UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

JARROD WHITSON, individually and on behalf of all others similarly situated, Plaintiff, v. FLOCK GROUP INC. Defendant.	CIVIL ACTION FILE NO. CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Jarrod Whitson ("Plaintiff"), for himself and for all others similarly situated, sues Defendant Flock Group Inc. ("Flock") and alleges as follows. Allegations about Plaintiff and his own conduct rest on personal knowledge. The remainder rests on the investigation of counsel, public records, and other publicly available information.

NATURE OF THE ACTION

1. Flock runs a surveillance network that spans the country. Cameras mounted along public roads photograph whatever drives past, extract the plate number, and stamp each sighting with a place and a moment. Flock keeps those

sightings and sells law enforcement agencies the software that searches them. Flock's system therefore does more than identify vehicles: it creates and maintains a searchable record of where vehicles have been and when they were there.

2. Flock reports that its network includes more than 120,000 cameras and processes more than 20 billion license plate readings each month.[1]

3. One camera records that a vehicle passed one location at one time. A network of cameras records where a vehicle has been over time. Flock markets that accumulation as the value of its product, including statewide and nationwide search functions that permit a user to retrieve records collected by cameras operated by other agencies.[2] By aggregating information collected from numerous cameras and agencies, Flock enables users to reconstruct the movements of vehicles across jurisdictions and over time.

4. Flock does not merely manufacture cameras. It supplies and operates the authentication, search, sharing, logging, and audit functions through which its customers' personnel obtain vehicle location information, and it retains contractual authority to restrict or suspend a customer's access.[3] Flock thus controls critical

---

[1] FLOCK SAFETY, *License Plate Reader (LPR) Cameras*, https://www.flocksafety.com/products/license-plate-readers (last visited September 9, 2026).

[2] FLOCK SAFETY, *Flock Safety Platform*, https://www.flocksafety.com/products/flock-safety-platform (last visited September 9, 2026).

[3] FLOCK SAFETY, *Terms and Conditions*, https://www.flocksafety.com/legal/terms-and-conditions (last visited September 9, 2026).

aspects of how ALPR information is accessed, searched, shared, and used by the law enforcement agencies that rely on its platform.

5. Officers have turned that access on the people in their own lives. Journalists working from police and court records counted, by August 2026, no fewer than 50 officers facing charges or allegations over their use of plate reader systems. Flock's platform featured in 46 of those. In 26, the person on the other end of the query was a wife, a girlfriend, an ex, an ex's new partner, or a woman the officer had taken an interest in.[4]

6. Between July and August 2026, the Georgia Bureau of Investigation announced the arrests of current and former Georgia law enforcement employees for accessing Flock systems for non-law enforcement purposes.[5] Each was charged under O.C.G.A. section 35-1-22, which governs the use of automated license plate recognition systems in Georgia.[6]

---

[4] Drew Harwell, Douglas MacMillan & Aaron Schaffer, *How Rogue Officers Turned a Nationwide Camera Network Into a Tool for Stalking*, WASHINGTON POST (Aug. 2, 2026), https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/ (last visited September 9, 2026).

[5] Georgia Bureau of Investigation, GBI Arrests Five Former Albany Police Department Officers for Misuse of a License Plate Reader (July 6, 2026), https://gbi.georgia.gov/press-releases/2026-07-06/gbi-arrests-five-former-albany-police-department-officers-misuse-license (last accessed September 9, 2026); see also Georgia Bureau of Investigation, GBI Arrests Conyers Police Department Employee for Misuse of a License Plate Reader System (July 23, 2026), https://gbi.georgia.gov/press-releases/2026-07-23/gbi-arrests-conyers-police-department-employee-misuse-license-plate (last accessed September 9, 2026).

[6] *Id*.

7. Flock cameras also misread plates. Flock states that its cameras accurately capture approximately 93 of every 100 license plates. Applied to the more than 20 billion readings Flock reports processing each month, a seven percent error rate produces approximately 1.4 billion inaccurate readings each month.

8. Roseville, California put that claim to the test. Reviewing the 1,427 Flock alerts its officers received during 2023 and 2024 flagging vehicles as stolen or tied to felonies, the City found a misread plate in 1,011 of them, a failure rate above seventy percent.[7]

9. Plaintiff and the members of the Class did nothing to warrant law enforcement attention. They drove to work, to school, to medical appointments, and to places of worship, and Flock recorded them doing it. Plaintiff brings this action on behalf of a nationwide Class to recover damages and to obtain injunctive relief.

PARTIES

10. Plaintiff Jarrod Whitson is a citizen of Tennessee residing in Wartburg, Morgan County, Tennessee. Plaintiff is a law enforcement officer with the Wartburg Police Department and a former officer with the Harriman Police Department and the Roane County Sheriff's Office. In the course of his ordinary daily activities, Plaintiff repeatedly drove past Flock cameras, which captured, recorded, and

[7] CITY OF ROSEVILLE, *Automated License Plate Reader Technology (ALPR)*, https://www.roseville.ca.gov/police/automated_license_plate_reader_technology_%28alpr%29.php (last visited September 9, 2026).

retained his license plate, vehicle images, and the date, time, and location of each detection. Following a public records request, Plaintiff discovered that his license plate data had been queried across 5,675 separate networks within Flock's surveillance system.

