UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

GRACE SCHULTE, individually and on behalf of all others similarly situated, Plaintiffs, v. FLOCK GROUP INC., Defendant.	CIVIL ACTION FILE NO. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Grace Schulte ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Flock Group Inc. ("Flock" or "Defendant"). Plaintiff alleges the following based on personal knowledge as to herself, the investigation of counsel, public records and other publicly available information and, as to matters principally within Flock's or its governmental customers' possession or control, and upon information and belief.

NATURE OF THE ACTION

1. Flock built a nationwide vehicle surveillance system that records where vehicles are seen and allows law enforcement users to search those records. Its roadside cameras photograph vehicles that pass within their view, read their license plates and record the date, time and camera location. Flock stores that information electronically and makes it searchable through software it supplies to law enforcement agencies.

2. Pursuant to that system, Flock operates a nationwide automatic license plate reader ("ALPR") network used by thousands of law enforcement agencies. Its cameras capture, in addition to license plate information, vehicle images, the precise location, and the date, time and location of each sighting. In taking pictures of vehicles and license plates, Flock cameras also often capture images of drivers and passengers in those vehicles.

3. The data captured by the ALPR readers is uploaded to Flock's centralized databases, where it can be searched through Flock's software platform and used to identify when and where particular vehicles were detected.

4. The power of Flock's system comes from accumulation of information, as well as sharing of that information. A single camera records that a vehicle was detected at one place and time. A network of cameras creates a history of where that vehicle has been detected, thereby enabling the monitoring, surveillance and tracking of those captured by Flock cameras. Further, when agencies share access, a Flock user can conduct searches to obtain license plate and vehicle location information collected outside the user's own agency, substantially expanding the geographic scope and amount of information available to that Flock user.

5. Flock operates its ALPR network at enormous scale. Flock reports that its network now includes more than 120,000 cameras and records billions of plate scans each month.

6. Throughout the country, ALPR usage is regulated. At least 30 states have regulations governing who may use or deploy ALPRs and for what purposes, where or under what conditions they may be installed, and how resulting plate location data may be collected, accessed, retained, shared, disclosed or destroyed.

7. Further, the Flock system places powerful location information in the hands of its users while depending on certain safeguards to distinguish legitimate law enforcement use from personal or other unauthorized use. This case concerns what happens when those safeguards fail or simply are not present.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because there are more than 100 Class members nationwide; the aggregate amount in controversy exceeds $5 million exclusive of interest and costs; and because the majority of Class members are of diverse citizenship from Defendant.

9. Flock Group Inc. is a Delaware corporation registered to do business in Georgia. Its headquarters and principal place of business are located in Atlanta, Georgia, in Fulton County. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Georgia. Defendant has continuous and systematic contacts with Georgia such that it has sufficient minimum contacts here. Further, Defendant intentionally avails itself of this jurisdiction by maintaining and conducting its corporate operations in Georgia.

10. Venue is proper, pursuant to 28 U.S.C. § 1391, because Defendant is headquartered and has its principal place of business in this District, intentionally and regularly conducts business in this District, and a substantial portion of the events, omissions and acts giving rise to Plaintiff and the Class's claims herein occurred in this District.

THE PARTIES

11. Plaintiff Grace Schulte is a citizen of Georgia and resides in Dahlonega, Lumpkin County, Georgia. Plaintiff's ALPR information was repeatedly captured by Flock as alleged herein.

12. Defendant Flock Group Inc. is an Atlanta-headquartered technology company that develops, markets, supplies and operates ALPR cameras, software and related search, networking, logging, auditing and safeguard functionality for law enforcement agencies in Georgia and throughout the United States.

