Ramzi Abadou (SBN 222567)
LAW OFFICE OF RAMZI ABADOU
79 Woodland Ave.
San Francisco, California 94117
Telephone: (415) 231-4313
rabadou@gmail.com

Counsel for Michael Moore and the Putative Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

MICHAEL MOORE, individually and on behalf of a class of all others similarly situated,

Plaintiff,

v.

THE CITY AND COUNTY OF SAN FRANCISCO and THE SAN FRANCISCO POLICE DEPARTMENT,

Defendants.

Case No. 3:25-cv-11011-SK

AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

CLASS ACTION

JURY TRIAL DEMANDED

"*Big Brother is watching you.*"[1]

I. PRELIMINARY STATEMENT

1. Plaintiff Michael Moore alleges the following based upon personal knowledge with respect to himself and, with respect to all other matters, the investigation of Counsel.

2. Counsel's investigation included a review and analysis of, *inter alia*: (i) regulatory filings and policies issued and disseminated by the City and County of San Francisco (the "City") and the San Francisco Police Department ("SFPD") (together "Defendants"); (ii) press releases, regulatory and contractual materials, media statements and marketing presentations issued and disseminated by Defendants; and (iii) investigative and media reports concerning automated license plate readers ("ALPRs"). Plaintiff believes that substantial additional evidentiary support exists for the allegations set forth herein after a reasonable opportunity for discovery.

3. Plaintiff asserts claims under: (i) California Senate Bill 34 ("S.B. 34"), which prohibits the sharing of ALPR information with out-of-state law enforcement agencies and provides other ALPR-related privacy protections, Civ. Code § 1798.90.5 *et seq*.; and (ii) the Fourth Amendment to the United States Constitution pursuant to 42 U.S.C. § 1983, alleging that Defendants have deprived and are depriving him and all similarly situated class members of their privacy rights.[2]

Summary of Allegations

4. This civil rights Action seeks to curtail Defendants' unconstitutional ALPR surveillance program in San Francisco.

5. The automobile has become the primary mode of transportation in the United States. Each year, more than 250 million registered automobiles travel the nation's public roads, including more than 15 million registered in California. The residents of San Francisco rely on their cars to travel

---

[1] George Orwell, "*1984*"

[2] The Honorable Chief District Court Judge Mark S. Davis denied defendants' motion to dismiss under facts and law virtually identical to those pled here. *See Schmidt et. al v. City of Norfolk et al*., Civil Action No. 2:24cv621 (E.D. Va. Feb. 5, 2025).

to and from work, visit their friends and family and to carry out everyday tasks. Consequently, knowing an individual's car location and associations can easily enable someone to pinpoint the individual's location and gain insight into their movements and assembly patterns.

6. ALPR technology is a powerful surveillance tool that Defendants are using to invade the privacy of individuals in the City and violate the rights of entire communities throughout the United States. ALPR systems collect and store location information about drivers whose vehicles pass through ALPR cameras' fields of view, which, along with the date and time of capture, can be organized by a database that develops a driver profile revealing sensitive details about where individuals work, live, associate, worship, protest and travel.[3] In an October 2025 lawsuit again El Cajon, California Attorney General Bonta confirmed that Flock "***ALPR systems are used for surveillance***; they can collect and store location information that reveals sensitive details about where individuals work, live, associate, worship, seek medical care, travel, shop, and more."[4]

7. Defendants have now installed and monitor a network of now approximately 500 Flock ALPR cameras ("Flock Surveillance Cameras") throughout San Francisco that make it functionally impossible to drive anywhere in the City without having one's movements tracked, photographed, and stored in an AI-assisted database that enables the warrantless surveillance of one's movements. While Mayor Breed lauded this development as a tool to combat shoplifting and car theft, local news simultaneously reported that "[p]rivacy advocates worry the cameras will be abused by officers, invading the privacy of San Franciscans or surveilling the general public."[5]

8. As the City's Flock Surveillance Cameras were being installed, former Mayor Breed

---

[3] https://sls.eff.org/technologies/automated-license-plate-readers-alprs

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

[5] https://www.ktvu.com/news/400-license-plate-cameras-coming-to-san-francisco-privacy-advocates-concerned

"directed staff and departments to eliminate red tape and any unnecessary delays." [6] As alleged herein, the consequences of Defendants' hasty engagement with the for-profit Flock Safety company ("Flock Surveillance") and its Chief Executive Officer ("CEO") have been detrimental to Plaintiff's and class members' civil liberties and privacy rights in the City.

9. In 2023, California Attorney General Bonta "remind[ed] agencies of their obligation to ensure that the storage, collection, sharing, and use of this [ALPR] information is consistent with California law[,]" including S.B. 34.[7] On November 21, 2025, the California Highway Patrol ("CHP") was forced to send Flock's CEO (Garrett Langley) a letter reminding him to abide by California privacy laws – including S.B. 34 – writing, "CHP'S contract with Flock prohibits providing the information gathered from these cameras to the federal government or any other entities outside the State of California, limits the time Flock can retain data and camera footage, and expressly requires compliance with state law governing ALPR systems, including SB 34 (2015) … ***State law on this issue is clear*** … In these turbulent times, it is more urgent than ever to respect our individual freedoms."[8] Turbulent times indeed.

10. The dragnet surveillance challenged in this Action is occurring at the very same time the President of the United States is seeking to use such surveillance to locate immigrants and intimidate his perceived political opponents – including those with the temerity to hold what Trump views "anti-American[], anti-capitalis[t], and anti-Christian[]" beliefs.[9] Against this backdrop, on December 26, 2025, *Politico* reported that "[f]ederal records show that ICE has increased its spending

---

[6] https://www.sf.gov/news--san-francisco-begins-installing-automated-license-plate-readers-disrupt-organized-theft-and

[7] https://oag.ca.gov/news/press-releases/attorney-general-bonta-advises-california-law-enforcement-legal-uses-and

[8] https://www.ktvu.com/news/chp-warns-flock-over-sharing-surveillance-data-federal-government (letter embedded). All emphasis added unless otherwise noted.

[9] https://www.whitehouse.gov/presidential-actions/2025/09/countering-domestic-terrorism-and-organized-political-violence/

on surveillance technology, looking to spend more than $300 million under Trump for social-media monitoring tools, facial recognition software, ***license plate readers*** and services to find where people live and work."[10]

11. "Starting on March 19, 2024, Flock began installing [Flock] ALPR cameras in various strategic locations across San Francisco. This rollout is expected to take place over the next 90 days."[11] The monitoring policy disclosed in the SFPD's announcement provided that: "[p]rior to being granted access to the Flock Safety portal, members will be required to complete training. A training video will be uploaded to Power DMS. Members will be notified when training becomes available. After completing the required training and being onboarded, the member will receive a welcome to Flock email which will provide access to the platform."[12]

12. The SFPD's March 20, 2024 Flock Surveillance Camera installation announcement provided a link to the SFPD's 2019 "Surveillance Technology Policy" which states in relevant part that "ALPR data collected by SFPD ***is not used for the enforcement of Immigration Laws***."[13] Defendants' assurance to Plaintiff and the class was false. It has since been disclosed that Defendants' ALPR Flock data was shared with, *inter alia*, the States of Texas and Georgia and Immigration Customs Enforcement ("ICE").

