Daniel L. Warshaw (CA Bar No. 185365)
Matthew A. Pearson (CA Bar No. 291484)
dwarshaw@pwfirm.com
mapearson@pwfirm.com
**PEARSON WARSHAW, LLP**
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

Renner K. Walker (CA Bar No. 295889)
Steven M. Nathan (CA Bar No. 153250)
rwalker@hausfeld.com
snathan@hausfeld.com
**HAUSFELD LLP**
33 Whitehall Street
14th Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

*Attorneys for Plaintiff and the proposed Class*
*[Additional counsel listed on signature page]*

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

JASON HELLERMAN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

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

Defendant.

Case No. 2:26-cv-00515

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

# 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 database. Defendant Flock Group, Inc. d/b/a Flock Safety ("Defendant" or "Flock") owns and leases many of those cameras, operates and maintains the database that holds the billions of images and data they capture, provides the software and AI architecture that makes nationwide coordination possible, and facilitates real-time information sharing through its networks. Flock's biggest customers are law enforcement agencies that rely on Flock to provide a secure service enabling quick and comprehensive investigations without unlawfully intruding on driver privacy.

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 potential law enforcement benefits of ALPR technology against the very real threat to privacy and civil liberties this unprecedented infrastructure poses. In 2015, California enacted Senate Bill 34 ("SB 34," codified at Cal. Civ. Code §§ 1798.90.5 *et seq.*), permitting ALPR technology but placing clear limits on the capture, use, storage, and sharing of ALPR data. Pertinent to this action, neither California law enforcement agencies nor Flock may share California ALPR data with federal agencies or out-of-state law enforcement agencies.

Yet California law enforcement agencies—sometimes deliberately, sometimes inadvertently, but always with Flock's assistance—have consistently flouted SB 34's restrictions on data sharing. Flock easily could have implemented policies to prevent California law enforcement agencies from violating SB 34; indeed, it was required to do so. But Flock has instead knowingly permitted its law enforcement clients to engage in unlawful information sharing, including with federal agencies, out-of-state law enforcement agencies, and the public at large, by not implementing access limitations or adequate security protocols. Meanwhile, it has openly disclaimed its

duty to prevent unlawful information sharing by California law enforcement agencies.

Flock has repeatedly and publicly disclaimed any responsibility for violations of SB 34, instead blaming California law enforcement agencies for any violations. In so doing, Flock has ignored its ability—and duty—not only to comply with SB 34 itself but also to ensure its California law enforcement clients' compliance. Plaintiff Jason Hellerman therefore brings this Class Action Complaint and Demand for Jury Trial against Flock for violating SB 34 (Cal. Civ. Code §§ 1798.90.5 *et seq.*) and California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code §§ 17200 *et seq.*) as well as breaching duties owed to Plaintiff and a proposed class of similarly situated individuals ("the Class," defined *infra* ¶ 160) under California common law.

## NATURE OF THE ACTION

1. In recent years, law enforcement authorities have expanded daily surveillance of citizens, including by leveraging increasingly sophisticated technology in public spaces.

2. One particularly intrusive surveillance advancement combines the deployment of thousands of cameras with ALPR technology, AI, and vast, interconnected databases. This allows law enforcement agencies to locate and track vehicles of interest over long distances retroactively, in real time, and even prospectively, predicting future journeys and flagging supposedly "suspicious" driving activity by surveilling every driver's daily patterns.

3. Private companies, like Flock, own and operate ALPR systems and facilitate the gathering, storage, use, and sharing of ALPR data. ALPR operators like Flock not only manufacture and own the ALPR cameras themselves but also create, operate, and maintain databases that enable law enforcement agencies, including California law enforcement agencies, to aggregate locally gathered ALPR data with ALPR data gathered by other law enforcement agencies. Flock is one of the largest ALPR operators in the United States and boasts of a nationwide web of ALPR networks, ALPR devices, and law enforcement agencies.

4. The California Legislature has recognized that any benefits to law enforcement, public safety, and security from leveraging ALPR technology must necessarily be balanced with the intrusion upon privacy and potential harm to civil liberties that widespread ALPR use unavoidably entails.

5. In 2015, the Legislature enacted SB 34, which cabins the discretion of law enforcement agencies and ALPR operators and strictly regulates the use and sharing of ALPR data.

6. Notably, SB 34 requires ALPR operators like Flock to "[m]aintain 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). Likewise, under SB 34, ALPR operators must "[r]equire that ALPR information only be used for the authorized purposes[.]" *Id.* § 1798.90.52(b).

7. Regarding "authorized purposes," SB 34 provides that "[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). Correspondingly, the statute defines "public agency" as "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.* § 1798.89.5(f), making clear that California law enforcement agencies may share ALPR information *only* with other California agencies—*not* federal agencies or out-of-state law enforcement agencies. Thus, the Office of California Attorney General Rob Bonta ("California AG") has sued individual California law enforcement agencies for violating SB 34.[1]

[1] 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, 2025), https://oag.ca.gov/news/press-releases/attorney-general-bonta-sues-el-cajon-illegally-sharing-license-plate-data-out.

8. Flock has ignored and willfully misconstrued both the plain language of SB 34 and the California AG's publicly provided interpretation of the statute. Flock failed to implement a policy to prevent law enforcement agencies outside of California from searching networks within California, which allowed, as an example, 5,757 law enforcement agencies to run more than 1.6 million unlawful searches of San Francisco's ALPR database.[2] Recently, the Los Angeles Police Department shared the results of a search of its Flock database with federal law enforcement agencies.[3] With Flock networks in hundreds of cities and communities across California,[4] Flock has violated SB 34—and Californians' privacy rights—an untold number of times by facilitating federal agencies and out-of-state law enforcement access to and use of its California ALPR databases.

9. Flock further violates California law by failing to maintain reasonable security procedures and practices as required by Cal. Civ. Code § 1798.90.51(a).

10. 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"[5]—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

[2] 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, *SFPD ICE Data Sharing*], https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing.

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

[4] *See ALPR Map*, DEFLOCK, https://deflock.me/map (last visited Jan. 2, 2026).

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

account did Flock make MFA its default setting—and even then, Flock still failed to *require* MFA.

11. 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."[6]

12. The lack of mandatory MFA is just one of Flock's failings. Recently, a security analyst known as Jon "GainSec" Gaines 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.

13. 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.[7]

14. 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":[8]

- ***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

[6] *Id.*

[7] 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.

[8] Walicek, *supra* note 5.

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."

- ***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."

- ***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."

15. In response to the GainSec white paper, Flock released a statement attempting to reassure clients, 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."[9]

16. 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 physical access to Flock cameras, that is easy to obtain because most

[9] *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.