11. Defendant Flock Group Inc. is a Delaware corporation with its headquarters and principal place of business at 1160 Howell Mill Road NW, Suite 210 in Atlanta, Fulton County, Georgia. Flock develops, markets, sells, and operates automated license plate recognition cameras, the software platform through which those cameras' output is searched and shared, and the logging, audit, and access control functions that govern that searching and sharing.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. section 1332(d)(2), because the proposed Class contains more than 100 members, the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, and at least one member of the proposed Class is a citizen of a state different from Flock.

13. This Court has general personal jurisdiction over Flock because Flock, a Delaware corporation, is registered to do business in Georgia and maintains its principal place of business in Georgia and is therefore at home in this State. Flock has continuous and systematic contacts with Georgia such that it has sufficient

minimum contacts here. Further, Flock intentionally avails itself of this jurisdiction by maintaining and conducting its corporate operations in Georgia.

14. Venue is proper in this District under 28 U.S.C. section 1391(b) because Flock resides in this District, maintains its principal place of business in this District, and a substantial part of the events and omissions giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

A. Flock Sells an Integrated System of Cameras, Databases, and Search Software

15. Flock is not in the camera business alone. What it sells is a chain: hardware that captures, software that indexes what the hardware captured, and a hosted platform where customers pull the indexed records back out and pass them to one another.

16. Access comes by contract with a governmental customer. Those contracts hand the customer a set of responsibilities and keep for Flock the power to curtail or shut off access in defined circumstances. Flock therefore stays in the loop long after the hardware is bolted to a pole.

17. Flock has marketed the reach of its network as a product feature, describing search functionality spanning participating agencies across a network covering forty-nine states.

18. The value of the system to a user increases with the number of cameras whose output that user can search. A user who can search only the cameras operated by the user's own agency learns whether a vehicle passed those cameras. A user who can search a statewide or nationwide network learns where a vehicle has been across a far larger area.

B. What the System Records, and What a User Can Learn From It

19. A Flock camera sits in one spot and runs continuously. It does not wait for a reason. Every vehicle entering its field is photographed and its plate is read, and the system writes down where the camera stands and what the clock said. It also captures or infers make, color and identifying marks, and its images take in whoever is sitting in the car.

20. This is what separates Flock from a red-light camera. A red-light camera fires because a driver did something. A Flock camera fires because a driver existed within its field of view. What the resulting record proves is correspondingly thin: one car, one place, one moment.

21. Those records travel to Flock's databases and become queryable through its platform. Run the same plate enough times and the answers line up into an itinerary, which is to say into a picture of where someone goes, on what schedule, and beside whom.

22. The locations a vehicle visits include physical and mental health care providers, places of worship, attorneys' offices, shelters, and the homes of family members and partners.

23. Sharing multiplies that. An officer at a participating agency can pull up sightings gathered by cameras his own department never installed. Flock built statewide and nationwide search for exactly this and sells the reach as a selling point.[8]

24. The person whose vehicle is searched cannot see that a search occurred. Flock provides them with no notice, and the system furnishes no means by which he could learn of it. Misuse is invisible to its subject even where Flock's own records capture it.

C. Flock Controls the Search, Sharing, Logging, and Audit Functions

25. Flock supplies and operates the software and data infrastructure through which users authenticate, search ALPR records, obtain access to records collected by other agencies, and generate records of their own searches.

26. Every query leaves a trace by design. Flock says it keeps those traces so that anyone auditing later can ask whether the person querying was entitled to and

[8] FLOCK SAFETY, *Controlled Access for Everyone*, https://www.flocksafety.com/trust/law-enforcement-access (last visited September 9, 2026).

had a proper reason. The retained fields, on Flock's account, cover who ran it, when, the reason they typed, and the plate or other term they ran. [9]

27. Whether a given category of query can be refused outright, rather than permitted and logged, is a switch that exists only where Flock has built one.

28. A customer decides who gets a login and how its own preferences are set. What those preferences are capable of expressing, and whether a prohibited query can be stopped rather than merely recorded, are questions only Flock answers, in code it alone writes.

D. Improper Access by Law Enforcement Users Is a Known and Recurring Failure

29. The reported failures do not share a single cause. Some involve credentialed officers hunting private targets. Some involve logins that outlived the employment they were issued for. Some involve Flock staff inside customer cameras. Some involve data crossing borders the customer never agreed to and the law did not allow. Some involve the software reading the wrong plate. Some involve it reading the right plate and someone drawing the wrong conclusion.