13. A September 8, 2025 investigative report by *The San Francisco Standard* titled "SFPD let Georgia, Texas cops illegally search city surveillance data on behalf of ICE" revealed that the SFPD has now publicly ***admitted*** that: "[a]ccording to a recent audit of our network, it appears agencies outside California had the ability to query SFPD's Flock system for a [purported] limited period of

---

[10] https://www.politico.com/news/2025/12/26/ice-high-tech-surveillance-lower-privacy-guardrails-00705401

[11] https://www.sanfranciscopolice.org/your-sfpd/policies/department-bulletins-notices/24-052

[12] *Id.*

[13] *Id.*

time."[14] Then, during a September 10, 2025, San Francisco Police Commission hearing, former interim SFPD Chief Paul Yep admitted that the SFPD was investigating audit findings showing queries of its Flock automated license-plate reader network from agencies ***outside California***. Defendants thereby violated not only S.B. 34, but the SFPD's own ALPR policies.[15]

14. Defendants' contract with Flock has now enabled Defendants to blanket San Francisco with approximately 494 advanced AI and cloud-enabled Flock Surveillance Cameras, which photograph and surveil ***every*** car that passes them. Defendants' surveillance dragnet establishes a detailed record of where every driver in San Francisco has travelled, and any person or entity with access to the Flock database can discover routes that any vehicle has travelled across San Francisco 24 hours a day and 365 days a year. This level of surveillance not only enables those granted access to Flock with a detailed map of the driver's travel patterns, but also their personal private associations.

15. Flock also provides advanced search and artificial intelligence functions that SFPD officers can use to output a list of locations a car has been captured, create lists of cars that have visited specific locations, and even track cars that are seen together. Upon information and belief, there are no meaningful restrictions on Defendants' access to this information. SFPD officers need only watch Flock's orientation video and create login credentials to use Defendants' Flock's database throughout their shift. Although SFPD officers are required to use the information only for law enforcement purposes, no one proactively monitors their use.

16. Defendants' ALPR system constitutes warrantless and unreasonable surveillance. This is so because the SFPD's Flock-enabled surveillance is conducted without a warrant, and SFPD officers do not have to establish probable cause, swear to the facts in a warrant application, and await the approval of a magistrate judge before accessing the Flock database. Defendants' Flock

---

[14] Tomoki Chien, SFPD let Georgia, Texas cops illegally search city surveillance data on behalf of ICE, THE SAN FRANCISCO STANDARD (September 8, 2025) https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing/.

[15] *Id*.

Surveillance Cameras photograph and store the information of every single driver in San Francisco that passes them — suspect or not. The photographs and information are then available to any Flock-trained SFPD officer to use.

17. Flock also maintains a centralized nationwide database with over one ***billion*** license plate reads ***every month***. So, even after a driver leaves San Francisco, state and federal authorities can potentially keep tracking them in the more than 5,000 communities where Flock currently operates its cameras. Likewise, any person or entity with access to Flock's centralized database can access the SFPD's information, potentially, even without the SFPD's knowledge. Such risks are not merely hypothetical.

18. On August 6, 2025, for instance, Congressmen Robert Garcia and Raja Krishnamoorthi sent Flock's CEO a letter requesting documents after it was disclosed that "local authorities in Texas reportedly used Flock's automatic license plate reader technology to conduct a nationwide search for a woman they claimed had a self-administered abortion in Texas. As part of this search, Texas law enforcement appears to have reviewed footage from more than 83,000 automatic license plate reader cameras, ***including cameras in Washington and Illinois***, ***where abortion is lawfully protected as a basic right***."[16] Plaintiff is concerned that out-of-state agencies who lack California's robust privacy protections now have access to his movements in the City.

19. Plaintiff is a retired public-school teacher, homeowner and longtime San Francisco resident who lives and drives in San Francisco. Nearly every day, he travels past Defendants' Flock Surveillance Cameras as he drives to the store, his sons' schools or to associate with friends and family. Plaintiff tries to maintain a reasonable amount of privacy and is troubled that the City's Flock Surveillance Cameras track him almost everywhere he goes, storing his movements in a government

---

[16] *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 Media (May 29, 2025) (online at www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/); *She Got an Abortion. So a Texas Cop Used 83,000 Cameras to Track Her Down.,* Electronic Frontier Foundation (May 30, 2025) (online at www.eff.org/deeplinks/2025/05/she-got-abortion-so-texas-cop-used-83000-cameras-track-her-down).

database for any officer or third-party to potentially exploit.

20. Due to the investigative work done by DeFlock – a public source transparency project which Flock's CEO has speciously called a "terrorist organization" – Plaintiff now knows that he routinely drives past some of the many Flock Surveillance Cameras posted at locations throughout San Francisco, and that he cannot drive outside his neighborhood without being surveilled. *See* n. 41, *infra*. The Supreme Court holds that "[Plaintiff] does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'" *Carpenter v. United States*, 585 U.S. 296 (2018) (Roberts, C.J.).

21. "It is [also] undisputed that the ALPR occasionally makes false 'hits' by misreading license plate numbers and mismatching passing license plate numbers with those listed as wanted in the database." *Green v. City and County of San Francisco*, et al., 751 F.3d 1039 (9th Cir. 2014). Such errors, of course, have a disparate impact on marginalized communities in San Francisco.[17] To that end, Flock has recently announced publication of patent application #11,416,545,B1 to monetize its surveillance technology by identifying individuals by race, gender and behavior.[18]

22. These rapidly-occurring developments are particularly acute under the Trump Administration – now well-known for exploiting national surveillance to quash political dissent and deport immigrants of color.[19] Indeed, a December 18, 2025 *KQED* article titled "*California Cities Double Down on License-Plate Readers as Federal Surveillance Grows*," reported that: "despite a series of media reports demonstrating local AI-enabled ALPR databases are feeding a federal surveillance system used by the Trump administration against immigrants and others … ***most***

---

[17] *See, e.g.*, https://www.africanelements.org/news/is-san-francisco-tracking-you-the-mass-surveillance-lawsuit/

[18] https://patents.google.com/patent/US11416545B1

[19] https://www.usatoday.com/story/news/politics/2025/06/04/trump-surveillance-state-federal-data/83924420007/

California officials appear to be digging their heels in."[20]

23. Municipalities elsewhere – including in deep red states – by contrast, have already begun cancelling their Flock contracts due to the privacy and civil liberties concerns raised in this Action. Recently, for instance, Hays County (Texas) terminated its contract with Flock alongside the cities of, *inter alia*: (i) Flagstaff, Arizona; (ii) Oak Park, Illinois; (iii) Charleston, South Carolina; (iv) Evanston, Illinois; and (v) Eugene, Oregon. The Police Chief (Jim William) in the City of Staunton, Virgina even recently publicly chastised Flock's CEO for suggesting that the City of Staunton and Flock were "under coordinated attack" by privacy advocates concerned with Flock's business practices.[21]