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."[10]

17. Flock's security failures extend beyond the purely technical to encompass operational and administrative procedures as well. Flock's monthly audit reports are subject to public records requests in many jurisdictions. Its audit reports for a given law enforcement agency contain all searches conducted by all Flock users that searched the agency's network and include the unredacted license plate numbers subject to and the rationale for each search. By failing to properly account for public records requests, Flock's audit reports have revealed hundreds of thousands of license plate numbers alongside the sensitive, but often warrantless, searches they were subjected to.[11]

18. Flock has shown a complete disregard for the laws of California. In doing so, it has violated the rights of millions of drivers within the state. Plaintiff seeks to remedy this harm and protect himself and his community from Flock's unlawful information sharing and failure to institute widely accepted industry-standard measures to prevent information sharing by California law enforcement agencies and hacking by threat actors. Plaintiff brings this Complaint alleging violations of SB 34, California's UCL, and California common law.

## PARTIES

19. Plaintiff Jason Hellerman is a natural person and a citizen of the State of California. Plaintiff Hellerman resides in the city of Los Angeles in Los Angeles County, California.

[10] Walicek, *supra* note 5.

[11] Jason Koebler, *Police Unmask Millions of Surveillance Targets Because of Flock Redaction Error*, 404 MEDIA (Jan. 13, 2026), https://www.404media.co/police-unmask-millions-of-surveillance-targets-because-of-flock-redaction-error.

20. Defendant Flock Group, Inc. d/b/a Flock Safety is a corporation formed under the laws of Delaware. Its principal place of business is located in Georgia.

## JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(a)(2) and 28 U.S.C. § 1332(d)(2).

22. This Court has personal jurisdiction over Flock 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, upon information and belief, 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 Californians' vehicles, and regularly interacts with California law enforcement agencies. Plaintiff's claims arise out of and relate to Flock's California contacts.

23. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events giving rise to the claims occurred in this District.

## COMMON FACTUAL BACKGROUND

### I. ALPR Technology.

24. ALPR systems—particularly in their modern form—combine several distinct pieces of technology.[12]

25. At the core of an ALPR system are cameras that take images of license plates. These cameras can be fixed (most often, they are attached to traffic lights or

[12] *Automatic License Plate Readers*, ELEC. FRONTIER FOUND.: ST. LEVEL SURVEILLANCE, https://sls.eff.org/technologies/automated-license-plate-readers-alprs (last visited Jan. 2, 2026) [hereinafter ELEC. FRONTIER FOUND., *Automatic License Plate Readers*].

streetlights) or placed on a vehicle (such as a police cruiser) or trailer that can be towed to an area and parked for an extended period. But the cameras are just the starting point.

26. Images taken by the cameras are uploaded to a central server, usually operated by the cameras' manufacturer, that analyzes the images using a variety of programs, algorithms, and increasingly, AI, focused on different features.

27. The most basic of these programs is optical character recognition ("OCR"). OCR takes many forms but, in essence, algorithmically recognizes and reads characters from an image for use in another document or file. ALPR systems use OCR to read license plates and store the license plate numbers in an easily searchable text format.

28. Modern ALPR systems increasingly leverage various AI technologies to identify and analyze vehicles. For example, Flock uses machine learning to identify a vehicle's make, body type, color, plate state, and other identifiers, including whether it has a roof rack, bumper stickers, etc.[13] Flock calls this identifying information a "Vehicle Fingerprint." Flock even holds a patent for a dynamic surveillance system that can be configured to identify "classes of people (male, female, race, etc.)."[14] While Flock claims in advertising material that it does not capture any personal information or use facial recognition, it certainly conducts some level of analysis of the occupants of the vehicle, providing as an example the ability to search its databases for a "red pickup truck with a dog in the bed."[15] Additionally, recent

[13] *License Plate Readers (LPR): Stop Crime in Its Tracks With Evidence That Drives Action*, FLOCK SAFETY [hereinafter Flock LPR Product Page], https://www.flocksafety.com/products/license-plate-readers (last visited Jan. 2, 2026).

[14] Sys. & Method for Object Based Query of Video Content Captured by a Dynamic Surveillance Network, U.S. Patent No. 11,416,545 B1 (filed Oct. 4, 2020) (issued Aug. 26, 2022), https://patentimages.storage.googleapis.com/77/9a/03/7b3b26499077d4/US11416545.pdf (on file with Hausfeld LLP).

[15] *Book a Demo – Short Form Paid*, FLOCK SAFETY, https://www.flocksafety.com/book-a-demo-short-form-paid (last visited Jan. 6, 2026).

reporting indicates that Flock's ALPR readers, in at least some instances, capture images of people's faces, saving them to a folder separate from the ALPR data.

29. After completing these analyses, ALPR systems use their vast databases to categorize the images and associated data, including location, date, and time. This allows end users to track a particular vehicle's travel history for as long as the manufacturer stores this information. With the advent of AI-powered computing tools, ALPR systems can increasingly form highly accurate conclusions and predictions about where drivers live, work, and visit.

30. Though potentially helpful in criminal investigations, these features when not properly constrained also enable privacy intrusions and abuses of civil liberties.

31. Modern ALPR cameras are distinct from traditional traffic-enforcement cameras (often known as "red light cameras") because ALPR cameras are "crime prevention and investigation tools" used exclusively for domestic surveillance, whereas red light cameras are used exclusively to detect traffic violations, such as speeding and running red lights. Further, "Flock cameras capture every passing vehicle, including license plate, vehicle image, and GPS location, whereas red light cameras only record when a violation occurs. Flock cameras can track vehicles in real-time, whereas red light cameras do not track vehicles continuously."[16]

## II. The History of ALPR Technology.

32. Although ALPR technology has existed in some form since the 1970s, its use in law enforcement has become more effective—and more intrusive—with technological advances in recent decades.

[16] 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.

**A. Early ALPR Technology: The 1970s Through the Early 2000s.**

33. ALPR technology was first developed in England in the late 1970s.

34. But early ALPR cameras, through at least the 1980s and 1990s, were ineffective and not widely adopted.

35. Early ALPR cameras had poor photo resolution and required infrared capabilities to be effective, meaning they could not use off-the-shelf traditional cameras and relied on specialized infrared-enabled models. For example, early ALPR cameras often did not take usable scans when the vehicle was far away, moving at a high speed, or changing lanes. They were also less effective at night or in bad weather, particularly when there was insufficient lighting or cover.