30. What unites them is authorship. Credentialing, permissioning, cross-agency distribution, query handling, logging, anomaly detection, character

[9] FLOCK SAFETY, *Compliance Tools*, https://www.flocksafety.com/trust/compliance-tools (last visited September 9, 2026).

recognition, and Flock's own reach into customer equipment are all Flock's work product.

1. Credentialed Users Have Turned the System on People They Knew

31. Albany, Georgia audited its own Flock usage in 2026, and the audit produced a criminal case. The Georgia Bureau of Investigation arrested five former officers of the Albany Police Department that July, reporting that each had gone into Flock repeatedly and put retained plate data to uses having nothing to do with police work. Charges ran from a single count to eleven, depending on the officer. [10]

32. A dispatcher supervisor at the Conyers, Georgia Police Department ran more than thirty Flock queries unrelated to any law enforcement purpose over roughly four months in 2026, according to the GBI, which announced the arrest that July.[11]

33. A former Polk County, Georgia officer held a login to the Cedartown Police Department's Flock system and, per the GBI, used it repeatedly across 2024

[10] GEORGIA BUREAU OF INVESTIGATION, *GBI Arrests Five Former Albany Police Department Officers for Misuse of a License Plate Reader* (July 6, 2026), https://gbi.georgia.gov/press-releases/2026-07-06/gbi-arrests-five-former-albany-police-department-officers-misuse-license (last visited September 9, 2026).

[11] GEORGIA BUREAU OF INVESTIGATION, *GBI Arrests Conyers Police Department Employee for Misuse of a License Plate Reader System* (July 23, 2026), https://gbi.georgia.gov/press-releases/2026-07-23/gbi-arrests-conyers-police-department-employee-misuse-license-plate (last visited September 9, 2026).

and 2025 on private business. Four counts of misusing a license plate reader system followed in August 2026.[12]

34. The former 911 director for the Dallas, Georgia Police Department drew two such counts the same month, the GBI reporting that she had been in her department's Flock system during 2024 and 2025 for reasons unconnected to law enforcement. [13]

35. None of this reads as a single lapse of curiosity. An officer in Orange City, Florida spent the summer of 2024 running the plate of a woman he used to date, at least 69 times by the count in the court record, alongside at least 24 runs of her mother's plate and 15 of her father's. [14]

36. Volume is a recurring feature of these matters. One Wisconsin deputy learned that a colleague she had once dated had queried her plate sixteen times in a single day. In a separate matter, Flock's records documented 179 queries directed at one woman and her partner.[15]

---

[12] GEORGIA BUREAU OF INVESTIGATION, *GBI Arrests Former Polk County Police Officer for Misuse of a License Plate Reader System* (Aug. 7, 2026), https://gbi.georgia.gov/press-releases/2026-08-07/gbi-arrests-former-polk-county-police-officer-misuse-license-plate-reader (last visited September 9, 2026).

[13] GEORGIA BUREAU OF INVESTIGATION, *GBI Arrests Former 911 Director in Paulding County for Misuse of a License Plate Reader System* (Aug. 12, 2026), https://gbi.georgia.gov/press-releases/2026-08-12/gbi-arrests-former-911-director-paulding-county-misuse-license-plate (last visited September 9, 2026).

[14] Jason Koebler, *Cops Keep Getting Arrested for Using Flock to Stalk People*, 404 MEDIA (June 10, 2026), https://www.404media.co/cops-keep-getting-arrested-for-using-flock-to-stalk-people/ (last visited September 9, 2026).

[15] *See* supra note 4.

2. The Querying Runs Into the Hundreds Before Anyone Stops It

37. Braselton, Georgia's former police chief queried the plates of an ex-girlfriend and her teenage daughter roughly 600 times. What the queries bought him was her calendar: the grocery runs, the dates, the doctor's appointments. She could not work out how he kept knowing. [16]

38. Richmond County, Georgia produced the largest figure yet reported. A former deputy there is alleged to have put one woman's plate through the system 1,639 times over several months.[17] The investigation also identified three other employees who each conducted more than 100 unauthorized searches.[18]

39. Every one of those queries wrote a log entry as it executed. Flock's records were complete enough, afterwards, to reconstruct precisely what had happened. They were not used to stop it while it was happening.

40. Flock has described its historical audit process as reactive.

3. Logins Outlive the Jobs They Were Issued For

41. An Ogeechee Circuit District Attorney's Office investigator, formerly of the Effingham County Sheriff's Office, still held a working login to that sheriff's

---

[16] INSTITUTE FOR JUSTICE, *The IJ Database of ALPR Abuse*, https://ij.org/the-ij-database-of-alpr-abuse/ (last visited September 9, 2026).

[17] *Richmond County Flock Scandal Grows with Three High-Profile Arrests*, **The Augusta Press** (June 2026), https://theaugustapress.com/richmond-county-flock-scandal-grows-with-three-high-profile-arrests/ (last accessed September 9, 2026).