24. On January 13, 2026, Santa Cruz became the first city in California to terminate its contract with Flock over data privacy concerns. *KQED* reported that the "Santa Cruz City Council voted 6-1 Tuesday to terminate the city's contract with Flock, citing reports the city's data has been accessed by out-of-state agencies, at a time when the Trump administration is pursuing an increasingly aggressive immigration enforcement agenda. 'For us, ***the threat to our civil liberties was greater than any benefit we could get from the flawed product***,' said Mayor Fred Keeley."[22]

25. Accordingly, as alleged throughout herein, Defendants' camera surveillance system violates Plaintiff's Fourth Amendment privacy rights. Tracking the whole of a person's public movements over (at least) 30 days is a search.[23] Here, the SFPD maintains its Flock recordings for

---

[20] https://www.kqed.org/news/12066989/california-cities-double-down-on-license-plate-readers-as-federal-surveillance-grows

[21] https://www.ci.staunton.va.us/home/showpublisheddocument/13448

[22] https://www.kqed.org/news/12069705/santa-cruz-the-first-in-california-to-terminate-its-contract-with-flock-safety

[23] The SFPD's purported Flock transparency portal states that its retention period is far beyond 30 days at 365 days. *See* https://transparency.flocksafety.com/san-francisco-ca-pd. Notably, Defendants' transparency portal is maintained by Flock and failed to so much as include the City's contract with Flock.

365 days. Defendants are gathering information about everyone who drives past any of its approximately 494 cameras to facilitate investigating purported crimes.[24] In doing so, Defendants are violating the longstanding societal expectation that people's movements and associations over an extended period are private. And because Defendants have engaged in this surveillance without a warrant—instead letting Defendants decide for themselves when and how to access an unprecedented catalogue of every person's movements throughout San Francisco and beyond—their searches are unreasonable.

26. This is exactly the type of police surveillance the Fourth Amendment and S.B. 34 were adopted to prevent. For instance, at least 19 searches run by external states and agencies into the SFPD's Flock database were marked as related to ICE,[25] such that Defendants unlawfully exposed sensitive driver location information to the federal government and U.S. states that lack California's rigorous privacy protections.[26] By unlawfully sharing such location information, Defendants are enabling out-of-state and federal agencies to track, locate, and potentially prosecute California residents and visitors, including for purposes expressly prohibited by the U.S. Constitution and California law.

27. To prevent these violations—and the harm caused by exposing driver information to hackers and out-of-state agencies—Plaintiff seeks herein to remedy the unlawfulness of such surveillance. This civil rights class action lawsuit is therefore designed to rectify Defendants' brazen efforts and/or failures to responsibly deploy and employ Flock's Orwellian ALPR technology against

---

[24] https://transparency.flocksafety.com/san-francisco-ca-pd.

[25] Tomoki Chien, SFPD let Georgia, Texas cops illegally search city surveillance data on behalf of ICE, THE SAN FRANCISCO STANDARD (September 8, 2025) https://sfstandard.com/2025/09/08/sfpd-flock-alpr-ice-data-sharing/.

[26] Article I, Section 1 of the California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and ***privacy***." (emphasis added). This provision creates a right to privacy more protective than the implicit privacy protections in the United States Constitution. (*In re Carmen M.*, 141 Cal.App.4th 478, 490 n. 10 (2006)).

Plaintiff and the putative class.

II. JURISDICTION AND VENUE

28. This is a civil-rights action brought under the Fourth Amendment to the U.S. Constitution; the Civil Rights Act of 1871, 42 U.S.C. § 1983; and the Declaratory Judgment Act, 28 U.S.C. § 2201. This court has jurisdiction under 28 U.S.C. §§ 1331 and 1343(a)(3) as this action seeks redress for the violation of Plaintiff's constitutional and civil rights.

29. This action is also brought pursuant to S.B. 34, Cal. Civ. Code § 1798.90.5 *et seq*. which provides a private right of action for violations of S.B. 34. This Court possesses supplemental jurisdiction over Plaintiff's S.B. 34 claim under 28 U.S.C. §1367.

30. Venue is proper under 28 U.S.C. § 1391 (a) and (b). As described below, Plaintiff and Defendants reside in this district, and the events giving rise to Plaintiff's claims occurred in this district and division.

III. PARTIES

A. Plaintiff

31. Plaintiff Michael Moore is a longtime adult resident of San Francisco and a retired public-school teacher. Plaintiff has a valid California driver's license and drives throughout San Francisco on a regular basis.

32. Defendant the City and County of San Francisco ("the City") is a municipal entity created under the laws of California. At all relevant times hereto, the City was responsible for the policies, practices and supervision of the City's Flock Surveillance Cameras.

33. Defendant SFPD is the police department for San Francisco. The SFPD is responsible for the administration and management of Defendants' contract with Flock and San Francisco's ALPR systems and Flock Surveillance Cameras.

IV. SUBSTANTIVE ALLEGATIONS

ALPR Technology

34. ALPRs are computer-controlled and now AI-enabled cameras mounted above ground level or on police cars (and now drones) that automatically capture all license plate numbers that come

into their view. These images are then transferred to a computer, server or cloud which uses optical character recognition software to convert the image into a license plate number.

35. ALPR is a relatively new technology and, as the technology has improved and become less expensive, it has gained more widespread adoption among law enforcement agencies. ALPRs operate around the clock and capture images of every car that passes their field of view within a fixed distance, including at high speeds or at night. Once an ALPR captures a license plate, it creates a record of the location and time of capture which is then stored in an AI database—perhaps indefinitely.

36. Companies that sell ALPRs and related software services to police departments and federal immigration agencies also offer their customers the capability to pool data. By opting-in to such data sharing—or neglecting to opt out—state and federal authorities create ***multijurisdictional*** databases tracking the movements of cars across virtually the entire country. Police departments commonly compare the license plate images to "hot lists" which typically include vehicles reported stolen and those suspected of involvement in a crime. Rather than address SFPD's 500 police officer shortfall to combat crime, however, Defendants created a high-tech surveillance hub with the financial assistance of a crypto billionaire called the Real-Time Investigation Center at 315 Montgomery St. in the City to house its ALPR surveillance dragnet.

37. In just 2019 alone, however, of the over 1 billion license plate scans collected by just 82 agencies nationwide, ***99.9% of this surveillance data was not actively related to any criminal investigation when it was collected***. Still, law enforcement agencies are stockpiling this data, often for years.[27]

38. The ACLU has aptly warned that "[a]utomatic license plate readers have the potential to create permanent records of virtually everywhere any of us has driven, radically transforming the consequences of ***leaving home to pursue private life***, and opening up many opportunities for abuse. The tracking of people's location constitutes a significant invasion of privacy, which can reveal many

---

[27] https://www.eff.org/deeplinks/2021/04/data-driven-2-california-dragnet-new-dataset-shows-scale-vehicle-surveillance.

things about their lives, such as what friends, doctors, protests, political events, or churches a person may visit."[28] Such is the case with Defendants' Flock Surveillance Cameras here in the City.

