 200 California law enforcement agencies use Flock's ALPR data.[4]

---

[1] Aaron Mak, *The CEO of Flock downloads on his surveillance cameras*, POLITICO (Dec. 22, 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.")

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

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

[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).

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

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

6. California's ALPR Privacy Act[5] explicitly prohibits California law enforcement agencies and Flock from sharing California ALPR data with federal agencies or out-of-state law enforcement agencies. It also requires Flock to ensure its California customers use ALPR information only for authorized purposes, and maintain reasonable security measures to prevent unauthorized access and use. Flock has blatantly violated these requirements for the California entities using its products and services.

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

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

---

[5] Throughout this Complaint, the ALPR Privacy Act will refer to the laws codified in Cal. Civ. Code §§1798.90.5 *et seq*.

[6] License Plate Readers (LPR): Stop Crime in Its Tracks with Evidence That Drives Action, FLOCK SAFETY [hereinafter Flock License Plate Readers], https://www.flocksafety.com/products/license-plate-readers [https://perma.cc/RZU8-K5HG] (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).

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

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

11. Across California, out-of-state and federal agency sharing is pervasive. For example, Flock allowed law enforcement agencies from outside of California to search the San Francisco Police Department's ALPR database more than 1.6 million times between August 2024 and February 2025.[7] Likewise, Flock allowed agencies from 48 other states to search the Los Altos, California database over a million times in 2024 and 2025.[8] And Flock shares El Cajon's ALPR network data with over 300 out-of-state law enforcement agencies, including those in Alabama, Minnesota, Ohio, and Texas.[9]

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

---

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

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

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

[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),

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

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

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

---

https://www.kqed.org/news/12072077/as-california-cities-grow-wary-of-flock-safety-cameras-mountain-views-shuts-its-off.

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

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

[13] Rachel Myrow, *Santa Cruz the First in California to Terminate Its Contract With Flock Safety*, KQED (Jan. 14, 2026), 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 license plate readers, after Santa Cruz, Los Altos Hills jettison Flock Safety service*, LOS GATAN (Jan. 28, 2026), 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.

[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,

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

PARTIES

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

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

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

JURISDICTION AND VENUE

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

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

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

22. Venue is proper in the County of San Francisco pursuant to California Code of Civil Procedure §§ 393 and 395, *et seq*., because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this County.

FACTUAL ALLEGATIONS

I. ALPR Cameras and California's ALPR Privacy Act

23. Modern ALPR technology uses specialized cameras and software to automatically scan, record, and convert vehicle license plates into digital data.[15] These systems are typically mounted onto local infrastructure and scan the license plate of every vehicle that passes by. While each camera captures one point in time, the data from each camera is merged to track and map a vehicle's movements across entire regions at all hours of the day, every day of the year. The ALPR cameras capture images of license plates, using Optical Character Recognition (OCR) to convert the images into machine-readable text in real time.

24. In 2015, the California Legislature enacted the ALPR Privacy Act to mitigate ALPR systems' risks to privacy and initiated strict requirements on operators and users of ALPR surveillance. The legislature noted that by aggregating license plate numbers with specific locations and timestamps, operators can reconstruct a person's exact location and day-to-day patterns:

> The collection of a license plate number, location, and time stamp over multiple time points can identify not only a person's exact whereabouts but also their pattern of movement. Unlike other types of personal information that are covered by existing law, civilians are not always aware when their ALPR data is being collected. One does not even need to be driving to be subject to ALPR technology: A car parked on the side of the road can be scanned by an ALPR system. This bill will put in place minimal privacy protections by requiring the establishment of privacy and usage protection policies for ALPR operators and end-users.[16]

---

[15] ALPR camera technology is distinguishable from a standard traffic camera. Traffic cameras only record specific violations at a single point in time, such as speeding on a stretch of road or running a red light at an intersection. In contrast, ALPRs are always recording, documenting, and uploading information into a centralized data store. Thus, ALPRs capture all vehicles that pass by ALPR cameras through a city or region. *See* Mario Lotmore, *Somebody's watching me: Flock versus red light cameras in Lynnwood*, LYNNWOOD TIMES (Nov. 10, 2025), https://lynnwoodtimes.com/2025/11/10/red-light.

[16] S. Comm. on Transportation and Housing, Bill Analysis, SB 34, ¶ 3 (2015).

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

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

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

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

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

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

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

[17] Cal. Civ. Code § 1798.90.5.

iii. A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

iv. The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.

v. The title of the official custodian, or owner, of the ALPR system responsible for implementing this section.

vi. A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.

vii. The length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information.