36. Early ALPR cameras could not identify a vehicle with a partially obscured or dirty license plate. They would also be rendered wholly ineffective when a driver made even rudimentary efforts to cover up their vehicle's license plate or make its text unreadable.

37. Early ALPR cameras were also difficult to set up and could only be placed in certain locations due to the need for access to power and maintenance.

38. Early ALPR systems were also unable to take advantage of effective OCR technology, which did not become widely and commercially available until the early 2000s. Disparities in the types of characters used on license plates by different licensing jurisdictions from the 1970s through the 2000s compounded the then-limited effectiveness of OCR technology. Further, gaps between letters and numbers in some jurisdictions' license plates were too narrow for early ALPR systems to recognize the characters.

39. Moreover, early ALPR cameras were—despite these many limitations—very expensive. Local law enforcement agencies did not have the budgets to install a comprehensive network of ALPR cameras.

40. The images captured by early ALPR systems were not as useful because those systems did not have access to computers with enough computing power to

handle high volumes of images. They also were not connected through a high-speed wireless internet network that enabled real-time information sharing.

41. Finally, early ALPR systems did not have access to machine learning, so their ability to identify a vehicle was limited to reading its license plate.

**B. Recent Advances in ALPR Technology.**

42. Beginning in the late 1990s and early 2000s, several advancements made ALPR technology more powerful and effective—and more widely available for local law enforcement agencies. The advent of AI and machine learning in recent years has only compounded this.

43. Advancements in camera lighting technology allow current ALPR systems to obtain high-definition color photos without the need for infrared. Such advancements allow ALPR systems to use off-the-shelf commercial cameras.

44. High-definition digital cameras are now widely available and much less expensive than their earlier counterparts.

45. Modern high-definition cameras permit wide fields of view and great clarity even at long distances and wide angles, as well as for vehicles moving at higher speeds.

46. For instance, Flock claims its ALPRs can capture images of vehicles traveling at up to 100 mph and at distances of up to 75 feet, regardless of lighting.

47. This allows current ALPR cameras to capture images that can be used to clearly identify multiple license plates. Additionally, higher clarity allows ALPR systems to extract details like vehicle make, body type, color, plate state, and other identifiers.

48. Modern high-definition cameras are so small and inexpensive that they can be easily mounted on vehicles like police cruisers. These mobile cameras are equally capable of capturing images useful for ALPR systems.

49. As far as camera hardware has progressed since the 1970s, computer servers have advanced even further, becoming extremely powerful and enabling new

kinds of analyses to be conducted with ALPR images. Advancements in machine-learning algorithms have also made it possible for computers to now identify a vehicle using not just its license plate but also other identifiers, such as bumper stickers, roof racks, and even dents or scratches.

50. The advent of high-speed internet connectivity has enabled live transmission of massive amounts of data from ALPR cameras to central computer systems.

51. Flock itself agrees that its ALPR products are of a different breed than traditional ALPR cameras; it has stated in marketing materials that "Flock Safety delivers more than just license plate information. We've taken license plate reading to the next level by including details on the entire vehicle. Our system captures things like color and type of vehicle. In fact, Flock can identify a temporary paper plate and even a vehicle where there is no plate present."[17]

52. And Flock doesn't just collect extensive data about individuals' movements—it analyzes that data to find patterns, draw conclusions, and even make predictions.

53. In 2025, Flock announced a suite of new capabilities through its "Investigations Manager" product, each aimed at proactively analyzing movement patterns and related data to flag vehicles as potentially suspicious. 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.'"[18]

---

[17] *Which Automatic License Plate Reading (ALPR) Camera is Best for My Needs?*, FLOCK SAFETY: BLOG (Apr. 3, 2019), https://www.flocksafety.com/blog/which-license-plate-reader-security-camera-is-best-for-my-needs.

[18] 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), 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.

54. The new capabilities Flock touts include a "Multi-State Insights feature" that alerts law enforcement "when suspect vehicles have been detected in multiple states"; "a 'Linked Vehicles' or 'Convoy Search'" which allows "police to 'uncover vehicles frequently seen together,' putting it squarely in the business of tracking people's associations, and a 'Multiple locations search,' which promises to 'Uncover vehicles seen in multiple locations.'"

55. As noted in recent reporting by the ACLU, each of these features "are variants on the same theme: using the camera network not just to investigate based on suspicion, but to *generate suspicion* itself."[19]

56. Bypassing warrants and laws designed to protect personal liberties, modern ALPR systems seek to track, catalogue, and analyze every turn of every driver's route, looking for "suspicious activity" to generate new business—not safer communities.[20]

57. Leveraging and combining these technological improvements, ALPR systems have advanced from limited, easily tricked devices to sophisticated national networks enabling law enforcement agencies to track—virtually in real time—any vehicle on the road, actively analyzing driving patterns using black-box algorithms to decide whether to act on potentially "suspicious" activity.

58. 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 of Californians.

## III. Senate Bill 34.

59. In 2015, California regulated and restrained the use of ALPR and the sharing of data captured by ALPR systems. Cal. Civ. Code §§ 1798.90.5 *et seq.*

60. In enacting the new ALPR law, the California Legislature emphasized numerous privacy concerns implicated by the use of this technology:

---

[19] *Id.*
[20] *Id.*

> 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.[21]

61. To achieve this goal, the ALPR law mandates that ALPR operators, such as Flock, and end users, such as law enforcement agencies, comply with three basic but essential requirements:

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

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

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.

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).

62. ALPR operators must comply with two additional requirements to ensure consumer privacy and protect against unauthorized access:

d. *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).

e. *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).

63. Importantly, 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).

64. "Public agency" for purposes of SB 34 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).

65. The California AG has interpreted this plain text of SB 34 (including, crucially, §§ 1798.90.5(f) & 1798.90.55(b)) as permitting sharing of ALPR data only with other California state and local agencies.[22]

66. The California AG emphasized:

> 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, SB 34 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

[22] 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.

maintain ALPR information collected from multiple databases and/or public agencies.[23]

67. Likewise, the California AG has clarified that, under SB 34, "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.'"[24]

68. SB 34 does not contain any exceptions permitting the sharing of ALPR data with federal or out-of-state agencies for any purpose. Consistent with the California AG's interpretation of SB 34, any such sharing is clearly prohibited by SB 34's plain text.

69. An individual harmed by a violation of SB 34—"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 (emphasis added).

## IV. Flock Collects Extensive Reams of Data.

70. 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.

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

---

[23] *Id.*

[24] *Id.* (emphases added) (quoting Cal. Civ. Code §§ 1798.90.51(a)–(b); 1798.90.53(a)–(b)).

72. 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.