39. Anyone with access to a police department's ALPR database can use the data to track any vehicle over time. With enough cameras, the data can be used to pinpoint a car's location and map its movements over any time period for which data exists. A driver can be tracked to a doctor's office, a peaceful political protest or almost anywhere else – all without a warrant.

40. ALPRs also create a record of every other car that was at those locations at the same time, revealing not just where the person driving travelled but also any persons in proximity to the driver at the same time. The data can then be analyzed to discern with whom a driver met or traveled, revealing the driver's community, colleagues and political and other associations. This is all done under the guise of fighting crime.

41. Flock also offers software that automates the tracking process, allowing an officer to easily compile these records with minimal effort. A warranted investigation that would have required a team of officers to tail someone for days or a team of investigators to cobble together information from multiple data sources now only takes an instant in this context. Software programs like Flock's enable the SFPD and federal authorities to map a driver's route and can even produce an analysis of vehicles commonly seen in the same vicinity. The sort of tracking that would have taken days, weeks or even months of effort, multiple officers, and significant resources just a decade ago now takes just a few mouse clicks. City officers can output a list of locations a car has been seen, create lists of cars that visited specific locations, and even track cars that are often seen together.

42. Unlike a police officer, ALPRs do not take breaks, do not blink, and do not sleep. They can operate around the clock and capture all license plates that pass within a fixed distance, even at high speeds or at night. Absent any warrant requirement, how authorities use these systems is left to their own discretion. Unmonitored officers can abuse their access to get information for illegitimate reasons—like tracking protestors or personal acquaintances. And third parties can gain access for

---

[28] https://www.aclu.org/you-are-being-tracked

nefarious and unlawful purposes. These threats are more than just theoretical.

43. For instance, multiple police officers (including a police chief) in Kansas used ALPR data from the same vendor (Flock) used by Defendants in the City to stalk their own former girlfriends.[29] U.S. Customs and Border Protection's ALPR vendor was hacked and license plate images of thousands of travelers at border crossings were made available on the dark web.[30] The U.S. Cybersecurity and Infrastructure Security Agency issued an alert after discovering a "low attack complexity" vulnerability in ALPRs sold by Motorola Solutions.[31]

44. Defendants' sharing of ALPR information with out-of-state entities for the purpose of assisting with immigration enforcement also violates S.B. 54, also called the California Values Act or California's "sanctuary" law, which places restrictions on the use of California state or local resources to assist with federal immigration enforcement. Attorney General Bonta has issued a helpful Information Bulletin clarifying that S.B. 54 "[p]rohibits use of [California law enforcement agency] resources to investigate, interrogate, detain, detect, or arrest persons for immigration purposes…"

Flock Surveillance Co.

45. Within the past few years, a number of companies have started to offer enhanced ALPRs and software to police departments across the country. Among the largest is Flock Surveillance, a Georgia-based tech start-up founded in 2017 that is currently valued at approximately $7.5 billion. Flock was founded in Georgia by current CEO Garrett Langley with investments from, *inter alia*, Peter Thiel, who has stated that he does not "believe that freedom and democracy are compatible."[32] Flock's cameras are located in over 5,000 communities throughout the United States.

46. Flock offers several different ALPR cameras to both government and private-sector

---

[29] https://www.kansas.com/news/politics-government/article291059560.html.

[30] https://www.washingtonpost.com/technology/2019/10/10/surveillance-contractor-that-violated-rules-by-copying-traveler-images-license-plates-can-continue-work-with-cbp/.

[31] https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-19.

[32] https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/

customers. Its cameras are compact and require little to no infrastructure, making them easy to install and operate. Its Falcon LR cameras, purchased and currently used by Defendants in San Francisco, for instance, can operate around the clock, power themselves with solar energy, and capture vehicles traveling up to 100 miles per hour from up to 150 feet away.

47. In March 2024, Mayor London Breed announced the city was installing 400 Flock Safety Falcon cameras.[33] Defendants' contract with Flock Group Inc. dba Flock Safety ("Contract") was executed by both Defendants on March 5, 2024.[34] The Contract confirms that the data each Flock Surveillance Camera captures includes: "i. Vehicles with license plates, paper plates, or no plates at all; ii. The color, type, or other make and model information of a vehicle (car, truck, motorcycle, etc.); iii. Vehicle characteristics that comprise a Vehicle Fingerprint, e.g., accessories, ***bumper stickers***, or decals; iv. Timestamps and location of captured images; and v. ***Other content that may be added through system updates or upgrades that are consistent with the authorized uses by law***."

48. The Contract's Product and Services Description includes "FlockOS," which is Flock's situational awareness operating system and Flock Safety Falcon which is a license plate reader that utilizes Vehicle Fingerprint technology. The Contract's FlockOS Features & Description reveals the true surveillance power of Flock's technology:

Community Network Access: Access to all privately owned Flock devices within

---

[33] https://www.flocksafety.com/blog/sf-takes-historic-step-to-solve-crime-with-400-lpr-cameras

[34] Proposition E, which facilitated Defendants' contract with Flock, barely passed in 2024 while President Biden was still in office. According to *Mission Local*, the "City Attorney's Office, for its part, has said Prop. E would create a loophole allowing for facial recognition, despite the city's ban." https://missionlocal.org/2024/02/prop-e-police-surveillance-sf/. The City Attorney's Office also provided a Memorandum regarding the implementation of Proposition E that stated that the SFPD "must hold a community meeting in the neighborhood being considered for the public safety camera to elicit feedback. The [police] Chief must review and consider the feedback from community members before making a final decision. Lastly, the [police] Chief must make a finding that installing the camera is likely to improve public safety in that area based on public safety considerations, such as the nature and frequency of criminal activity in the area and information provided by members impacted in the community." https://www.sfcityattorney.org/wp-content/uploads/2024/03/Implementation-of-Proposition-E.pdf. Upon information and belief, the SFPD did not hold such meetings and/or make any such findings before the Flock Cameras began being installed in San Francisco in March 2024.

your jurisdiction that have been shared with you.

Unlimited Users: Unlimited users for FlockOS

State Network (License Plate Lookup Only): Allows agencies to look up license plates on all cameras opted in to the statewide Flock network.

Nationwide Network (License Plate Lookup Only): Allows agencies to look up license plates on all cameras opted in to the nationwide Flock network.

Time & Location Based Search: Search full, partial, and temporary plates by time at particular device locations

License Plate Lookup: Look up specific license plate location history captured on Flock devices

Vehicle Fingerprint Search: Search footage using Vehicle Fingerprint™ technology. Access vehicle type, make, color, license plate state, missing / covered plates, and other unique features like ***bumper stickers***, decals, and roof racks.

Insights & Analytics: Reporting tool to help administrators manage their LPR program with device performance data, user and network audits, plate read reports, hot list alert reports, event logs, and outcome reports.