FACTUAL ALLEGATIONS

A. Flock Built and Operates an Integrated Surveillance System

13. While Flock is a manufacturer of roadside cameras, it does much more. Flock sells an integrated camera, database and software service in which Flock-manufactured cameras capture vehicle information; Flock's software converts that information into searchable records and Flock's cloud-based platform permits users to retrieve and share those records. Flock describes its license plate reader product as

combining its cameras and vehicle intelligence with searchability and networked reach of the resulting data.[1]

14. Flock contracts with governmental customers for use and access to its platform. While Flock's Terms and Conditions assign customers certain responsibilities, that agreement expressly reserves authority to Flock to restrict or suspend access in specified circumstances. Thus, Flock performs continuing access and control functions even after its equipment is in its customer's hands.[2]

15. Flock's business model also depends on aggregation of data. A camera at one location can establish that a vehicle was detected there at a particular time. Flock's software makes the records of that one location and of other locations searchable, and network sharing can permit an authorized user to retrieve records collected by other participating agencies. The resulting value, and risk, of the Flock system comes from converting many discrete camera detections into searchable information concerning a vehicle's locations over time.

16. Flock has touted its nationwide and statewide search capability as a product feature. Searches can reach as many as thousands of cameras, spanning participating

[1] Flock Safety, Flock LPR, https://www.flocksafety.com/products/license plate readers (last accessed August 25, 2026).
[2] Flock Safety, Terms and Conditions (Aug. 2026), https://www.flocksafety.com/legal/terms-and-conditions (last accessed August 25, 2026).

agencies in Flock's forty-nine state network, demonstrating the breadth that networked access can provide.[3]

B. What Flock's ALPR System Records and Allows Users to Learn

17. Flock places cameras at fixed locations where they automatically capture information about passing vehicles. The cameras record license plate information and images of vehicles, together with the date, time and location at which the vehicle was detected. Flock's technology may also record or derive vehicle characteristics such as make, color and distinguishing features. In addition, images of the vehicle's driver and passengers may also be captured.

18. Unlike a camera that is activated by a traffic violation, an ALPR camera records vehicles simply because they pass within its view. Thus, the resulting record does not seek out or establish any wrongdoing. Rather, the image simply establishes that a particular vehicle was detected at a particular location and time.

19. The captured data is uploaded to Flock's databases, where it can be searched through Flock's software platform and used to identify when and where particular vehicles were detected. Repeated searches for the same license plate can reveal a sequence of locations and times associated with the vehicle. Depending on the responsive records available, those searches can reveal aspects of a person's movements, routines and associations.

[3] See Flock Safety, Flock LPR, https://www.flocksafety.com/products/license plate readers (last accessed August 25, 2026).

20. Those recorded movements can include traveling to physical and mental healthcare providers or to other personally sensitive locations.

21. Flock's system is networked. Where participating agencies share access, a user can search license plate and vehicle location records collected by cameras operated by other agencies. Flock offers Statewide and National search functionality and markets the breadth of its network as a feature of the product.[4]

22. This networked design can materially expand the surveillance available to one Flock user. Instead of learning only whether a vehicle passed cameras operated by the user's agency at a given time, the user also may obtain records collected by participating agencies across a broader geographic area.

23. Flock's platform therefore enables aggregation. A user who repeatedly queries a plate can retrieve observations of the same vehicle across different locations and times.[5] Repeated searches also can reveal various aspects of the vehicle user's movements, locations and associations.

C. Flock Controls Search, Sharing and Safeguards

[4] Controlled Access for Everyone, https://www.flocksafety.com/trust/law enforcement-access (last accessed August 21, 2026); Flock Safety, Offense Type Dropdown: A Simpler, More Accurate Audit, https://www.flocksafety.com/blog/offense-type-dropdown-a-simpler-more-accurate-audit (last accessed August 21, 2026).

[5] What the Flock Is Happening With License Plate Readers? The 2026 Network and Privacy Fight, Aug. 14, 2026 https://carcody.com/what-the-flock-is-happening-with-license plate readers-the-2026-network-and-privacy-fight/ (last accessed August 21, 2026).

24. Flock does not merely manufacture fixed roadside cameras. It also supplies and operates software and data infrastructure architecture through which users search ALPR information, access shared data and generate records of their searches.