73. Flock ALPR cameras collect at least the following information:

a. License plate image;

b. Vehicle image;

c. Vehicle characteristics (e.g., color, make, other visual details);

d. License plate number;

e. License plate state;

f. Date;

g. Time; and

h. Camera location.

74. The below image from a Flock presentation shows the type of information captured and stored by Flock's ALPR cameras, including that the SUV belongs to a "non resident" and was "[s]een three times in the last 30 days."


75. An individual Flock camera can take thousands of license plan scans; for example, Oak Park, Illinois, has just eight Flock cameras that collectively take more than 300,000 scans each month.[25]

76. The Los Angeles County Sheriff's Department alone operates ***476*** Flock ALPR cameras.[26]

77. The San Francisco Police Department and Oakland Police Department are reported to collectively operate hundreds of Flock cameras.[27]

---

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

[26] 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.

[27] 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*],

78. More than 200 California law enforcement agencies collect and use images captured by Flock ALPR cameras.[28]

79. Flock boasts that its cameras are used by more than 4,800 law enforcement agencies nationwide.[29] Thus, Flock brags that it has the nation's largest fixed ALPR network: "With billions of monthly plate reads, Flock connects communities, businesses and law enforcement in a shared network[.]"[30]


80. 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

---

https://sfstandard.com/2025/07/14/oakland-san-francisco-ice-license-plate-readers (last updated July 17, 2025, at 18:07 PT)

[28] Rachel Myrow, *California Cities Double Down on License-Plate Readers as Federal Surveillance Grows*, KQED (Dec. 18, 2025), 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).

[29] *National LPR Network: Real-Time Vehicle Leads, Nationwide*, FLOCK SAFETY, https://www.flocksafety.com/products/national-lpr-network (last visited Jan. 2, 2026).

[30] Flock LPR Product Page, *supra* note 1313.

> 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.[31]

81. Flock's ALPR cameras do not just scan license plates. They also identify the color and make of the vehicle and provide other identifying information such as bumper damage or a roof rack, as seen in the following image on Flock's website.[32]


82. Flock's AI-powered system can also provide information about how often a particular vehicle is seen at a certain location or on a certain route; it can even predict future activity for a specific vehicle based on past data about that vehicle.

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

[32] The image is taken from Flock's website. ("roof rack" as an example is from the Flock Evidence Policy. *See Flock Evidence Policy*, FLOCK SAFETY, https://www.flocksafety.com/legal/flock-evidence-policy (last updated July 22, 2025)).

83. Consequently, "ALPR systems collect and store location information about drivers that can be built into a database that reveals sensitive details about where individuals work, live, associate, worship, seek medical care, and travel."[33]

84. In May, Flock announced the development of a new product ("Nova") that would integrate its ALPR systems with data-broker lookups—and even stolen personal information from data breaches—to give law enforcement agencies even more invasive ways to track individuals (without procuring a warrant),[34] demonstrating that Flock was willing to enable even greater (and even more highly offensive) invasions of privacy in its pursuit of profits.

85. But once reporting on the announcement of the capabilities of the Nova product spread, prompting substantial negative response from the public, Flock abandoned (at least for now) its plan to integrate information obtained from data breaches into Nova.[35] "In a muddled and evasive statement, Flock seemed to be attempting to simultaneously deny that it had ever used such data while also promising that it would stop using it going forward."[36]

---

[33] Letter from Jennifer Pinsof, Staff Att'y, Elec. Frontier Found.; Matt Cagle, Senior 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 ELEC. FRONTIER FOUND., *Automatic License Plate Readers*, *supra* note 1212; *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).

[34] 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.

[35] Joseph Cox & Jason Koebler, *Flock Decides Not to Use Hacked Data in People Search Tool*, 404 MEDIA (May 30, 2025), https://www.404media.co/flock-decides-not-to-use-hacked-data-in-people-search-tool.

[36] Walicek, *supra* note 5 (citing Thad Reuter, *Flock Safety Pushes Back on Data*

## V. Flock Has Violated SB 34 and Facilitated Routine Violations of SB 34 by California Law Enforcement Agencies.

### A. ICE, CBP and Out-of-State Law Enforcement Agencies Routinely (and Unlawfully) Obtain Access to Flock's ALPR Data from California Law Enforcement Agencies.

86. Flock ALPR data is frequently used in contravention of SB 34 by federal law enforcement agencies, including Immigration and Customs Enforcement ("ICE") and Customs and Border Protection ("CBP"). Local police, disregarding the guidance from the California AG regarding the permissible uses of ALPR under SB 34, readily perform lookups in Flock's AI-supported ALPR system for "immigration" related searches, for CBP, for the U.S. Department of Homeland Security Investigations department, and as part of other ICE investigations, giving these federal agencies side-door access to a tool they currently do not have a formal contract for.[37]

87. An April 2025 California Highway Patrol search of 845 ALPR systems, including Flock systems, was labeled "ICE case."[38]

88. The Riverside County Sheriff's Department has stated the reason for searches as "HSI," a reference to ICE's Homeland Security Investigations unit.

89. An investigation by the San Francisco Standard found that San Francisco and Oakland police officers repeatedly violated SB 34 by sharing data from ALPR cameras with federal law enforcement, including ICE and the Federal Bureau of Investigation ("FBI").[39]

---

*Breach Product Criticism*, GOV'T TECH.: GOVTECH BIZ (May 30, 2025), https://www.govtech.com/biz/flock-safety-pushes-back-on-data-breach-product-criticism).

[37] 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 Network*], https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows.

[38] 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.

[39] Chien, *SF/Oakland ICE LPRs*, *supra* note 272727.

90. Likewise, in apparent contravention of SB 34, the Los Angeles Police Department, as well as Sheriff's Departments in Los Angeles, San Diego, and Orange Counties, searched license plate readings contained in Flock's database on behalf of ICE and CBP.[40]

91. A 2023 analysis by the Electronic Frontier Foundation found that at least 71 California law enforcement agencies had violated SB 34 that year.[41]

92. This unlawful conduct is not limited to cooperation between California and federal law enforcement agencies. 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 for investigations to assist ICE.[42]

93. The California AG has interpreted SB 34 as prohibiting the sharing of California ALPR data with federal agencies and out-of-state law enforcement agencies. To ensure compliance with this interpretation, the California AG's office has initiated enforcement actions against at least 20 California law enforcement agencies.

94. The California AG has become more aggressive in seeking to curtail violations of SB 34. Though the California AG's office had previously only issued notices of violation to California law agencies, it recently instituted legal proceedings against the City of El Cajon.[43]

---

[40] Johnson & Al Elew, *supra* note 3.