ESRI Based Map Interface: Flock Safety's maps are powered by ESRI, which offers the ability for 3D visualization, viewing of floor plans, and layering of external GIS data, such as City infrastructure (i.e., public facilities, transit systems, utilities), Boundary mapping (i.e., precincts, county lines, beat maps), and Interior floor plans (i.e., ***hospitals***, corporate campuses, ***universities***)

Real-Time NCIC Alerts on Flock ALPR Cameras: Alert sent when a vehicle entered into the NCIC crime database passes by a Flock camera

Unlimited Custom Hot Lists: Ability to add a suspect's license plate to a custom list and get alerted when it passes by a Flock camera

Law Enforcement Network Access: The ability to request ***direct access to evidence detection devices from Law Enforcement agencies outside of your jurisdiction***.

49. On June 24, 2025, Flock released its Q2 2025 Law Enforcement Product Launch Summary which disclosed that: "[i]n a move that will transform the largest network of LPR cameras in the nation, Flock announced that every existing Flock LPR camera can soon become video-enabled at no cost to the customer. 'Flock customers don't have to do a thing or pay a thing,' said Flock Safety's

Chief Strategy Officer, Bailey Quintrell. 'This will be a no-cost software update ***we push over the cloud***.' This optional software upgrade gives agencies immediate visual context to accompany their LPR reads. For example, if five vehicles match a description near a crime scene, the added video helps narrow that list to the one vehicle fleeing the scene. ***Agencies don't need to purchase new hardware***."[35] Furthermore, Defendants' March 2024 contract with Flock provides that Flock "may make any upgrades to system or platform that ***it deems necessary or useful*** to (i) maintain or enhance the quality or delivery of Flock's products or services to its agencies, the competitive strength of, or market for, Flock's products or services such platform or system's cost efficiency or performance, or (ii) to comply with applicable law." Upon information and belief, Defendants have not disclosed whether they are using Flock's new "free" software upgrades.

50. Once Flock Surveillance Cameras capture an image of a car, Flock's software uses machine learning to create what Flock calls a "Vehicle Fingerprint." The "fingerprint" includes the color and make and model of the car and any distinctive features, like, for instance, an anti-Trump or anti-ICE bumper sticker. Flock's software converts each of those details into text and stores them in an organized database. Flock users can then easily filter their searches based on those features because the "Vehicle Fingerprint" automatically links different images of the same car within Flock's database, creating a record of that car's movements over time.

51. Flock offers other software features for police departments to use in conjunction with its cameras. These features: (i) create real-time alerts against hotlists; (ii) analyze patterns of movement; (iii) flag repeat visitors to the area; (iv) provide a streamlined advanced search; (v) project information onto maps; (vi) analyze vehicles frequently seen in proximity to one another; and (vii) generate lists of vehicles that have visited multiple locations of interest like a "No Kings Protest." Flock advertises these features as "a force multiplier" for police departments that can significantly

[35] https://www.flocksafety.com/blog/flock-safetys-q2-2025-law-enforcement-product-launch-summary-increasing-speed-for-law-enforcement

streamline and expedite investigations and tracking.[36]

52. Flock also enables its customers (like Defendants) to pool their data into a centralized database that provides police departments access to over 1 billion monthly datapoints across Flock's more than 5,000 customers. Flock thus gives police departments the ability to track drivers not just within their own jurisdiction, but potentially across the entire nation. For this same reason, in June 2025, the Illinois Secretary of State's Office said it was investigating Flock over alleged illegal searches by out-of-state law enforcement of data produced from Illinois' Flock camera readers.[37]

53. On September 8, 2025, *The San Francisco Standard* published an investigative report titled "SFPD Let ***Georgia***, Texas cops illegally search city surveillance data on behalf of ICE: Out-of-State authorities made 1.6 million searches of San Francisco's license-plate reader data – likely in violation of California law."[38] Its investigative report revealed, *inter alia*, that:

> San Francisco police let out-of-state cops run more than ***1.6 million illegal searches of the city's license-plate reader database*** — including at least 19 that were marked as related to U.S. Immigration and Customs Enforcement;
>
> The controversial surveillance technology, produced by Atlanta-based Flock Safety, captures the license plate and description of every passing vehicle, then stores the information for use in police investigations. In San Francisco, where 400 Flock Cameras line major roadways, ***it's nearly impossible to escape the camera readers' eye***.
>
> [R]eporting by *The Standard*, *404 Media* … and others has revealed that police nationwide are illegally handling license-plate data and ***giving ICE backdoor access to their Flock networks***, renewing long-held concerns about abuse of the technology.
>
> [N]ewly unearthed logs show that the questionable sharing of data was far more widespread than previously understood: The SFPD gave out-of-state agencies direct access to the City's data between at least August 2024 and February 2025, ***enabling a far higher volume of illegal searches than was***

---

[36] https://www.flocksafety.com/why-flock.

[37] https://www.ilsos.gov/news/2025/august-25-2025-giannoulias-audit-finds-license-plate-reader-company-in-violation-of-state-law.html

[38] Flock Surveillance is headquartered in Atlanta, Georgia.

known before.

54. *The San Fransico Standard's* review of the entry logs demonstrated that "[e]ach entry includes the agency that initiated the search, the reason for the search, the time of submission, and the number of Flock networks the agency searched for a given license plate. Police departments often simultaneously search thousands of Flock networks across multiple states and municipalities in a given query. ***The SFPD redacted the reasons for searches in its public records disclosure***."

55. *The Standard*, however, was able to determine the reasons:

> [B]y cross-referencing agency names and timestamps with more than 35 million unredacted Flock searches published on the website Muckrock … The Standard filled in many of the blanks. For instance, the SFPD's logs show that on Dec. 26 at 7:16 p.m, the Franklin County Sheriff's Office in ***Georgia made a search of San Francisco's data that was later redacted***.
>
> But logs from the Danville Police Department in Illinois — another of the 5,757 law enforcement agencies queried in the same search — are unredacted. The reason supplied: 'ICE FUGOPS,' an apparent reference to the agency's Fugitive Operations program, whose goal … is to 'locate, arrest and remove fugitive aliens from the United States.'
>
> The logs show the SFPD's data was searched at least 19 times for 'ICE Fugitive, 'Assist ICE,' or specific ICE detention numbers. The majority of those searches were made between Oct. 23 and Dec. 27, 2024, by the Franklin County Sheriff ***in Georgia***, the Dallas Police Department, and the Milford Police Department in Massachusetts.
>
> ICE has a criminal investigations wing that's less known than its deportation operation, so a search for 'ICE case' isn't necessarily related to immigration. City contracting documents show the SFPD agreed to pay Flock more than $3.9 million for access to its technology between Feb. 20, 2024, and Feb. 19, 2027.[39]

56. While the data the Flock Surveillance Cameras collect belongs to the SFPD, Flock retains that data on at least a rolling 30-day basis. The SFPD, however, maintains a far longer 365-day retention period for the data Defendants' Flock Surveillance Cameras capture.[40]

---

[39] *Id*.