25. According to Flock, it maintains these records to, among other things, facilitate audits concerning whether access was made by authorized persons for legitimate purposes and in compliance with law and policy. Flock also controls product functionality capable of restricting or excluding categories of searches.[6]

26. Flock records ALPR searches. This enables Flock to audit those records. According to Flock, its audit records include the username, date, time, stated purpose and the license plate or other information used to conduct the search.[7] Thus, while customers may manage authorized users and local settings, Flock supplies the authentication, search, sharing, logging and safeguard functions through which those choices are implemented.

27. The person whose vehicle information is searched ordinarily cannot see, and thus, does not know, that a law enforcement user has queried the system. The misuse can therefore remain invisible to the person being surveilled even while the system itself generates records capable of revealing the search activity.

---

[6] Flock Safety, Response to Illinois LPR Data-Sharing Concerns (June 12, 2025), https://www.flocksafety.com/blog/flock-safetys-response-to-illinois-lpr-data-use-and-out-of-state-sharing-concerns (last accessed August 21, 2026).

[7] Flock Safety, Compliance Tools, https://www.flocksafety.com/trust/compliance-tools (last accessed August 25, 2026).

D. Improper User Access Is a Known and Recurring Risk

28. Flock's systems have been associated with numerous, recurring problems involving different aspects of the technology and its operation.

29. Reported incidents have involved law enforcement personnel using Flock to conduct personal surveillance, repeated improper searches continuing before detection, former agency personnel retaining access to agency accounts, Flock employees accessing customer-integrated camera feeds in sensitive locations and government customers discovering that the access actually provided through Flock exceeded the access they intended or understood themselves to have authorized.

30. Other reported problems have involved data sharing contrary to legal restrictions, inaccurate license plate identification producing false police alerts and accurate vehicle location records being treated as evidence of criminal activity they did not establish. These incidents do not arise from a single type of misuse or technical failure. Rather, they implicate multiple components of Flock's integrated system, including account access, permissions and configuration, network sharing, search functionality, audit and monitoring functions, automated plate recognition and Flock's own access to customer systems. Moreover, they demonstrate persistent problems affecting the collection, access, use and reliability of information maintained and made available through Flock.

(a) Flock Systems Have Repeatedly Been Used for Personal Surveillance and Stalking

31. Flock's nationwide network has repeatedly been misused by law enforcement personnel to locate and monitor people for personal rather than law enforcement purposes.

32. In July 2026, in Albany, Georgia, an internal audit of the Flock system led to a GBI investigation and arrests of five former police officers. The GBI reported that the officers had accessed Flock on multiple occasions and used retained license plate data for non-law enforcement purposes; the charged misuse counts ranged from one to eleven per officer.[8]

33. In Conyers, Georgia, the GBI reported that a police department dispatcher supervisor accessed Flock more than thirty times between April and July 2026 for non-law enforcement purposes.[9]

34. In Polk/Cedartown, the GBI reported that a former Polk County police officer with access to the Cedartown Police Department's Flock system accessed it multiple times during 2024 and 2025 for non-law enforcement purposes. She was charged in August 2026 with four counts of misuse of a license plate reader system.[10]

---

[8]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 August 21, 2026).

[9] 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 August 21, 2026).

[10] 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 accessed August 25, 2026).

35. In Paulding County, the GBI reported that a former Dallas Police Department 911 director accessed the department's Flock system during 2024 and 2025 for non-law enforcement purposes. She was charged in August 2026 with two counts of misuse of a license plate reader system.[11]

36. An August 2026 Washington Post investigation of police and court records identified at least 50 law enforcement officers charged with or accused of misusing automated license plate reader systems, with Flock's system involved in 46 of those cases. In 26 cases, investigators or prosecutors alleged that officers used the technology to surveil wives, girlfriends, former partners, new partners of former partners, or women the officers wanted to meet.[12]

37. The reported conduct was not limited to isolated or one-time curiosity. In Orange City, Florida, Officer Jarmarus Brown repeatedly searched Flock for his former girlfriend and her parents during the summer of 2024. Court records reviewed by 404 Media reflected at least 69 searches for his former girlfriend's plate, at least 24 for her mother's plate and at least 15 for her father's plate.[13]

---

[11] 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 accessed August 25, 2026).