[41] Press Release, Elec. Frontier Found., Civil Liberties Groups Demand California Police Stop Sharing Drivers' Location Data With Police In Anti-Abortion States (May 25, 2023), https://www.eff.org/press/releases/civil-liberties-groups-demand-california-police-stop-sharing-drivers-location-data.

[42] Chien, *SFPD ICE Data Sharing*, *supra* note 2.

[43] Petition for Writ of Mandate & Complaint for Injunctive & Declaratory Relief, California *ex rel*. Bonta v. City of El Cajon, No. 25CU053437C (Cal. Super. Ct. filed Oct. 3, 2025).

95. Nevertheless, some California law enforcement agencies continue to violate SB 34. For example, the Riverside County Sheriff's Department continued to perform ALPR searches on behalf of federal agencies even after being informed repeatedly that its practice of sharing ALPR with federal agencies "violates state law."

96. Flock was required to, but did not, implement and maintain an adequate policy to prevent unlawful information sharing, including that which continues to be undertaken by the Riverside County Sheriff's office.

97. California law enforcement agencies' continued routine violations of SB 34, 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.

98. Had Flock implemented required and reasonable measures—such as requiring use of MFA, preventing interstate and state–federal sharing of California ALPR data, ensuring its ALPR cameras were protected against security flaws that allowed surveillance feeds to be readily broadcast online, and redacting sensitive data in files subject to public records requests—it would have complied with SB 34 itself as well as prevented California law enforcement agencies from violating SB 34. This is well within Flock's capabilities.

99. But Flock chose not to do so. "Flock Safety—the company that sells the ALPR systems popular in California and across the U.S.—makes it easy for police to share data."[44]

100. As one example, "[o]nce a department allows another agency to access its system, the outside agency can search the data without needing approval each time."[45] Likewise, users can query multiple networks simultaneously: Searches of Oakland's ALPR data were found to reach hundreds of other networks at once.

[44] Chien, *California cops are breaking surveillance laws*, *supra* note 3838.
[45] Chien, *SFPD ICE Data Sharing*, *supra* note 2.

101. Worse still, some agencies were themselves unaware that Flock was allowing their ALPR databases to be used in violation of SB 34. Indeed, 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" and apparently admitted that "[t]he searches violated two laws," including SB 34.[46]

102. 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 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]

103. Flock, then, not only enabled many California law enforcement agencies to actively and willfully violate SB 34—it also effectively turned others into violators of SB 34 whether they knew it or not.

104. This violation of trust and others like it have led multiple localities to cut ties with Flock; most recently, the Santa Cruz City Council voted 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."[48]

105. At the January 13 meeting where the City Council ultimately decided to end its contract with Flock, Councilmember Susie O'Hara stated: "Flock has made

[46] Joan Hammel, *Eyes in the Sky: Santa Cruz discloses violations involving ALPRs, launches review of camera use*, GOODTIMES (Nov. 26, 2025), https://www.goodtimes.sc/santa-cruz-alpr-violations-review-flock-safety.

[47] *Id.*

[48] 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/.

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."[49]

106. After reporting on Flock's extensive violations gained traction, Flock announced and implemented a series of technical changes, tacitly conceding that its previous practices violated SB 34. As detailed below, however, these changes still do not bring Flock into compliance.

107. Flock's continued disregard of SB 34 has enabled a nationwide network of unlawful law enforcement coordination and information sharing.

**B. Flock Did Not Implement and Maintain an Adequate Policy to Prevent Unlawful Information Sharing.**

108. SB 34 requires ALPR operators like Flock to implement and maintain a policy sufficient to ensure their ALPR system will be used exclusively for permissible purposes.

109. Flock has an ALPR policy, which was last updated on November 13, 2025.[50]

110. In its Terms and Conditions, Flock defines "Permitted Purpose" as "legitimate public safety and/or business purpose, including but not limited to the awareness, prevention, and prosecution of crime; investigations; and prevention of commercial harm, *to the extent permitted by law*."[51]

111. But Flock's policy did not even arguably provide sufficient protection against unauthorized access to and sharing of California ALPR data until June 2025, after Flock removed all cameras deployed in California from its national lookup system. Until that time, federal or out-of-state law enforcement agents searching for

---

[49] *Id.*

[50] *License Plate Reader Policy*, FLOCK SAFETY [hereinafter Flock LPR Policy], https://www.flocksafety.com/legal/lpr-policy (last updated Nov. 13, 2025).

[51] *Terms and Conditions*, FLOCK SAFETY, https://www.flocksafety.com/legal/terms-and-conditions (last updated Dec. 19, 2025) (emphasis added).

a license plate in Flock's system would have unlawfully been presented with relevant results in California, even if they did not understand the implications.[52]

112. Though these system changes are a step in the right direction, Flock is still not in compliance with SB 34.

113. Even with Flock's system changes, officers from the San Francisco and Oakland Police Departments continued sharing California Flock ALPR data with at least seven federal agencies.[53]

114. Additionally, "many of the same [California] law enforcement agencies" that were running illegal immigration-related searches before being exposed by reporting in July 2025 have since "run hundreds of searches with no case number referenced and no reason given to the search beyond 'investigation,' raising concerns that the sharing could be ongoing."[54]

115. Flock still disclaims its obligation to ensure compliance with SB 34, maintaining that its "[c]ustomers choose whether to share LPR data with other customers in accordance with their laws and policies."[55]

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

117. 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.

---

[52] Joseph Cox & Jason Koebler, *Flock Removes States From National Lookup Tool After ICE and Abortion Searches Revealed*, 404 MEDIA (June 25, 2025), https://www.404media.co/flock-removes-states-from-national-lookup-tool-after-ice-and-abortion-searches-revealed.

[53] Chien, *SF/Oakland ICE LPRs*, *supra* note 2727.

[54] Jesse Kathan, *Dozens of California agencies shared license plate data with feds, Santa Cruz records show*, SANTA CRUZ LOCAL (Dec. 9, 2025), https://santacruzlocal.org/2025/12/09/dozens-of-california-agencies-shared-license-plate-data-with-feds-santa-cruz-records-show.

[55] Flock LPR Policy, *supra* note 3.

118. For example, federal law enforcement agencies have been increasingly marshalled to support mass deportations at odds with California law (including SB 54, codified at Cal. Stats. 2017, Ch. 495), and public policy.

119. And 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 self-administered an abortion.[56] Abortion criminalization is also at odds with California law (including laws such as AB 1242, codified at Cal. Stats. 2022, Ch. 627, which prohibits state and local agencies from providing abortion-related information to out-of-state agencies) and public policy.