[40] https://transparency.flocksafety.com/san-francisco-ca-pd

57. The SFPD does not require officers to establish probable cause or obtain a warrant to access the Flock data. And Flock Cameras capture the start of nearly every trip Plaintiff makes in his car, so he cannot drive in in San Francisco without being surveilled. As alleged in ¶20, *supra*, Plaintiff knows where Defendants' Flock Surveillance Cameras are located and that they monitor him whenever he leaves his neighborhood due to the transparency efforts of the DeFlock project,[41] which Flock's CEO has speciously called a "terrorist organization."[42]

58. Plaintiff routinely drives past some of the many Flock Cameras posted at locations throughout San Francisco. Images of Plaintiff's car and the associated data about his movements are stored in a database accessible to any SFPD officer, as well as anyone else the SFPD has either knowingly or unwittingly granted access. Flock users can leverage this information to follow Plaintiff's movements throughout San Francisco, and even throughout other jurisdictions that let Flock pool their data. SFPD officers can map nearly all of Plaintiff's movements for 365 days a year.

59. Flock's "Convoy Analysis" feature also lets users identify vehicles that are often seen together so that anyone with access to Flock's record of Plaintiff's movements can use it to see who he meets, when, and where. They can thereby assess who Plaintiff's closest friends are and with whom he associates. Plaintiff does not expect government officials to record his movements and subsequently be permitted to track and analyze his patterns and affiliations for over 30 days without once being identified as the target of a criminal investigation.

60. According to ALPR industry analysts for *404 Media*, "[d]ata from a license plate-scanning tool that is primarily marketed as a surveillance solution for small towns to combat crimes like car jackings or finding missing people ***is being used by ICE*** …"[43] Local police around the country are performing lookups in Flock's AI-powered ALPR system for "immigration" related searches and

---

[41] https://deflock.me/map#map=10/37.787936/-122.407520

[42] *C/f Harper's Weekly*, "What publicity Can Do" by Louis D. Brandeis ("Sunlight is said to be the best of disinfectants.") (1913).

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

as part of other ICE investigations, giving federal law enforcement ***side-door access***. Indeed, 404 Media has reported that Customs Border Patrol has "access to more than 80,000 Flock AI Cameras ***nationwide***."[44]

61. The massive trove of data obtained and shared with *404 Media* shows more than 4,000 nation and statewide lookups by local and state police done either at the behest of the federal government, as an "informal" favor to federal law enforcement, or with a potential immigration focus, according to statements from police departments and sheriff offices. While Flock does not have a contract with ICE, the agency sources data from Flock's cameras by making requests to local law enforcement or other private surveillance providers.[45]

62. Flocks' cameras are no longer just recording vehicular movements — now, their systems are actively evaluating drivers to assess whether one should be reported to law enforcement as ***potential*** participants in organized crime. In a February 13, 2025 press release touting an "Expansive AI and Data Analysis Toolset for Law Enforcement," Flock announced several new capabilities, including something called "Multi-State Insights." The selling point Flock provided for this tool was that: "[m]any large-scale criminal activities—such as human and narcotics trafficking and Organized Retail Crime (ORC)—involve movement across state lines. With our new Multi-State Insights feature, law enforcement is alerted when suspect vehicles have been detected in multiple states, helping investigators uncover networks and trends linked to major crime organizations."[46]

63. Flock Surveillance offers this capability through what it calls an "Investigations Manager," which urges police departments to "Maximize your LPR data to detect patterns of

---

[44] https://www.404media.co/cbp-had-access-to-more-than-80-000-flock-ai-cameras-nationwide/

[45] The data reviewed by *404 Media* was obtained using a public records request from the Danville, Illinois Police Department, and shows the Flock search logs from police departments around the country. *See* ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows, May 27, 2025 (Joseph Cox).

[46] https://www.flocksafety.com/blog/flock-safetys-q2-2025-law-enforcement-product-launch-summary-increasing-speed-for-law-enforcement

suspicious activity across cities and states." Flock also offers a "Linked Vehicles" or "Convoy Search" allowing police to "uncover vehicles frequently seen together," enabling it to track people's associations, and a "Multiple locations search," which promises to "[u]ncover vehicles seen in multiple locations." Flock can therefore now deploy it camera network not just to investigate based on suspicion, but to generate suspicion itself.

64. Flock's business practices have also become the subject of Congressional inquiries. On November 3, 2025, for instance, Senator Ron Wyden and Congressman Raja Krishnamoorthi asked the Federal Trade Commission to investigate Flock for its "negligent cybersecurity practices" stating that "Flock has unnecessarily exposed Americans' sensitive personal data to theft by hackers and foreign spies. While Flock offers support for MFA, a widely recognized cybersecurity best practice, Flock does not require it, which the company confirmed to Congress in October. Moreover, Flock continues to support insecure methods of MFA, such as sending a numeric code to a phone by text message, which is vulnerable to interception and phishing."[47] Plaintiff and the class have been harmed by Defendants' hasty enabling of Flock's negligent cybersecurity practices.

65. Indeed, on January 6, 2026, local San Francisco news blog *SFist* reported that it "[t]urns out ***anyone with an internet connection, and not even a password, could access the feeds of a line of the Flock surveillance cameras that are currently all the rage with the SFPD and Oakland Police Department***."[48] Plaintiff is deeply concerned with Flock's security vulnerabilities.

66. Similarly, on August 6, 2025, members of the Congressional Committee on Oversight and Government Reform requested documents from Flock's CEO, writing:

> ICE agents have also reportedly used Flock data to track immigrants, improperly accessing license plate data in states and localities with laws or ordinances in place that prohibit the use of their resources to assist with the arrest of law-abiding undocumented residents. Given the vast amount of data collected by Flock cameras, and the enormous potential for abuse, it is critical that Flock, law enforcement entities, and state and local governments are ***transparent and accountable*** for how

---

[47] https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf

[48] https://sfist.com/2026/01/06/report-flock-safety-maker-of-sfs-license-plate-reader-cameras-had-gobsmacking-security-flaw/

this sensitive data is accessed and by whom.[49]

67. Defendants have, of course, contracted with Flock using San Francisco taxpayer money – including Plaintiff's and the class's. Plaintiff is deeply concerned that he can no longer drive in the City without Defendants tracking his movements, who he associates with and that Flock Surveillance Cameras have chilled his willingness to protest peacefully and assemble freely without being surveilled. And he is concerned that his uniquely private movements are being tracked using his and the class's taxpayer money without their consent.

68. The term of Defendants' contract with Flock ends on February 28, 2027, but Defendants have options to renew the contract for up to an additional five years for a total of eight years. The annual fee for those eight years ranges from $1,535,00 per year to $1,200,000 per year. Plaintiff is also deeply troubled that the City of San Francisco would contract with a for-profit surveillance company that is so deeply aligned with the Trump Administration's national surveillance efforts. And for good reason.