[18] *Id*.

office Flock account after moving on. Between 15 June and 5 July 2026 he used it more than sixty times on private business, according to the GBI. [19]

42. Flock could have closed that account under its own contract. It did not.

4. Flock Personnel Have Accessed Customer Cameras in Private and Sensitive Locations

43. Flock's own personnel have opened customer camera feeds with no customer asking them to. Records obtained from the City of Dunwoody, Georgia show that during a Flock sales demonstration and testing session, Flock staff pulled up privately owned cameras the City had connected to its Flock real-time crime center. Among the feeds they opened were a gymnastics room used by children, a playground, a school, a Jewish community center, and a swimming pool. [20]

44. Flock's answer was that future demonstrations would use more public cameras. The answer concedes the mechanism: Flock's staff hold technical reach into integrated camera environments, and that reach extends to privately owned cameras trained on private and sensitive places.

---

[19] GEORGIA BUREAU OF INVESTIGATION, *GBI Arrests Former Ogeechee Circuit District Attorney's Office Investigator for Stalking and Misuse of a License Plate Reader System* (July 27, 2026), https://gbi.georgia.gov/press-releases/2026-07-27/gbi-arrests-former-ogeechee-circuit-district-attorneys-office (last visited September 9, 2026).

[20] Jason Koebler, *City Learns Flock Accessed Cameras in Children's Gymnastics Room as a Sales Pitch Demo, Renews Contract Anyway*, 404 MEDIA (Apr. 30, 2026), https://www.404media.co/city-learns-flock-accessed-cameras-in-childrens-gymnastics-room-as-a-sales-pitch-demo-renews-contract-anyway/ (last visited September 9, 2026).

5. Flock Settings Have Provided Access Beyond What Customers Authorized or Law Permitted

45. Mountain View, California set out to learn who could see its Flock data and could not get an answer. The City disclosed in January 2026 that federal agencies had reached the output of its first Flock camera by way of a nationwide search setting Flock switched on without asking or telling the police department. Its audit also found a statewide search function running outside the limits the City had set, open to California agencies the City never cleared. Flock could not produce the historical records that would have explained how either happened. [21]

46. Illinois reached a similar conclusion. An audit announced by the Secretary of State in August 2025 concluded that Flock had opened Illinois plate cameras to U.S. Customs and Border Protection, allowing surveillance of Illinois drivers contrary to state law, and that the company had not put proper data-sharing safeguards in place. [22]

---

[21] CITY OF MOUNTAIN VIEW, *City Statement on Flock Safety Automated License Plate Reader System* (Jan. 30, 2026), https://content.govdelivery.com/accounts/CAMOUNTAINVIEW/bulletins/406f640 (last visited September 9, 2026).

[22] ILLINOIS SECRETARY OF STATE, *Giannoulias Audit Finds License Plate Reader Company in Violation of State Law* (Aug. 25, 2025), https://www.ilsos.gov/news/2025/august-25-2025-giannoulias-audit-finds-license-plate-reader-company-in-violation-of-state-law.html (last visited September 9, 2026).

E. Flock's Automated Output Produces Inaccurate Readings at Scale

47. On Flock's telling, character recognition exceeds 96 percent in good conditions. A separate Flock figure puts plate read accuracy at 93 percent.

48. Take Flock's own arithmetic. Twenty billion reads a month against a 96 percent success rate leaves roughly 800 million wrong records every month, and 9.6 billion across a year. Against the 93 percent figure Flock states elsewhere, the monthly total is about 1.4 billion. On the company's own numbers the system is wrong hundreds of millions of times a month.

49. Real world performance has been worse than Flock's stated figures. Roseville, California found misread plates in 1,011 of 1,427 reviewed alerts, a rate exceeding seventy percent.

50. Roseville reported its results to Flock directly. Flock responded publicly by restating its greater than 96 percent character recognition figure under optimal conditions and attributing the results to Roseville, and asserted that Roseville's performance had improved, which Roseville disputed.[23]

[23] Nicole Einbinder, *In One California Town, Flock Misread License Plates in 71% of the Alerts It Sent to Police*, BUSINESS INSIDER (July 31, 2026), https://www.businessinsider.com/flock-camera-misread-license-plate-reader-california-roseville-police-2026-7 (last visited September 9, 2026).

51. Those errors reach people. Motorists have been pulled over, held, handcuffed, taken to jail, and approached by officers with weapons drawn, because a camera misread a plate or an alert carried bad information. [24]

F. Flock Markets Its Product as a Tool for Drawing Investigative Connections From Location Data

52. Here is the whole of what a Flock record proves: this car, this spot, this minute. It does not identify the driver. It does not supply a reason for the trip. It says nothing about what anyone in the car was doing, and nothing about whether anyone in it broke a law.