[12] 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 accessed August 21, 2026).

[13] 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 accessed August 25, 2026); Harwell et al., supra note 12.

38. Other reported incidents illustrate the sensitivity of information that repeated vehicle location searches can reveal. The Washington Post reported a case in which a Wisconsin deputy's plate was searched 16 times in one day by a fellow deputy with whom she had been romantically involved and different case in which Flock records showed 179 searches of a woman and her partner.[14]

(b) Misuse of Flock's Systems Can Continue for Prolonged Periods Without Detection or Intervention By Flock

39. Improper searching can continue at substantial volume before intervention. The Washington Post reported that the former Braselton, Georgia police chief searched tags associated with his former girlfriend and her teenage daughter roughly 600 times. The searches allegedly allowed him to know about ordinary activities including grocery shopping, dates and medical appointments before the woman understood how he was obtaining that information.[15]

40. Further, June 2026 reporting found that a Richmond County, Georgia former deputy searched one woman's plate **1,639 times** over several months for personal monitoring and that the same investigation identified three additional employees who each conducted more than 100 unauthorized searches. The matter demonstrates that extraordinary volumes of repeated targeting can accumulate and remain reconstructable from search records.[16]

---

[14] Harwell et al., supra note 12.
[15] *Id.*
[16] Institute for Justice, The IJ Database of ALPR Abuse, https://ij.org/the-ij-database-of-alpr-abuse/ (last accessed August 25, 2026); see also Atlanta Journal-Constitution, Georgia Officers Misuse

41. Flock has described its own previous safeguards – a historical audit process – as "reactive."[17]

(c) Flock Access Can Persist After Users Leave the Agency Whose Account They Used

42. Reported incidents also identify failures at the boundary between an agency's personnel and continuing system access.

43. In July 2026, the Georgia Bureau of Investigation reported that Andrae Wright, then an investigator for the Ogeechee Circuit District Attorney's Office and a former Effingham County Sheriff's Office employee, still had access to the Effingham County Sheriff's Office Flock account. As a result, he was able to access that account more than 60 times between June 15 and July 5, 2026 for non-law enforcement purposes.[18] Notably, this was despite Flock having the authority to restrict or terminate access to its systems.

(d) Flock Personnel Have Accessed Customer-Integrated Cameras in Sensitive Private Locations

---

License Plate Reader Databases: Can They Be Stopped? (June 30, 2026), https://www.ajc.com/news/2026/06/georgia-officers-misuse-license plate reader-databases-can-they-be-stopped/ (last accessed August 25, 2026).

[17] Flock Safety, Flock Safety Introduces Audit Assistance, Its Latest Trust & Compliance Tool, to Set a New Standard for Accountable Public Safety Technology (Apr. 14, 2026), https://www.globenewswire.com/news-release/2026/04/14/3273480/0/en/flock-safety-introduces-audit-assistance-its-latest-trust-compliance-tool-to-set-a-new-standard-for-accountable-public-safety-technology.html. (last accessed August 25, 2026).

[18] 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 accessed August 25, 2026).

44. The reported access problems are not limited to misuse by police personnel. Public-record reporting from Dunwoody, Georgia showed that Flock employees accessed privately owned cameras integrated into Dunwoody's Flock-powered real-time crime system during a Flock demonstration and testing meeting. The accessed feeds included cameras at a children's gymnastics room, a playground, a school, a Jewish community center and a pool.[19]

45. Flock thereafter stated that its employees would conduct demonstrations using more public locations. However, the incident identifies a separate access mechanism for misuse: that Flock personnel can possess technical access to integrated camera environments and that the scope of access available through the platform may extend to privately owned cameras located in private and even sensitive locations, connected to a governmental surveillance network.