69. The City of San Francisco is currently suing the Department of Justice to obtain $6.25 million in federal funding for the SFPD which the Trump Administration is refusing to release unless Defendants agree to "obey all of President Trump's 200+ executive orders issued since January [2025] as well as any new ones going forward."[50] One of those executive orders is designed to create a massive surveillance database requiring all federal "[a]gency Heads shall take all necessary steps, to the maximum extent consistent with law, to ensure the Federal Government has ***unfettered access to comprehensive data from all State programs that receive Federal funding***, including, as appropriate,

---

[49] https://krishnamoorthi.house.gov/sites/evo-subsites/krishnamoorthi.house.gov/files/evo-media-document/2025-08-06.garcia-krishnamoorthi-to-flock-re-lpr-tech-and-tracking.pdf?ref=404media.co

[50] https://sf.gazetteer.co/sf-sues-trump-over-police-funding. On January 13, 2026, President Trump announced that, starting on February 1, 2026, he will deny federal funding to any states that are home to local governments resisting his administration's immigration policies, expanding on previous threats to cut off resources to the so-called sanctuary cities themselves. San Francisco is, of course one such city.

data generated by those programs but maintained in ***third-party databases***."[51] Flock is such a third-party database.

70. Flock Surveillance Cameras therefore have the capacity to reveal intimate information; to facilitate cheap, widespread surveillance of much of society; to enable permanent storage and retrospective searches of data; and to provide information inaccessible *via* traditional police observation.

INJURY TO PLAINTIFF AND THE CLASS

71. Defendants' installation and operation of Flock Surveillance Cameras and platform in San Francisco create a running record of the whole of Plaintiff's and the class's movements throughout San Francisco and other jurisdictions enabling Flock and Defendants to intentionally or unkowingly share his data with out-of-state agencies.

72. On March 20, 2024, the SFPD announced that "[s]tarting on March 19, 2024, Flock Safety began installing ALPR cameras in various strategic locations across San Francisco. This rollout is expected to take place over the next 90 days."[52] Because of Defendants' installation and operation of the Flock Cameras, Defendants have photographed Plaintiff's car virtually every time he has driven in the City after the first 100 Flock Cameras were installed in San Francisco on or around June 12, 2024.[53]

73. After the Flock Cameras photograph Plaintiff's' and the class's cars, the Flock database creates a "Vehicle Fingerprint" that links different images of their vehicles and thereby creates a detailed record of their movements in and around San Francisco. Every image the Flock Cameras capture of Plaintiff's cars is stored in Flock's database for at least 30 days but Defendants have

---

[51] https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/

[52] https://www.sanfranciscopolice.org/your-sfpd/policies/department-bulletins-notices/24-052

[53] https://www.sf.gov/news--san-franciscos-new-public-safety-camera-technology-delivering-early-results

contracted with Flock such that the "[f]ootage will be available for Authorized End Users to access and download via the Web Interface for 365 days …"[54] A record of the whole of their movements over at least the past 30 days is accessible to any SFPD officer and anyone else the SFPD has granted access for no less than 365 days.

74. The SFPD has a policy or custom of: (i) not requiring probable cause or individual suspicion for access to Flock data; and (ii) allowing that same access without a warrant. Thus, any SFPD officer can access the whole of Plaintiff's or any other San Francisco driver's movements over at least the past 30 days without a warrant or probable cause.

75. Plaintiff, like most people, tries to maintain a degree of privacy. The installation and operation of the Flock Cameras and platform throughout San Francisco, however, has given him deep consternation about his uniquely private movements. Plaintiff values his privacy and personal security, and is concerned about how the SFPD, an individual officer, or another Flock user might use or misuse the records of his movements. He is also reasonably concerned that malicious, third-party hackers might one day gain access to Flock's database to, for instance, intimidate him for his political views.

76. Flock's vulnerabilities have also caught the attention of Congress, which is seeking to investigate Flock and its CEO, Garrett Langley, for its security vulnerability failures. On November 3, 2025, Senator Ron Wyden and Congressman Raja Krishnamoorthi asked the Federal Trade Commission to investigate Flock "the license plate surveillance camera company, and, where appropriate, hold the company responsible for its negligent cybersecurity practices. Flock's surveillance data can reveal Americans' movements over time, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, as well as places of worship and protests. By not requiring industry-standard multi-factor authentication (MFA) to secure law enforcement accounts, Flock has needlessly exposed Americans' sensitive personal data captured by the company's surveillance cameras to theft by hackers …"

---

[54] The Contract defines "authorized end user" as "any individual employees, agents, or contractors of Customer accessing or using the Services, under the rights granted to Customer pursuant to this Agreement."

77. Defendants' capture, analysis, and sharing of this data therefore violates his Constitutional privacy rights. Plaintiff has no control over how Defendants, Flock, or anyone else with access to Defendant's Flock platform uses the record of their movements. Plaintiff lacks any say about when, or even if, those records will be deleted – besides filing this action. And if Plaintiff's information was to be misused or a data breach was to occur, he may never know - unless the SFPD or Flock was compelled to disclose that information.

78. In essence, Defendants have captured the whole of Plaintiff's vehicular movements since at least June 2024 when the first 100 Flock Cameras were installed in San Francisco and will continue to do so unless enjoined. Defendants therefore have unfettered access to Flock data and will continue to have such access unless enjoined.

V. CLAIMS FOR RELIEF

COUNT I
Violation of Plaintiff's Fourth Amendment Rights
(42 U.S.C. §1983 and the Declaratory Judgment Act)

79. 255. Plaintiff repeats and realleges each and every allegation above as if fully set forth herein.

80. The Fourth Amendment to the U.S. Constitution guarantees the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."

81. The Fourth Amendment requires a warrant as a precondition to a search, unless an exception applies.

82. The Fourth Amendment applies to state and local governments through the Fourteenth Amendment's Due Process Clause.

83. Defendants' operation of the Flock Surveillance Cameras is a search.

84. Defendants' installation and operation of the Flock Cameras is purposeful investigative conduct. Defendants use the Flock Surveillance Cameras to investigate crimes and gather evidence about criminal conduct.

85. Defendants' installation and operation of the Flock Cameras also violates a subjective

expectation of privacy that society recognizes as reasonable.

86. Plaintiff has a subjective expectation of privacy in the whole of his long-term physical movements. His expectation is that, as a practical matter, neither an ordinary person nor Defendants could create a long-term record of his movements throughout San Francisco and other Flock jurisdictions. *See Carpenter v. United States*, 585 U.S. 296, 310 (2018) (Roberts, C.J.).

87. Society's expectation is that law enforcement officers could and would not monitor and catalogue the whole of a person's movements without a warrant for over 30 days. Likewise, society does not expect state and federal authorities to be able to reconstruct the entirety of a person's movements retrospectively, even without knowing in advance that they want to follow a particular person. As such, Plaintiff's expectation of privacy in the whole of his physical movements is one that society is prepared to recognize as reasonable. *See id.*

88. Defendants' surveillance policies are official municipal policies, adopted under color of state law, that violate Plaintiff's rights.