53. Flock does not leave that inference to the user. It builds and sells the tools that produce it, promoting a platform that lets officers search, filter, and link vehicle records to build cases quickly and to turn fragments into leads. Its Enhanced LPR line advertises Multi-Geo Search, which surfaces vehicles appearing at several investigator-chosen locations, and Convoy Search, which surfaces vehicles moving near a target vehicle. [25]

54. Flock markets Vehicle Signature, which permits searching by vehicle characteristics rather than by plate, and FreeForm, which permits natural language

---

[24] Christopher Ingraham, *Dozens of Innocent Motorists Have Been Pulled Over, Detained at Gunpoint, or Jailed Due to AI License Plate Camera Errors*, INSTITUTE FOR JUSTICE (July 1, 2026), https://ij.org/dozens-of-innocent-motorists-have-been-pulled-over-detained-at-gunpoint-or-jailed-due-to-ai-license-plate-camera-errors/ (last visited September 9, 2026).

[25] FLOCK SAFETY, *Enhanced LPR: Stop Crime Patterns That Standard LPRs Cannot See*, https://www.flocksafety.com/enhanced-lpr-stop-crime-patterns-that-standard-lprs-cant-see (last visited September 9, 2026).

searches across video and license plate evidence and, where authorized, across shared camera systems.[26]

55. A car keeps turning up somewhere because its owner lives there, works there, shops there, gets treated there, prays there, or simply drives that way. Two cars keep turning up together because the drivers share an office, a street, a family, a commute, or nothing at all beyond the same stretch of road at the same hour. Software written to find repetition, coincidence, and company will find all of it, and cannot tell which kind it has found.

56. A Columbine Valley, Colorado woman drove her usual work route, which happened to pass a house someone had stolen a package from. Flock had her truck on that route repeatedly, correctly, because that is where she drove. Police read the pattern as evidence and accused her of the theft. Clearing herself took GPS logs, vehicle records, and video she had to assemble herself. [27]

57. Nothing malfunctioned. The camera read her plate correctly every time. The harm came from the use Flock advertises for a correct reading.

---

[26] FLOCK SAFETY, *Flock FreeForm*, https://www.flocksafety.com/products/flock-freeform (last visited September 9, 2026).

[27] Olivia Prentzel, *After Police Used Flock Cameras to Accuse a Denver Woman of Theft, She Had to Prove Her Own Innocence*, COLORADO SUN (Oct. 28, 2025), https://coloradosun.com/2025/10/28/flock-camera-police-colorado-columbine-valley/ (last visited September 9, 2026).

G. Flock Knows of the Misuse and the Error Rates and Has Not Corrected Them

58. Flock is not a small or unsophisticated firm. It fields a surveillance platform across the country, and how that platform is misused goes to its customers, its design choices, its regulatory exposure, and its revenue.

59. That Flock answers these incidents publicly at all establishes two things: information about misuse reaches it, and the controls bearing on misuse are within its power to change.

60. One adjustment Flock made was to cut default search-data retention from thirty days to seven. Shortening how long a record persists does nothing to stop a user querying repeatedly during the window it does persist.

61. Flock presents its audit tooling as accountability. Audit tooling documents misconduct once it is finished. In Richmond County it documented 1,639 queries by one employee and more than 100 apiece by three others, all of it after the fact.

62. Flock's Chief Executive Officer Garrett Langley characterized Flock misuse in April 2026 as a trade-off that he could make, weighing the incidents against the number of investigations he stated Flock technology supported. In a later interview he described abuse as exceptionally rare.[28]

---

[28] PROTON, *We Asked Flock's CEO About Surveillance Abuse. Here Is What He Said* (Aug. 19, 2026), https://proton.me/blog/flock-ceo-interview (last visited September 9, 2026).

63. Flock has left anti-abuse protections optional where it has provided them at all, and has continued to expand the products, the network, and the number of ways the system can be searched.

H. The Vehicle Location Data Flock Collects Has Economic Value

64. Commercial entities purchase data about individuals, including location history, from data brokers and other sources in order to target advertising and services.

65. Data brokers combine elements drawn from private and public sources into composite profiles. A single source supplies a few elements about a person's activities; combined sources supply a detailed view.

66. Historical data about where a person's vehicle has traveled increases the value of existing datasets about that person. Where a vehicle travels indicates purchasing decisions, routines, and interests.

67. Flock developed its Nova product to combine third-party datasets with Flock datasets. Flock Nova is an AI-powered data platform designed to streamline police investigations by consolidating information from Flock's devices, Computer-Aided Dispatch (CAD), Record Management Systems (RMS), and open-source intelligence into a single interface. The platform enables investigators to link people

and locations while allowing agencies to share CAD and RMS data across different jurisdictions through opt-in agreements.[29]

68. The vehicle movement data Flock collects has economic value. Flock collected Plaintiff's data and the Class members' data and paid them nothing for it.

I. Plaintiff and the Class Cannot Avoid the System

69. To reach work, school, medical care, and places of worship, Plaintiff and the Class members drive on roads where Flock cameras are placed.

70. Flock puts cameras where people simply go. Public reporting in September 2025 located at least nineteen of them run by two agencies around Dahlonega and Lumpkin County, Georgia, a town whose year-round population sits near 7,000.[30]

71. Plaintiff and the Class members are recorded, their records are retained, and their records are made searchable, without their consent and without any suspicion that they have done anything wrong.