Id. §§ 1798.90.51(b), 1798.90.53(b).

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

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

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

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

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

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

31. The California AG emphasized:[18]

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

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

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

---

[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.

[19] *Id*.

[20] *Id*.

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

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

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

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

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

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

39. Flock's most popular products, the "Falcon" and the "Sparrow," are ALPR cameras that monitor driving activity and photograph all passing vehicles.

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

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

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

a. License plate image;

b. Vehicle image;

c. Vehicle characteristics (e.g., color, make, other vehicle attributes);

d. License plate number;

e. License plate state;

---

[21] Frequently Asked Questions: What kind of vehicles can a Flock Safety camera identify?, FLOCK SAFETY, https://www.flocksafety.com/faq [https://perma.cc/L4MU-CVPW] (last 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://perma.cc/HT32-3JXD].

[22] License Plate Reader Policy, FLOCK SAFETY [hereinafter Flock LPR Policy], 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).

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

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

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

48. Flock's "Investigations Manager" tool[28] proactively analyzes movement patterns and related data to flag potentially "suspicious" vehicles. It identifies vehicles that tend to move together and labels the cars and affiliated individuals as "suspect networks." In marketing materials for Investigations Manager, Flock "urges police departments to 'Maximize [their] LPR data to detect patterns of suspicious activity across cities and states.'"[29]

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

---

[25] *Id.*; Flock License Plate Readers, *supra* note 6 ("No Plate? No Problem. Turn images into actionable evidence – no plate required.").

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

[27] Flock License Plate Readers, *supra* note 6.

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

[29] Jay Stanley, *Surveillance Company Flock Now Using AI to Report Us to Police if It Thinks Our Movement Patterns Are "Suspicious"*, ACLU: NEWS & COMMENTARY (Aug. 7, 2025), [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.

together," thus tracking people's associations; and [3] a "Multiple locations search," which aims to "Uncover vehicles seen in multiple locations."[30]

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

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

52. The use of Flock's high-end but inexpensive tools and the associated databases that Flock has created allow law enforcement agencies across the country to have instant access to shared data from tens of thousands of cameras—exactly the kind of practice that the ALPR Privacy Act regulates.

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

---

[30] *Id.*

[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-

54. The Los Angeles County Sheriff's Department alone operates 476 Flock ALPR cameras.[32]

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

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

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

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

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

---

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

[32] Rebecca Ellis, *L.A. County moves to keep ICE away from data that show where people drive*, 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.

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

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

[35] Flock National LPR Network, *supra* note 6.

[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.

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

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

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

---

[38] Letter from Jennifer Pinsof, Staff Att'y, Elec. Frontier Found.; Matt Cagle, Senior 18 Staff Att'y, ACLU Found. of N. Cal.; Mohammad Tasjar, Senior Staff Att'y, ACLU Found. of S. Cal.; & David Trujillo, Chief Program & Strategy Officer, to Att'y Gen. Rob Bonta, Off. of the Att'y Gen., Cal. Dep't of Just., at 2 (Jan. 31, 2024) [hereinafter EFF–ACLU Joint Letter], https://www.eff.org/files/2024/01/30/2024-01-31_letter_to_ag_bonta_re_sb_34_final.pdf (citing *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).

[39] Jay Stanley, *"Suspicious" Movement Patterns*, supra note 29.

[40] Joseph Cox, *License Plate Reader Company Flock Is Building a Massive People Lookup Tool, 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/.

62. ALPR technology's potential as a crime-fighting tool must be weighed against the increasingly invasive—and highly offensive to a reasonable person—widespread domestic surveillance[41] and profiling of California drivers.

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

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

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

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

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

---

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

[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-

67. For example, Flock enabled federal law enforcement agencies, including the Department of Homeland Security ("DHS") and DHS's Customs and Border Control ("CBP")[43] to access Flock's National Lookup utility. Flock never even alerted its customers that federal agencies would have access.[44]

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

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

---

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

[43] Byron Tau and Garance Burke, *Border Patrol is monitoring US drivers and detaining those 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/.