89. Defendants have a policy or custom of providing SFPD officers with access to Flock's database.

90. Defendants have a policy or custom of enabling SFPD officers to log into and use Flock's database for the entirety of their shifts.

91. Defendants have a policy or custom of not seeking or requiring a warrant, probable cause, or any level of individualized suspicion to operate the Flock Surveillance Cameras.

92. Defendants have a policy or custom of not requiring a warrant, probable cause, or any level of individualized suspicion to access, use, or search Flock's database.

93. Defendants have a policy or custom of not seeking or requiring a warrant, probable cause, or any level of individualized suspicion to download and store the photographs and other information that the Flock Surveillance Cameras collect.

94. Defendants have a policy or custom of not requiring a warrant, probable cause, or any level of individualized suspicion to access, use, or search information downloaded from Flock's database.

95. Defendants have a policy or custom of giving each SFPD officer discretion over whether and how to access and use the information available in, or downloaded from, Flock's database.

96. No exception to the Fourth Amendment's warrant requirement justifies the dragnet surveillance of the whole of Plaintiff's and other drivers' movements as alleged herein.

COUNT II
Violations of S.B. 34
(Civ. Code § 1798.90.5 et seq.)

97. Plaintiff repeats and realleges each and every allegation above as if fully set forth herein.

98. The California Legislature has imposed limitations on the use of ALPR data to protect privacy rights of individuals. In 2015, the Legislature passed—and the Governor signed—Senate Bill (SB) 34, codified as Civil Code section 1798.90.5 et. seq., which prohibits California's state and local law enforcement agencies from sharing ALPR data with federal and out-of-state agencies, where the data's use is beyond the reach of California's oversight and regulation.

99. Under the California Civil Code, as amended by Senate Bill No. 34, "[a] public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law." Civ. Code § 1798.90.55(b). A "public agency" is defined as "the state, any city, county, or city and county, or any agency or political subdivision of the state." *See* Civ. Code § 1798.90.5(f). Defendants are such public agencies.

100. The California Supreme Court has recognized that "ALPR data showing where a person was at a certain time c[an] potentially reveal where that person lives, works, or frequently visits." *Am. C.L. Union Found. v. Super. Ct*. (2017) 3 Cal.5th 1032, 1044. With concern for the harms of ALPR surveillance, the California Legislature enacted Civil Code section 1798.90.5 et seq. ("S.B. 34"). It imposes critical privacy and security obligations on parties that operate or use ALPR. Among other things, ALPR operators and end-users need to maintain strict policies and security procedures for their ALPR databases and the private information they contain, including mechanisms to track unauthorized access to people's locations.

101. The Cal. Civil Code prohibits Defendants from sharing or transferring ALPR

information with out-of-state agencies. Accordingly, California Attorney General's Office has instructed California agencies that "SB 34 does not permit California [law enforcement agencies] to share ALPR information with private entities or out-of-state or federal agencies…."[55] This prohibition applies to all sharing of ALPR information, regardless of the purpose. SB 34 allows any person "who has been harmed by a violation" of the law to sue for damages or equitable relief. (Civ. Code, § 1798.90.54, subd. (a).)

102. In enacting S.B. 34, the California legislature noted various privacy concerns about the use of ALPR technology, stating that 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."

103. Defendant SFPD is an "ALPR end-user" under Cal. Civ. Code § 1798.90.5(a) because it accesses or uses an ALPR system. Defendant SFPD's conduct violates the Privacy Requirement under §§ 1798.90.51(b)(1) & 53(b)(1) because it does not implement a meaningful usage and privacy policy in order to ensure that its collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties.

104. Defendant SFPD has admitted that it violated S.B. 34 by sharing ALPR data with out-of-state agencies. Plaintiff and the Class have been harmed by Defendant's conduct because their private and sensitive personal information has been improperly collected and used without their notice or consent.

105. By reason of the foregoing, Defendants are liable to Plaintiff and putative class

---

[55] California Automated License Plate Reader Data Guidance: Information Bulletin, CALIFORNIA DEPARTMENT OF JUSTICE (Oct. 27, 2023) https://oag.ca.gov/system/files/media/2023-dle-06.pdf.

members under S.B. 34.

VI. CLASS ACTION ALLEGATIONS

106. Plaintiff brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on his behalf and others similarly situated who were harmed by the conduct asserted herein. Defendants are excluded from the Class.

107. The Class is defined as all San Francisco residents with valid California driver's licenses who drive in the City and do not opt out from this Action.

108. The members of the class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court.

109. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the class that predominate over questions that may affect individual class members including whether Defendants are violating Plaintiff's and the class's privacy rights under the Fourth Amendment to the United States Constitution.

110. Plaintiff's claims are typical of those of the putative class because they each were similarly harmed by Defendants' warrantless surveillance of their vehicular movements.

111. Plaintiff will adequately protect the interests of the class and has retained counsel who is experienced in federal class action litigation. Plaintiff has no interests that conflict with those of the Class.

112. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulties in the management of this action that would preclude its maintenance as a class action.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment as follows:

A. Declaring this action to be a proper class action pursuant to Rule 23(a) and Rule 23(b)(3) of the Federal Rules of Civil Procedure on behalf of the Class defined herein;

B. Declaring that Defendants' policies and customs described in this Action are unlawful and violate the Fourth Amendment (incorporated through the Fourteenth Amendment) to the U.S. Constitution and S.B. 34;

C. Enjoining Defendants from operating their Flock Surveillance Cameras;

D. Ordering Defendants to delete all images, records, and other data generated by the Flock Cameras;

E. Enjoining Defendants and their officers, employees, agents, and any others acting on their behalf from using Flock Surveillance Cameras to collect images or information without first obtaining a warrant based on probable cause;

F. Enjoining Defendants and their officers, employees, agents, and any others acting on their behalf from accessing any images, records, or other data generated by Flock Surveillance Cameras without first obtaining a warrant based on probable cause;

G. Awarding Plaintiff's counsel reasonable attorneys' fees and litigation costs, including but not limited to fees, costs, and disbursements pursuant to 42 U.S.C. § 1988; and

H. Ordering all other relief to which Plaintiff and the class are entitled, regardless of whether such relief is demanded in this Complaint.

VIII. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury in this action for all issues so triable.

Respectfully submitted,

Dated: January 19, 2026

Law Office of Ramzi Abadou

By: */s/ Ramzi Abadou*

Ramzi Abadou (SBN 222567)
79 Woodland Ave.
San Francisco, California 94117
Telephone: (415) 231-4313
rabadou@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that on **January 19, 2026**, I electronically filed the foregoing with the Clerk

of the Court using the CM/ECF system and I hereby certify that I will mail the foregoing document or paper via the United States Postal Service to the named Defendants on the Manual Service list.

s/ Ramzi Abadou
RAMZI ABADOU

U.S. MAIL/MANUAL SERVICE LIST

City and County of San Francisco and
San Francisco Police Department

City Hall, Room 200
1 Dr. Carlton B. Goodlett Pl.
San Francisco, CA 94102