TOLLING OF THE STATUTE OF LIMITATIONS

[29] *Flock Safety Launches New AI-Powered Tools to Accelerate Police Investigations*, Police1 (2026), https://www.police1.com/police-products/police-technology/publicsafetysoftware/flock-safety-launches-new-ai-powered-tools-to-accelerate-police-investigations (last accessed September 9, 2026).

[30] About Our Town, City of Dahlonega, https://www.dahlonega.gov/community/about-our-town/ (last accessed September 9, 2026).

72. Flock did not disclose to the public that its nationwide search functionality had been enabled on customer cameras, in some instances without the customer agency's knowledge or approval.

73. When customer agencies inquired, Flock attributed the results to system bugs, early settings, and logging limitations that prevented those customers from identifying the cause. Flock informed the Sheriff's Office that "other agencies experienced similar issues" and stated that "due to limitations in technical logging, it was impossible to determine the specific cause."[31]

74. Flock represented to customers that it had no contracts with federal agencies. In reality, Flock had secretly entered into a memorandum of understanding and pilot agreement in May 2025 with the United States Border Patrol (as well as Homeland Security Investigations) to provide federal agencies with direct account access, a fact that was concealed from its local law enforcement customers until exposed by investigative reporting in August 2025.[32]

75. Plaintiff and the Class members did not know, and in the exercise of reasonable diligence could not have known, that their vehicle location information

---

[31] *Flock License Plate Readers Shared Data with Out-of-State Agencies, Ventura County Audit Finds*, CBS Los Angeles (2026), https://www.cbsnews.com/losangeles/news/flock-license-plate-readers-shared-data-with-out-of-state-federal-agencies/ (last accessed September 9, 2026).

[32] Spencer Soicher, Flock admits federal immigration agents have direct access to tracking data, despite previous claims, 9NEWS (August 19, 2025) https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8aee742-56d4-4a57-b5bb-0373286dfef8? (last accessed September 9, 2026).

was being collected, retained, searched, and shared as alleged. The system supplies no notice to the person whose records are searched.

76. Plaintiff and the Class members learned of the conduct alleged here only when investigative reporting and public records disclosures published in 2025 and 2026 revealed it. Any applicable limitations period is tolled accordingly.

CLASS ACTION ALLEGATIONS

77. Plaintiff brings this action under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4), on behalf of the following nationwide Class:

> Every person whose vehicle was photographed and whose plate was read, recorded, and retained by any Flock automated license plate recognition camera anywhere in the United States during the Class Period.

78. Excluded from the Class are Flock; its officers, directors, employees, agents, affiliates, parents, and subsidiaries; any entity in which Flock holds a controlling interest; the judge assigned to this action and that judge's staff and immediate family; persons who timely and validly request exclusion; and Plaintiff's counsel.

79. Plaintiff reserves the right to modify or amend the definitions of the Class, before the Court determines whether certification is appropriate.

80. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. Flock reports operating more than 120,000 cameras and processing more than 20 billion license plate readings each month. The members are identifiable

from Flock's own records, which record the plate, the date, the time, and the camera location for every detection.

81. **Commonality.** Questions common to every member include: which parts of the credentialing, query, distribution, logging, audit and safeguard architecture Flock authored and administers; what Flock knew about misuse and when; whether Flock's design and operation of those functions met the standard of reasonable care; whether Flock's warnings to customer agencies were adequate; whether Flock's conduct breached O.C.G.A. section 35-1-22; whether Flock acted knowingly, willfully, or in reckless disregard; and what relief follows.

82. **Typicality.** Plaintiff's claims are typical of the claims of the members. Plaintiff's license plate data was captured, recorded, retained, and made searchable by the same system, operating in the same way, as that of every other member.

83. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class. His interests do not conflict with those of the members, and he has retained counsel experienced in complex class litigation.

84. **Predominance.** Common questions predominate over any questions affecting only individual members. The core liability questions concern Flock's architecture, its controls, its knowledge, and its safeguards, all of which are common to every member.

85. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Most members will never learn that their records were searched, because the system supplies no notice. Individual actions would duplicate the same inquiry into the same Flock-controlled mechanisms and risk inconsistent adjudications.

86. **Rule 23(b)(2).** Flock has acted and refused to act on grounds generally applicable to the Class, making final injunctive and corresponding declaratory relief appropriate as to each as a whole.

87. **Rule 23(c)(4).** In the alternative, Plaintiff seeks certification of particular issues, including whether Flock designed and operated the functions alleged, whether Flock knew of the misuse and error alleged, and whether Flock's conduct breached the duties alleged.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE PER SE
O.C.G.A. section 35-1-22
(On Behalf of Plaintiff and the Class)

88. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

89. O.C.G.A. § 35-1-22 governs automated license plate recognition systems in Georgia and restricts access to and use of captured license plate data to

law enforcement purposes. The statute defines "captured license plate data" to include global positioning coordinates, date and time, photographs, license plate numbers, and other data captured by or derived from an automated license plate recognition system. O.C.G.A. § 35-1-22(a)(1)-(2).