(e) Flock System Settings Can Provide Interagency Access Beyond the Scope That Its Customers Intended or Is Allowed By Law

46. Official findings also document circumstances in which the operative access provided through Flock did not correspond to the access a government customer believed it had authorized. In January 2026, the City of Mountain View, California reported that federal agencies had accessed data from the City's first Flock camera through a nationwide-search setting that Flock had turned on without the police department's

[19] 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 accessed August 25, 2026).

permission or knowledge. The City's audit separately found that a statewide-search function was not operating within the control limitations Mountain View had established and had allowed access by California law enforcement agencies that Mountain View had not approved. When Mountain View pressed for an explanation, Flock could not provide the historical records needed to explain what occurred.[20]

47. In August 2025, the Illinois Secretary of State announced that an audit found that Flock had allowed U.S. Customs and Border Protection to access Illinois license plate cameras and surveil drivers in violation of Illinois law. The Secretary's office stated that Flock lacked proper safeguards for data sharing.[21]

(f) Flock's Automated Output Produces a Massive Number of Errors – Even Under Flock's Calculations.

48. According to Flock, its cameras accurately capture approximately 93 out of every 100 license plates. Flock also reports that its network processes more than 20 billion license plate readings each month. Even accepting Flock's claimed accuracy at face value (which is in dispute), application of a seven-percent error rate at that scale would produce approximately **1.4 billion inaccurate license plate readings each**

[20] 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 accessed August 25, 2026).

[21] 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 accessed August 25, 2026).

month. Thus, even performance consistent with Flock's own reported accuracy necessarily produces an enormous volume of inaccurate data within the system.[22]

49. Real-world performance has at times been substantially worse. The City of Roseville, California reviewed 1,427 Flock alerts involving vehicles identified as stolen or associated with felonies during 2023 and 2024. The City found that 1,011 of those alerts – over seventy percent – contained a misread license plate.[23]

50. The consequences of such errors can be significant. Documented incidents involving Flock and other automated license plate readers have resulted in innocent motorists being repeatedly stopped, detained, handcuffed, jailed or confronted by officers with firearms drawn because a plate was misread or because of erroneous information generated by an alert.[24]

(g) Flock Encourages Users to Draw Investigative Connections from Vehicle Location Data, Creating a Separate Risk Even When the Underlying Data Is Accurate

51. A different problem arises when Flock accurately identifies a vehicle but the resulting location information is treated as establishing something the data simply cannot or does not establish or demonstrate. A Flock record establishes, at most, that a particular

[22] 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, updated July 20, 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 accessed August 25, 2026).
[23] City of Roseville, Automated License Plate Reader Technology (ALPR), https://www.roseville.ca.gov/police/automated_license_plate_reader_technology_%28alpr%29.php (August 25, 2026).
[24] Ingraham, supra note 22.

vehicle was captured at a particular location at a particular time. Standing alone, it does not establish who was driving the vehicle, why the vehicle was there, what its occupants were doing or whether any occupant committed a crime.

52. Flock affirmatively designs and markets its products to encourage law enforcement to "connect the dots," *i.e.,* to connect vehicle sightings, identify patterns and generate investigative leads from accumulated vehicle information. Flock states that its platform allows users to search, filter and link vehicle data to build cases faster and to turn partial details into leads. Its Enhanced LPR product expressly promotes tools designed to "connect the dots," including Multi-Geo Search, which identifies vehicles appearing at multiple locations selected by an investigator, and Convoy Search, which identifies vehicles traveling near a targeted vehicle.[25]

53. Flock also markets Vehicle Signature and FreeForm as means of generating investigative leads from *incomplete information* rather than from a known license plate. Vehicle Signature permits users to search by vehicle characteristics, while FreeForm permits natural-language searches across video and LPR evidence and, where authorized,

[25] Flock Safety, Flock Safety Platform, https://www.flocksafety.com/products/flock-safety-platform (last accessed August 25, 2026); Flock Safety, License Plate Readers (LPR) Cameras, https://www.flocksafety.com/products/license plate readers (last accessed August 25, 2026); Flock Safety, Enhanced LPR: Stop Crime Patterns That Standard LPRs Can't See, https://www.flocksafety.com/enhanced-lpr-stop-crime-patterns-that-standard-lprs-cant-see (last accessed August 25, 2026).