### C. Flock's Press Releases and Public Relations Materials Confirm that It Has Violated SB 34.

120. Flock has made several public statements in which it tacitly acknowledged that it violated SB 34 but attempted to shift its own burdens to law enforcement agencies in order to avoid acknowledging its own responsibilities under the law.

121. For example, in a June 19, 2025, blog post announcing the removal of California from Flock's national lookup service after media backlash, Flock CEO and

[56] 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.").

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." [57]

122. In a section in the same blog post, titled "Local Autonomy in working with Federal Agencies," 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."[58]

123. Langley misstated the situation: The burden of compliance rests not just on law enforcement agencies but on Flock and other ALPR operators, too. Flock's policy changes at most brought Flock closer to (but certainly not within) compliance with SB 34, which 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."

124. Similarly, 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."[59] This 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 SB 34. In other words, Flock's recent 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 SB 34.

---

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

[58] *Id.*

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

125. Flock has implicitly admitted its noncompliance in communications beyond those written by Langley. For example, Flock's User Guide published in August 2023 instructed users that their agency could enable national lookups, which allowed all law enforcement agencies in the country with the same feature enabled to search that agency's ALPR system as well, with no limitation on California law enforcement agencies. Flock's user interface presented this option without informing law enforcement agency users within California that such a setting would be unlawful.[60]

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

126. Additionally, Flock fails to maintain the reasonable security procedures and practices required by SB 34.

127. For example, Flock does not require MFA. Requiring MFA is a basic, reasonable measure used to secure virtually any important online service, including the Federal Courts' PACER filing system.

128. Flock's failure to require MFA, among other flaws, *supra* ¶ 10–11, is one reason Russian hackers are able to sell functional Flock logins on the dark web.[61]

129. Additionally, as above, GainSec recently revealed **fifty-one (51)** vulnerabilities in Flock's hardware and software offerings.[62] These vulnerabilities included critical security issues such as the ability to gain complete access to and control over a Flock camera through simple physical access. This vulnerability is particularly serious for devices deployed exclusively in public.

---

[60] Koebler & Cox, *ICE Taps into Network*, *supra* note 37373737 (citing FLOCK SAFETY, FLOCK SAFETY USER GUIDE AUGUST 2023, at 3 (2023), https://www.documentcloud.org/documents/24172417-flocksafetyuserguideaug2023).

[61] Walicek, *supra* note 5.

[62] Jon Gaines, GainSec, Examining the Security Posture of an Anti-Crime Ecosystem (2025), https://zenodo.org/records/17529424.

130. Worse still, Flock left unprotected troves of its testing data as well as live feeds from many of its Condor cameras, which allowed journalists to watch live as Flock's devices surveilled drivers and pedestrians going about their lives.[63] These feeds could be accessed with minimal technical sophistication. Several of the unsecured feeds were from cameras in California.

131. Most egregious of all, Flock's audit reports—which, again, are subject to public records requests—have led law enforcement agencies to leak hundreds of thousands of license plate numbers alongside the reason the agencies searched for them.[64] In response, rather than providing a specific audit report for public records requests or redacting sensitive information by default, Flock has removed wholesale the ability to view officer names and license plate numbers in audit reports.[65] This both makes the audit reports insufficient under Cal. Civ. Code § 1798.90.52(a) and demonstrates that Flock has no interest in "mak[ing] compliance easier"[66] for its customers—it is merely making poor, ad hoc decisions in a slipshod attempt at damage control amid mounting public scrutiny.

132. Flock's leaking of hundreds of thousands of unredacted license plates, the fifty-one vulnerabilities exposed by GainSec, and Flock's failure to require MFA clearly demonstrate that Flock does not maintain reasonable security procedures and practices, thereby providing insufficient protection for the privacy and civil liberties of drivers in California.

/ / /

/ / /

/ / /

/ / /

[63] Koebler, *supra* note 7.
[64] *Id.*
[65] *Id.*
[66] Langley, *supra* note 57.

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

### A. Law Enforcement Agencies Have Used Flock for Discriminatory Purposes.

133. Laws like SB 34 exist in part because ALPR systems are not simply neutral tools to enhance public safety. On the contrary, they are increasingly being used to aid discriminatory policing practices in low-income neighborhoods and in areas with significant populations of Black and Latino residents.

134. Across the country, ALPR tools enable and amplify racial profiling by embedding longstanding policing biases into cutting edge surveillance technologies.

135. "As with other surveillance technologies, police often disproportionately deploy license plate readers in communities experiencing poverty and historically overpoliced communities of color, regardless of crime rates."[67]

136. When police run a search through the Flock Safety network, which links thousands of ALPR systems, they are prompted to provide a reason and/or case number for the search.

137. Data from these searches reveals that Flock's sophisticated surveillance systems expand discriminatory police practices by allowing their use across an unprecedented geographic area and through access to information that would

[67] EFF–ACLU Joint Letter, *supra* note 3333, at 2 (citing Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, ELEC. FRONTIER FOUND. (Jan. 21, 2015), 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").

otherwise require search warrants or other types of particularized, reasonable suspicion.

138. For example, more than 80 law enforcement agencies across the United States have used pejorative terms to describe Romani people when searching the nationwide Flock Safety ALPR network, according to Flock audit logs obtained and analyzed by the Electronic Frontier Foundation.[68]

139. In May 2025, for example, officers from the Sacramento Police Department ran at least six searches for a racial slur directed at Romani people; these searches covered 468 networks, representing 12,885 different ALPR devices.[69]

140. Likewise, in February and May 2025, the Irvine Police Department ran eight searches using the term "roma" in the "reason" field. The searches covered 1,420 networks, representing 29,364 different ALPR devices.

141. 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.[70]

142. As above, SB 34 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.

143. Moreover, 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.

---

[68] 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.

[69] *Id.*

[70] FREEDOM TO THRIVE OAK PARK, *supra* note 252525.

### B. ALPR Data Has Been Shared with Out-of-State Jurisdictions, Threatening Access to Abortion Access and Gender-Affirming Care in California.

144. ALPR information is even more vulnerable to exploitation and weaponization against those seeking, providing, and facilitating access to abortion services.[71]

145. Law enforcement agencies in jurisdictions that limit or prohibit abortion access can use driver location information collected by California-based ALPRs to closely monitor clinics that provide abortion services, the vehicles seen around the clinics, and the movements of patients and providers at the clinics.