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

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

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

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

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

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

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

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

---

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

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

[49] Garrett Langley, *Setting the Record Straight: Statement on Flock Network Sharing, Use 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.

near-unanimously to terminate its contract with Flock, "citing rising tensions with ICE, and weak trust in the company following Flock's lackluster response to the data breaches."[51]

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

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

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

77. **1:1 Sharing:** Law enforcement agencies using Flock can enter into 1:1 agreements with other agencies to share ALPR data. Flock makes this possible by allowing any law enforcement agency to "request" access from another agency. An agency may grant the individual or bulk requests through the click of a button, and sometimes even automatically.[54] Flock's

---

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

[52] *Id.*

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

[54] Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, 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/.

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

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

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

80. "Once a department allows another agency to access its system, the outside agency can search the data without needing approval each time."[58] Likewise, users can query multiple

---

[55] Spencer Soicher, *Flock admits federal immigration agents have direct access to tracking data, despite previous claims*, 9NEWS (August 19, 2025), https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8aee742-56d4-4a57-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/

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

[57] El Cajon Transparency Portal, *supra* note 9.

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

networks simultaneously—searches of Oakland's ALPR data, for example, were found to reach hundreds of other networks at once.[59]

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

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

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

---

[59] *Id.*

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

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

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

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

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

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

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

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

---

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

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

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

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

agencies despite knowing that its practice of sharing ALPR with federal agencies "violates state law."[67] Flock's 1:1 agreement sharing settings means that any one of these searches exposed hundreds of California agencies—and millions of California drivers—to CBP and ICE surveillance against California law.

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

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

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

---

[67] Chien, *California cops are breaking surveillance laws*, *supra* note 58.

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

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

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

92. **Flock Investigative Tools:** The investigative tools that Flock developed and offers to its customers have also flouted agencies' sharing settings and agreements. Features like "Multi-State Insights" let an investigator in one state see that a vehicle of interest has traveled through other states, including California.[71] Additionally, if a California vehicle is added to a national hotlist, a Flock camera detecting it in California will generate a real-time alert[72] that is visible to any agency nationwide monitoring that hotlist.

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

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

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

95. Flock has an ALPR policy, which was last updated on November 13, 2025.[73]

96. In its Terms and Conditions, Flock defines its authorized or "permitted" purpose as "legitimate public safety and/or business purpose, including but not limited to the awareness,

---

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

[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.

prevention, and prosecution of crime; investigations; and prevention of commercial harm, *to the extent permitted by law*."[74]

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

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

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

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

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

[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).

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

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

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

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

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

---

[75] Flock Aligns License Plate Reader Technology with State-Specific Legal Frameworks, 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].

[76] Langley, *Ensuring Local Compliance*, *supra* note 44.

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

[78] Flock LPR Policy, *supra* note 22.

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

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

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

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

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

V. Flock's Security Measures Fall Far Below Reasonable Procedures and Practices

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

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

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

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

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

115. A security analyst known as Jon "GainSec" Gains published a formal white paper exposing "*dozens* of security vulnerabilities"—many of which the white paper describes as "critical" in Flock's cameras, including its ALPR readers.[79]

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

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

---

[79] Jon Gains, *Examining the security posture of an Anti-Crime Ecosystem*, GAINSEC, (Nov. 11, 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/.*

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

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

i. **Physical vulnerabilities:** "Pressing an easily accessible button on the back of Flock cameras (which, you may recall, are mounted in public across the country) a handful of times in an extremely simple sequence will open a wireless access point, which is easily hijacked to grant root access to the camera's systems; once you have 'root,' you can connect to the device, access its video data, and install whatever you'd like. Flock cameras' exposed USB ports offer another avenue to gain control of the device to scrape data, insert fake camera feeds or anything else, obtain police information, and generally perform an endless variety of manipulations."

ii. **Unsupported operating system:** "Flock cameras still run on Android Things 8.1— an outdated mobile system that, crucially, has been discontinued and is no longer supported by Google with security patches. Unsupported operating systems are essentially undefended, riddled with known exploits."

iii. **Unprotected testing data:** "Flock . . . left its internal testing data accessible online: a trove that included police names and phone numbers, patrol areas, suspect hotlists, full license plates and even geographic information systems (GIS) data showing the live location of patrol cars."

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

119. This statement is misleading at best. As noted in the article, "[t]he failings are farcical for a purported 'security' company." As above, to the extent these exploits require

---

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

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

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

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

VI. Flock's Facilitation of California Law Enforcement Agencies' Unlawful Information Sharing Is Highly Offensive

A. Flock's Network Amplifies Discriminatory Policing Practices

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

123. As noted by several privacy advocates and the ACLU, "police often disproportionately deploy license plate readers in communities experiencing poverty and historically overpoliced communities of color, regardless of crime rates."[86]

---

[83] Tyler Walicek, *Vast Camera System Feeds Information*, *supra* note 81.