across shared camera systems. These functions are designed to surface vehicles or evidence that the Flock system deems potentially relevant to an investigation.[26]

54. A vehicle's repeated presence near a location may reflect nothing more than where its owner lives, works, shops, receives medical care, worships, socializes or routinely travels. Vehicles may appear together because their drivers are coworkers, neighbors, relatives, commuters traveling the same road or strangers moving through the same traffic. When software is specifically designed to identify recurring locations, common appearances and travel associations, ordinary and innocent activity can itself become the factual basis from which an investigative connection is drawn.

55. Flock promotes using its software to act as an investigative accelerant to identify recurring locations, common appearances and travel associations. As a result, ordinary and innocent activity can itself become the factual basis from which an erroneous investigative connection is drawn.

56. Chrisanna Elser's experience in Columbine Valley, Colorado illustrates the problem. Flock cameras accurately recorded Elser's truck traveling through an area where a package had been stolen. Because Elser routinely drove through the area for work, Flock had repeatedly recorded her vehicle there – thus making her routine travel a suspicious activity. The police relied upon the Flock location records and other

[26] Flock Safety, Frequently Asked Questions, https://www.flocksafety.com/faq (last accessed August 25, 2026); Flock Safety, Flock FreeForm, https://www.flocksafety.com/products/flock-freeform (last accessed August 25, 2026).

surveillance to accuse Elser of stealing the package. To prove her innocence, Elser assembled GPS, vehicle and video evidence demonstrating that she had not committed the theft.[27]

57. The Elser incident did not result from Flock misreading her license plate. The system apparently did what it was designed to do: it recorded that her vehicle had been at a particular location. The error occurred because Flock's promotional materials and tools for linking sightings, locations and associations are designed to promote "investigative connections" from mere happenstance.

58. Flock cameras are deployed at locations where ordinary daily activity predictably generates substantial proverbial traffic. In September 2025, publicly reported citing of cameras identified at least nineteen Flock ALPRs operated by two law enforcement entities in Dahlonega and Lumpkin County, Georgia[28] at a time when Dahlonega had an estimated year-round population of approximately 7,000.[29]

59. Among other places, a Flock camera is positioned near Lumpkin County High School and directed toward a roadway upon which vehicles routinely queue while traveling toward the school. Such placement permits Flock to capture significant amounts

[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, updated Nov. 11, 2025), https://coloradosun.com/2025/10/28/flock-camera-police-colorado-columbine-valley/ (last accessed August 25, 2026).
[28] Electronic Frontier Foundation, Atlas of Surveillance, Dahlonega, Georgia, https://www.atlasofsurveillance.org/search?location=Dahlonega%2C+GA&commit=Search+the+Data (last accessed August 25, 2026).
[29] About Our Town, City of Dahlonega, https://www.dahlonega.gov/community/about-our-town/ (last accessed August 25, 2026).

of vehicle information, simply because people are traveling to work, school or other ordinary locations.

(h) Flock's Own Statements and Actions Reflect Its Knowledge of the Rampant Misuse and Error Problems

60. Flock is a large, sophisticated company operating a nationally deployed law enforcement surveillance platform. Significant publicly reported misuse and error of its core product directly concern its customers, product design, legal compliance and business.

61. Flock's own responses to reported incidents further demonstrate that it receives or develops information concerning misuse and has the ability to modify controls directed to that misuse.

62. However, Flock's incremental changes do not address the more profound problems with the Flock system. An example of this is Flock's change of the default retention period of search data from thirty days to seven. However, such a change does not prevent a user from repeatedly conducting improper searches while the data remains available.

63. Similarly, Flock has characterized its audit capabilities as a means of "accountability."[30] However, even if Flock's system can preserve evidence sufficient to prove misuse after hundreds of searches, it fails to prevent or timely surface the misuse as it occurs. For example, Richmond County, where one employee reportedly conducted

[30] See supra, note 7.