146. Given those jurisdictions' plans to criminalize and prosecute those who seek or assist in facilitating out-of-state abortions, sharing Flock ALPR information with out-of-state law enforcement agencies threatens those obtaining, providing, or otherwise facilitating abortion-related services in California.[72]

147. The same risks are true for people seeking gender-affirming care in California, given some states' efforts to criminalize and prosecute those who go to another state to receive such medical care.[73]

---

[71] EFF–ACLU Joint Letter, *supra* note 3333, at 2 (citing Johana Bhuiyan, *How expanding web of license plate readers could be 'weaponized' against abortion*, THE GUARDIAN (Oct. 6, 2022, at 11:00 BST), https://www.theguardian.com/world/2022/oct/06/how-expanding-web-of-license-plate-readers-could-be-weaponized-against-abortion).

[72] *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.

[73] *See, e.g.*, Maya Yang, *Idaho bill that criminalizes medical trans youth treatments passes house*, THE GUARDIAN (Mar. 10, 2022, at 12:16 ET), https://www.

148. As with use and sharing of ALPR data for discriminatory purposes, the use and sharing of ALPR data against those seeking abortion services or gender-affirming care heightens the highly offensive nature of the widespread collection, storage, use, and sharing of ALPR data generally.

**PLAINTIFF'S INDIVIDUAL EXPERIENCE**

149. Plaintiff Jason Hellerman lives in Los Angeles, Los Angeles County, California.

150. Plaintiff Hellerman currently owns and drives a navy-blue Mazda CX-3.

151. Plaintiff Hellerman regularly drives in Los Angeles County.

152. Plaintiff Hellerman drives for work four to five times a week, including to locations in Santa Monica, Burbank, and Downtown Los Angeles.

153. The fastest driving routes to locations Plaintiff Hellerman must regularly travel to for work would require him to drive on specific sections of Olympic Boulevard, a major arterial thoroughfare in Los Angeles.

154. Plaintiff Hellerman witnessed the installation of Flock cameras on Olympic Boulevard, an experience that informed his decision to avoid specific sections of Olympic Boulevard.

155. To avoid Flock cameras, Plaintiff Hellerman avoids driving on these specific sections of Olympic Boulevard whenever possible, particularly on his way back home.

156. Plaintiff Hellerman's decision to avoid Olympic Boulevard regularly results in the addition of 10 to 15 minutes per driving trip he must make for work. Given that he drives for work four to five times per week and usually avoids Olympic Boulevard on at least his return trip, he generally drives more than an hour longer than necessary per week due to Flock cameras.

---

theguardian.com/us-news/2022/mar/10/idaho-bill-trans-youth-treatment-ban-passes-house.

157. Plaintiff Hellerman has experienced emotional distress, including anxiety about Flock cameras capturing images of his car and his young child. Plaintiff Hellerman is careful about how he and his family share images of their young child on social media and is fearful of Flock potentially using or misusing images of him, his family, and his child, including by improperly sharing or failing to adequately secure and protect such data.

158. Plaintiff Hellerman reasonably fears how Flock, federal agencies, and out-of-state law enforcement agencies use, store, and protect California ALPR data.

159. Plaintiff Hellerman's frequent use of alternative, longer routes has increased the amount of energy he consumes while driving and the amount of time it takes him to go about his daily life activities. He is also forced to spend more time searching for these Flock-less routes.

## CLASS ACTION ALLEGATIONS

160. **Class Definitions**: Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3) individually and on behalf of the Class, defined as follows:

> All persons whose license plate data was collected by Defendant Flock in the State of California using an automatic license plate reader operated by Defendant Flock and was accessible by, and thus disclosed to, federal law enforcement agencies, out-of-state law enforcement agencies, or the public at large on or after January 15, 2022 (the "Class Period").

161. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest and its officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released;

(5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

162. Members of the Class ("Class Members") are ascertainable. Flock maintains a database of scanned license plates. License plates are evidence of state of residence. When an agency searches ALPR data from Flock, it saves a log entry. Each entry includes the requesting agency, reason for the request, time of submission, and number of Flock networks included in the search. The Class will include the owners of any license plate scanned in a California network that was searched by federal or out-of-state law enforcement agencies and/or leaked in an audit log in response to a public records request.

163. **Numerosity**: The exact number of Class Members is unknown and not available to Plaintiff at this time, but individual joinder is clearly impracticable. On information and belief, Flock has photographed the license plates and time-stamped geolocation data of tens of millions of drivers in California, and Flock's policies have permitted unauthorized sharing of millions of drivers' ALPR data with federal agencies, out-of-state law enforcement agencies, and the public at large. As above, Class Members can be identified through Flock's records.

164. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, which predominate over any questions that may affect individual Class Members. These include—but are not necessarily limited to—the following:

(a) Whether Flock implemented and maintained a policy that complied with SB 34;

(b) Whether Flock complies with the Notice, Privacy, Security, Audit, and Proper-Use Requirements set forth in SB 34;

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

(d) Whether Flock's policy permitted 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 federal agencies and out-of-state law enforcement agencies;

(f) Whether Flock knew or should have known that its inadequate policy facilitated unauthorized sharing of Class Members' ALPR data with federal agencies and out-of-state law enforcement 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 SB 34 and California common law.

165. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in data privacy litigation, complex litigation, and class actions. Plaintiff's claims are representative of the claims of the other members of the Class; that is, Plaintiff and Class Members each sustained damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the Class.

166. **Predominance and Superiority:** Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all members of the Class is impracticable. Individual litigation would not be preferable to a class action because it would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties

and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

167. Plaintiff reserves 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**
**Unlawful Sharing of ALPR Data – Cal. Civ. Code §§ 1798.90.5 *et seq.***
**(On Behalf of Plaintiff and the Class)**

168. Plaintiff incorporates the foregoing factual allegations as if fully set forth herein.

169. This cause of action is brought under Cal. Civ. Code §§ 1798.90.5 *et seq.*

170. Plaintiff brings this count against Flock individually and on behalf of the Class.

171. Flock operates an ALPR system that collects photographs of license plate numbers, together with other physical features of as well as the location, time, and date of Plaintiff's and the Class's vehicles.

172. On information and belief, Flock is not a transportation agency acting subject to Cal. Streets & Highways Code § 31490.

173. Flock is thus an "ALPR operator" under Cal. Civ. Code § 1798.90.5(c) because it operates an ALPR system.

174. In addition (or in the alternative), Flock is an "ALPR end-user" under Cal. Civ. Code § 1798.90.5(a) because it accesses or uses an ALPR system, including but not limited to its use of ALPR footage to train its AI algorithms.

175. California law prohibits Flock from accessing or using ALPR information unless it complies with the Notice, Privacy, Security, Audit, and Proper-Use Requirements defined above.