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

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

[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),

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

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

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

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

---

https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data; Barton Gellman & Sam Adler-Bell, *The Disparate Impact of Surveillance*, CENTURY FOUND. (Dec. 21, 2017), 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 Police and Lenders Target the Poor*, THE ATLANTIC (Apr. 22, 2016), https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436 (summarizing data indicating that Oakland Police Department deployed ALPRs disproportionately, often in low-income areas and in 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.

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

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

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

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

---

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

[90] Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 MEDIA (May 29, 2025), 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 insisted that the search was not "related to enforcing Texas's abortion ban" and that "media accounts" were "'false,' 'misleading,' and 'clickbait.'" These claims were proven false. *See* Dave Maass & Rindala Alajaji, *Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation.*, ELEC. FRONTIER FOUND. (Oct. 7, 2025), https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it ("New documents and court records obtained by EFF show that Texas deputies queried Flock Safety's surveillance data in an abortion investigation. The new information shows that deputies had initiated a 'death investigation' of a 'non-viable fetus,' logged evidence of a woman's self-managed abortion, and consulted prosecutors about possibly charging her."); Jason Koebler & Joseph Cox, *Police Said They Surveilled Woman Who Had an Abortion for Her 'Safety.' Court Records Show They Considered Charging Her With a Crime*, 404 MEDIA (Oct. 7, 2025), 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/.

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

C. Flock's ALPR System Threatens Protected First Amendment Activity

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

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

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

---

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

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

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

[94] *Id*.

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

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

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

PLAINTIFFS' EXPERIENCES

I. Plaintiff Javorsky's Experience

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

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

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

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

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

---

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

[96] *Id*.

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

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

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

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

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

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

II. Plaintiff Mayor's Experience

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

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

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

---

[97] Chien, Tomo, *Oakland police illegally shared license plate data: lawsuit*, S.F. STANDARD (Nov. 18, 2025), https://sfstandard.com/2025/11/18/oakland-police-opd-lawsuit-flock-surveillance/; Chien, *Georgia, Texas cops illegally search*, supra note 7; *Why Are The Alameda 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-sharing-so-much-data-with-287g-agencies.

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

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

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

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

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

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

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

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

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

---

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

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

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

III. Plaintiffs' Data from Flock Cameras Has Economic Value

161. Every day, commercial entities purchase data about individuals—including their location history—from data brokers[99] and other sources to run advertisements and target their services.[100]

162. For the past decade, data brokers have sought out and combined data from private and public sources. While individual data sources "may provide only a few elements about a person's activities, data brokers combine these elements to form a detailed, composite view of the consumer's life."[101]

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

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

---

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

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

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

165. Indeed, Flock itself developed its "Nova" product to fuse—and thus enhance the value of—both third-party and Flock datasets.[102]

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

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

CLASS ACTION ALLEGATIONS

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

a. All individuals whose license plate data was collected in California by the Flock ALPR system and was accessible by, and thus disclosed to, federal law enforcement agencies, out-of-state agencies on or after February 26, 2022 (the "Class Period").

b. All individuals whose license plate data was collected in California by the Flock ALPR system and was searched for by federal law enforcement agencies and/or out-of-state agencies during the Class Period.

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

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

---

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

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

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

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

(a) Whether Flock implemented and maintained a policy that complied with California's ALPR Privacy Act;

(b) Whether Flock complies with the Notice, Privacy, Security, Audit, and Proper-Use Requirements set forth in California's ALPR Privacy Act;

(c) Whether Flock gathered location data and license plan scans of Class Members;

(d) Whether Flock's policies permit unauthorized access of Flock ALPR data owned by California law enforcement agencies by federal agencies or out-of-state law enforcement agencies;

(e) Whether Class Members' data was shared with out-of-state or federal agencies;

(f) Whether Flock knew or should have known that its infrastructure and inadequate policy facilitated unauthorized sharing of Class Members' ALPR data with federal and out-of-state agencies;

(g) Whether the unauthorized sharing of Class Members' ALPR data has harmed the Class;

(h) Whether Flock's violations of California law have harmed the class; and

(i) Whether Flock is subject to punitive damages under California's ALPR Privacy

Act and California common law.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT II
Negligence
(On behalf of Plaintiffs, the Class, and the Subclass)

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

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

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

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

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

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

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

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

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

202. Plaintiffs and the Class are the class of persons the ALPR Privacy Act is intended to protect—drivers within California whose data is subject to ALPR collection.