90. Under O.C.G.A. § 35-1-22(b), captured license plate data may not be accessed except for a "law enforcement purpose," which the statute defines as the investigation of an offense or activity initiated by a law enforcement agency. O.C.G.A. § 35-1-22(a)(4), (b).

91. Georgia prosecutors have brought charges under that statute against the law enforcement personnel described above for reaching into Flock systems on personal business. Every one of those accesses ran through software Flock wrote, hosted, and administered, on an account Flock had the contractual power to suspend.

92. Flock designed, supplied, operates, hosts, and materially controls the software through which law enforcement agencies access and use Flock's ALPR system, including the functions governing the collection, retention, search, sharing, logging, auditing, and restriction of access to captured license plate data.

93. Flock knew or should have known that its system contains captured license plate data and that law enforcement personnel could access that data through Flock's system for personal or other non-law-enforcement purposes.

94. Flock nevertheless permitted law enforcement personnel to access and use captured license plate data through Flock's system for personal and other non-law-enforcement purposes, including the unauthorized searches described above.

95. Flock's violations of O.C.G.A. section 35-1-22 constitute negligence per se, the statute having been enacted to protect individuals against the unauthorized collection, use, and dissemination of ALPR information.

96. Flock's conduct was the actual and proximate cause of harm to Plaintiff and Class, including: (a) the unauthorized access to and use of their ALPR information; (b) the loss of control over the record of their movements; and (c) diminution in the value of that information.

97. Plaintiffs seek compensatory and punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT II

INVASION OF PRIVACY BY INTRUSION UPON SECLUSION

(On Behalf of Plaintiff and the Class)

98. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

99. Plaintiff and Class Members hold a reasonable expectation of privacy in their movements, their routines, their associations, and in the accumulated record of where their vehicles have been.

100. Flock intentionally intruded upon the solitude, seclusion, and private affairs of Plaintiff and Class Members by photographing their vehicles, reading and recording their plates, logging the time and place of each detection, retaining those records, and making them searchable across agencies and jurisdictions, without notice and without consent.

101. Flock did so without regard to whether any of these people was suspected of anything.

102. Assembled, those records disclose where Plaintiff and Class Members go, which places they return to, and, as detections accumulate, the shape of their routines and the company they keep.

103. Flock's intrusion would be highly offensive to a reasonable person. It reaches every road a person drives, including the routes to a doctor, a place of worship, a lawyer's office, and a relative's home. A reasonable person would be highly offended to learn that a private company had assembled a searchable history of his movements and opened it to thousands of agencies, without telling him and without any suspicion that he had done anything wrong.

104. Flock built the system knowing it records people who are suspected of nothing, and knowing what the resulting records disclose about them.

105. Plaintiff and Class Members suffered actual harm from Flock's intrusion, including: (a) the violation of their privacy in their movements and

associations; (b) diminution in the value of their personal information; (c) the risk that their location history reaches unauthorized parties; and (d) a chilling effect on their freedom to travel, to associate, and to seek care.

106. Plaintiff and Class Members seek compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT III

NEGLIGENCE

(On Behalf of Plaintiff and the Class)

107. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

108. Flock owed Plaintiff and Class Members a duty to exercise reasonable care in collecting, retaining, and making searchable their ALPR information, including a duty to implement reasonable safeguards against unauthorized access, use, and disclosure.

109. That duty followed from Flock's own position: it wrote the software, it holds the data, it administers the accounts, and it decides what the safeguards are capable of doing.

110. Flock breached that duty by, among other things: (a) offering preventive controls against prohibited searching as optional settings rather than defaults, where it offered them at all; (b) accepting user-typed search justifications it never verified; (c) treating after-the-fact audit logs as a substitute for catching

abnormal search patterns as they happen; (d) leaving accounts reachable by personnel who had left the agency the account belonged to; and (e) turning on interagency and nationwide search settings without confirming its customers had authorized them.

111. Flock knew what it was risking. Recurring misuse incidents, its own audit records, communications from customers, and its own product roadmap all told it that authentication, typed search reasons, and retrospective auditing were not containing the problem.

112. Flock's breaches were the actual and proximate cause of harm to Plaintiff and Class Members, including: (a) unauthorized access to and use of their vehicle location information; (b) diminution in the value of that information; (c) loss of control over the record of their movements and associations; and (d) exposure to the misuse and the error rates described above.

113. Flock's conduct was knowing, willful, and in reckless disregard of the rights of Plaintiff and Class Members.

114. Plaintiff and the Class seek compensatory and punitive damages, injunctive relief, and attorneys' fees and costs.

115. Plaintiff and the Class further seek an award of the value of the vehicle location information Flock took from them without compensation.

COUNT IV

NEGLIGENT DESIGN

(On Behalf of Plaintiff and the Class)

116. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

117. Flock owed Plaintiff and Class Members a duty to exercise reasonable care in choosing and implementing the design of the functions it controls, measured against the foreseeable risk that authorized users would put authorized access to unauthorized use.