176. On information and belief, Flock deliberately collected Plaintiff's and the Class's ALPR information and disclosed that information to its law enforcement

clients, allowing them to identify physical characteristics of, movement patterns of, and locations visited by Plaintiff's and Class Members' vehicles, as well as potentially other identifying information.

177. SB 34 requires ALPR operators to "[m]aintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure." *Id.* § 1798.90.51(a).

178. SB 34 also requires ALPR operators to "[i]mplement 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) (emphasis added).

179. Among other requirements, this policy must include "[a] description of how the ALPR system will be monitored to ***ensure*** the security of the information and ***compliance with applicable privacy laws***." *Id.* § 1798.90.51(b)(2)(C) (emphases added).

180. Under SB 34, ALPR operators must also "require that ALPR information only be used for the authorized purposes described in the usage and privacy policy required by subdivision (b) of Section 1798.90.51"—in other words, **ALPR operators in California must *require* that all uses of ALPR information comply with SB 34.** *See id.* § 1798.90.52(b).

181. SB 34 prohibits public agencies from "sell[ing], shar[ing], or transfer[ing] ALPR information, except to another public agency." *Id.* § 1798.90.55(b).

182. "Public agency" 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).

183. Among other security failures, Flock did not require MFA for access to or searches of its ALPR database. Flock's unreasonable security practices were

demonstrated by a researcher's recent exposure of fifty-one (51) distinct vulnerabilities in its hardware and software.

184. Flock did not implement a policy that required use of reasonable security measures or technological tools to prevent unlawful sharing of Plaintiff's and Class Members' information with federal agencies and out-of-state law enforcement agencies.

185. 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 SB 34.

186. 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 SB 34.

187. Flock thus failed to ensure "respect for individuals' privacy and civil liberties" as well as "the security of the information and compliance with applicable privacy laws"—as relevant here, SB 34. *See* Cal. Civ. Code. §§ 1798.90.51(b)(1), (b)(2)(C). These outrageous failures are highly offensive to a reasonable person, amount to gross negligence, and constitute willful, wanton, and reckless indifference to Plaintiff's and Class Members' rights.

188. Plaintiff and the Class have been harmed by Flock's conduct because their private and sensitive personal information has been insufficiently protected and improperly shared with federal agencies and out-of-state agencies without notice or their consent.

189. Flock is therefore liable to each Class Member under SB 34 for actual damages, but not less than liquidated damages of $2,500.

190. Flock's violation of SB 34 was willful or in reckless disregard of the law; accordingly, punitive damages are appropriate.

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

191. Plaintiff incorporates the foregoing factual allegations as if fully set forth herein.

192. Plaintiff brings this cause of action individually and on behalf all other class members.

193. California Business & Professions Code Section 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising."

194. Plaintiff alleges a claim under the unfair and unlawful prongs of the UCL.

195. Flock's conduct constitutes "unfair" business acts and practices within the meaning of the UCL, in that its conduct was injurious to Plaintiff and Class Members, offended public policy, and was unethical and unscrupulous. Flock's violation of Plaintiff and Class Members' privacy and civil liberties resulted in injuries to them.

196. Flock's conduct was unfair because it knew or should have known that it was collecting and sharing sensitive private information and continued to do so anyway despite knowing about the consumers' privacy rights and the harms that could result by disseminating such information to law enforcement agencies including, but not limited to, ICE, CBP and other law enforcement agencies outside of California.

197. Plaintiff also alleges a violation under the "unlawful" prong of the UCL because Flock's conduct violated SB 34 and Cal. Civ. Code. §§ 1798.90.51(b)(1), (b)(2)(C).

198. Plaintiff 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.

199. Plaintiff seeks an injunction prohibiting Flock's ongoing violations under the UCL.

**COUNT III**
**Negligence**
**(On Behalf of Plaintiff and the Class)**

200. Plaintiff incorporates the foregoing factual allegations as if fully set forth herein.

201. This cause of action is brought under the common law of California.

202. Plaintiff brings this count against Flock individually and on behalf of the Class.

203. Flock has a duty to prevent unauthorized information sharing and maintain reasonable and adequate information- and data-security practices.

204. Flock's duty is demonstrated by SB 34.

205. Flock breached that duty by violating SB 34—allowing federal and out-of-state law enforcement agencies access to California ALPR data and failing to maintain reasonable and adequate information- and data-security practices.

206. Plaintiff 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 Plaintiff 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.

207. Flock's conduct proximately caused Plaintiff's and the Class's injuries.

208. Flock's failure to limit ALPR information-sharing and maintain reasonable and adequate information- and data-security practices was precisely the kind of conduct SB 34 was designed to prevent.

209. Plaintiff and the Class are the class of persons SB 34 is intended to protect—drivers within California whose data is subject to ALPR collection.

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

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

212. There is no justification or excuse for Flock's violation of SB 34.

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

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

214. An order certifying the Class as defined above, appointing Plaintiff as the representative of the Class, and appointing his counsel as Class Counsel;

215. An order declaring that Defendant's actions, as set out above, violate Cal. Civ. Code §§ 1798.90.5 *et seq.* and California common law;

216. An injunction requiring Defendant to cease all unlawful activities;

217. An award of liquidated or actual damages (whichever is higher), punitive damages, costs, and attorneys' fees under the applicable law including Cal. Code Civ. Pro. § 1021.5; and

218. Such other and further relief that the Court deems reasonable and just.

## JURY TRIAL DEMANDED

Plaintiff requests a trial by jury of all claims that can be so tried.

Dated: January 17, 2026

**PEARSON WARSHAW, LLP**
By: */s/ Daniel L. Warshaw*
Daniel L. Warshaw

Daniel L. Warshaw (CA Bar No. 185365)
Matthew A. Pearson (CA Bar No. 291484)
dwarshaw@pwfirm.com
mapearson@pwfirm.com
**PEARSON WARSHAW, LLP**
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

Renner K. Walker (CA Bar No. 295889)
Steven M. Nathan (CA Bar No. 153250)
Gisela Rosa*
Jacob Leiken*
rwalker@hausfeld.com
snathan@hausfeld.com
zrosa@hausfeld.com
jleiken@hausfeld.com
**HAUSFELD LLP**
33 Whitehall Street, 14th Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

James J. Pizzirusso*
Ida Abhari (CA Bar No. 346569)
jpizzirusso@hausfeld.com
iabhari@hausfeld.com
**HAUSFELD LLP**
1201 17th Street NW, Suite 600
Washington, DC 20036
Telephone: (202) 540-7200
Facsimile: (202) 540-7201

*Attorneys for Plaintiff and the proposed Class*
**pro hac vice forthcoming*