203. Flock's willful and reckless breach of its duty caused Plaintiffs and the Class to suffer damages.

204. Under California law—specifically, the evidentiary doctrine of negligence per se—these circumstances create a presumption of negligence.

205. There is no justification or excuse for Flock's violation of the ALPR Privacy Act.

206. Flock is therefore liable for compensatory and punitive damages under California law.

COUNT III
Invasion of Privacy Under California's Constitution
(On behalf of Plaintiffs, the Class, and the Subclass)

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

208. Plaintiffs and Class Members have an interest in: (i) conducting lawful personal and political activities without surveillance, intrusion, or interference, including, but not limited to, the right to move from place to place without being subjected to highly intrusive and surreptitious surveillance and tracking; (ii) not having detailed profiles about their vehicle and movements generated and logged over a period of weeks, months, or years that third parties may use to determine their location and/or predict future movements; (iii) precluding the dissemination, use, or abuse of the aforementioned information, including the fusing of this information with any other third party data sets profiles about Plaintiffs and Class Members; (iv) not sharing the aforementioned information with out-of-state or federal law enforcement agencies; and (v) controlling the dissemination of private information about themselves.

209. By conducting widespread and round-the-clock surveillance of Plaintiffs' and Class Members' movements using its ALPR technology, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights, as well as intruded upon Plaintiffs' and Class Members' seclusion.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

225. Such damages are needed to deter Flock from engaging in such conduct in the future.

226. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT IV
Intrusion Upon Seclusion
(On behalf of Plaintiffs, the Class, and the Subclass)

227. Plaintiffs incorporate all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class, pursuant to California law.

228. To state a claim for intrusion upon seclusion "[Plaintiffs] must possess a legally protected privacy interest … [Plaintiffs'] expectations of privacy must be reasonable … [and Plaintiffs] must show that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc*. 47 Cal. 4th 272, 286-87 (2009).

229. Plaintiffs and Class Members have an interest in: (i) conducting lawful personal and political activities without surveillance, intrusion, or interference, including, but not limited to, the right to move from place to place without being subjected to highly intrusive and surreptitious surveillance and tracking; (ii) not having detailed profiles about their vehicle and movements generated and logged over a period of weeks, months, or years that third parties may use to determine their location and/or predict future movements; (iii) precluding the dissemination, use, or abuse of the aforementioned information, including the fusing of this information with any other third party data sets profiles about Plaintiffs and Class Members; (iv) not sharing the aforementioned information with out-of-state or federal law enforcement agencies; and (v) controlling the dissemination of private information about themselves.

230. By conducting widespread and round-the-clock surveillance of Plaintiffs' and Class Members' movements using its ALPR technology, Defendant intentionally invaded Plaintiffs' and Class Members' privacy rights, as well as intruded upon Plaintiffs' and Class Members' seclusion.

231. By aggregating and analyzing Plaintiffs' and Class Members' vehicle characteristics and movements over extended periods of time using its proprietary software,

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT V
Violations of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of Plaintiffs, the Class, and the Subclass)

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

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

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

246. Flock's acts, omissions, and conduct, as alleged herein, constitute "business practices" within the meaning of the UCL.

247. Flock violated the "unlawful" prong of the UCL by violating, *inter alia,* Plaintiffs and Class Member' constitutional rights to privacy, state privacy statutes, state consumer protection statutes, and ALPR technology specific statutes.

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

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

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

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

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

253. Plaintiffs seek an injunction prohibiting Flock's ongoing violations under the UCL.

PRAYER FOR RELIEF

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

a. Certification of this action as a class action and appointment of Plaintiffs and Plaintiffs' counsel to represent the Class;

b. A declaratory judgement that Defendant violated Cal. Civ. Code §§1798.90.5 *et seq.* and California common law;

c. An order enjoining Flock from engaging in the unlawful practices and illegal acts described herein; and

d. An order awarding Plaintiffs and the Class: (1) actual or liquidated damages (whichever is higher); (2) punitive damages—as warranted—in an amount to be determined at trial; (3) injunctive relief as the Court may deem proper; (4) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil Procedure § 1021.5 and/or other applicable law; (5) pre-judgment and post-judgment interest as provided by law; and (6) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

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

Dated: February 26, 2026

GIBBS MURA LLP

By: _____

David M. Berger (SBN 277526)
Jane Farrell (SBN 333779)
Jennifer Sun (SBN 354276)
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

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