118. The choices belonging to Flock included, among others: (a) whether to require a search purpose and whether to check it; (b) how access and sharing default; (c) what the audit log captures and who reads it; (d) whether prohibited categories of search can be blocked outright; (e) whether abnormal or repetitive querying is surfaced while it is happening; and (f) whether anything escalates, restricts, or interrupts an account once misuse appears.

119. Flock's own catalogue answers the feasibility question. It has shipped search-term exclusion, case-number requirements, sharing controls, and automated monitoring that reads recorded activity and surfaces atypical patterns. Flock has never said that these controls were unavailable to it earlier for any technical reason.

120. A reasonably designed safeguard architecture would have blocked defined categories of improper access, surfaced abnormal and repetitive querying

for prompt review, and interrupted misuse once identified rather than preserving a record of it.

121. Flock's design failed at each of those three points, and its failure was the actual and proximate cause of harm to Plaintiff and Class Members, including the unauthorized access to and use of their ALPR information, the loss of control over the record of their movements, and diminution in the value of that information.

122. Flock's conduct was knowing, willful, and in reckless disregard of the rights of Plaintiff and Class Members. Plaintiff and the Class seek compensatory and punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT V

FAILURE TO WARN

(On Behalf of Plaintiff and the Class)

123. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

124. Flock understood that a credential issued for police work can be spent on private business, and that the private business in question has included stalking, tracking, and sustained personal surveillance.

125. Flock also understood that typed search justifications and after-the-fact logs were not containing that conduct, and that its customer agencies needed to be told so, together with what configuring, monitoring, auditing, and intervening would actually require of them.

126. Having built the architecture and held the knowledge, Flock owed a duty to warn its customer agencies of those risks and to instruct them on the measures available to meet them.

127. Flock breached that duty by, among other things: (a) not conveying the scale or the recurrence of the misuse it knew about; (b) not disclosing what typed search reasons and retrospective auditing do not accomplish; (c) not instructing agencies on the configuration, monitoring, and audit practices needed to catch misuse in progress; and (d) not telling agencies what to do once misuse surfaced.

128. Warned adequately, agencies would have enabled, configured, or enforced safeguards and review practices that would have stopped, caught, limited, or cut short improper searches of Plaintiff and Class.

129. Flock's silence was the actual and proximate cause of harm to Plaintiff and Class Members, including: (a) improper searches that would not have occurred; (b) improper searches that ran longer than they would have; and (c) the delay in anyone identifying either.

130. Flock's conduct was knowing, willful, and in reckless disregard of the rights of Plaintiff and Class Members. Plaintiff and the Class seek compensatory and punitive damages, injunctive relief, and attorneys' fees and costs.

COUNT VI
INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS
(On Behalf of Plaintiff and the Class)

131. Plaintiff repeats and realleges paragraphs 1 through 87 as if fully set forth herein.

132. Flock operates a system capable of creating searchable records revealing where a person has been, and Flock has continued to operate and expand that system despite recurring incidents in which access to the system was used for personal surveillance.

133. Flock's continued operation of the system without safeguards reasonably sufficient to address categories of misuse of which Flock knew or should have known constitutes reckless and wanton disregard for the privacy of persons whose movements are recorded through the system.

134. Under the circumstances alleged, Flock's conduct was extreme and outrageous.

135. Plaintiff and Class suffered emotional distress as a result of Flock's conduct and seek compensatory and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

a. Certify this action as a class action under Rule 23, appoint Plaintiff as Class Representative, and appoint Plaintiff's counsel as Class Counsel;

b. Enter judgment in favor of Plaintiff and the Class on all counts;

c. Award compensatory, consequential, and nominal damages;

d. Award punitive damages;

e. Enter injunctive and declaratory relief requiring Flock to implement preventive controls against prohibited access, to identify abnormal and repetitive search activity as it occurs, and to interrupt identified misuse;

f. Award the costs and expenses of this litigation and reasonable attorneys' fees;

g. Award pre-judgment and post-judgment interest; and

h. Grant such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted, this 11th day of September, 2026.

HERMAN JONES LLP

/s/ John C. Herman

John C. Herman
(Georgia Bar No. 348370)
Candace N. Smith
(Georgia Bar No. 654910)
3424 Peachtree Road, N.E.
Suite 1650
Atlanta, Georgia 30326
Tel: (404) 504-6500
Fax: (404) 504-6501
jherman@hermanjones.com
csmith@hermanjones.com

LEVI & KORSINSKY, LLP

Mark S. Reich
Mark Jensen
500 Fifth Avenue, 42nd Floor
New York, New York 10110
Telephone: (212) 363-7500
Email: mreich@zlk.com
Email: mjensen@zlk.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Flock Lawsuit Calls Out Alleged Law Enforcement Misuse of Nationwide License Plate-Reading Camera Network