1,639 searches and three others each conducted more than 100 unauthorized searches, illustrates the difference between retrospective auditability and timely intervention.

64. Further, Flock's increasing menu of products that are promoted as speeding up the investigative process creates further risk of errors, rather than minimizing them.

65. Taken together, Flock's own product evolution reflects recognition of several distinct control problems implicated by the incidents listed above while also displaying a lack of willingness to address them in a way that interferes with the networking of the Flock system, the expansion of the use of the Flock system and the increase in the ways it can be used.

E. Flock Has Acted Willfully in Its Failure to Adequately Address the Error and Misuse Problem

66. Flock has been repeatedly confronted with evidence that its nationwide vehicle surveillance system can harm innocent people both when users deliberately abuse it and when the technology itself produces inaccurate information. Flock nevertheless has repeatedly minimized the significance of those failures by describing abuse as rare or isolated, emphasizing its claimed successes as the denominator against which failures should be judged, and claiming accuracy percentages that, even if true, obscure the enormous number of inaccurate readings necessarily produced at the scale at which Flock operates.

67. Flock has known from its inception that law enforcement users could misuse its system for personal surveillance. By August 2026, reporting had identified at least 50

law enforcement officers accused, charged, or convicted of misusing Flock or other license plate reader systems. This does not include those merely disciplined or terminated. Flock nevertheless has left important anti-abuse protections optional, when Flock has provided them at all.

68. Notwithstanding this, Flock's Chief Executive Officer Garrett Langley repeatedly characterized Flock misuse as comparatively insignificant. In April 2026, Langley marginalized Flock's role in the misuse. Further, in balancing the incidents with the number of investigations he maintained that Flock technology supported, Langley characterized that as "a trade-off that I can make." In a later interview, Langley called abuse "exceptionally rare."[31]

69. Flock has taken a similar approach to failures in the accuracy of its technology. Flock publicly states that, under optimal conditions, its cameras accurately read more than 96% of license plate characters. But Roseville, California repeatedly reported substantial real-world errors directly to Flock. Flock responded publicly by continuing to emphasize its greater-than-96% character-recognition figure under optimal conditions and blaming Roseville. Flock also asserted that Roseville's performance had significantly improved, an assertion Roseville disputed.[32]

[31] Proton Team, We Asked Flock's CEO About Surveillance Abuse. Here's What He Said, Proton (Aug. 19, 2026), https://proton.me/blog/flock-ceo-interview (last accessed August 25, 2026).
[32] 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 accessed August 25, 2026).

70. Even Flock's own headline accuracy claims obscure the practical magnitude of error created by a surveillance network operating at Flock's scale. Flock states that its network records approximately 20 billion vehicle reads each month. A 96% accuracy rate applied to 20 billion readings would leave approximately 800 million inaccurate readings each month, or 9.6 billion over a year. Other Flock materials have stated a 93% plate-read accuracy rate; at the same scale, that would imply approximately ***1.4 billion*** inaccurate readings each month. Thus, even accepting Flock's own advertised accuracy figures, a seemingly small percentage error can translate into billions of inaccurate records annually when multiplied across Flock's nationwide surveillance network.

71. Thus Flock's response to known problems has followed a recurring pattern. Faced with repeated personal misuse, Flock has characterized the problem as rare, isolated misconduct by "bad apples" and emphasized the volume of crimes it claimed the system helped solve. Faced with substantial documented accuracy problems reported directly by a customer, Flock emphasized an optimal-conditions accuracy percentage and blamed the customer. And when public scrutiny intensified, Flock made selective improvements but failed to address larger systemic issues. Flock has known its system presented recurring risks of both abuse and technological error but repeatedly has minimized the practical significance and scale of those risks rather than timely imposing safeguards commensurate with the breadth and power of the surveillance system it had built.

F. Defendant's Actions Have Caused Plaintiff and Class Members Harm as a Result of Their Exposure to Flock's System

72. In order to go to work, Plaintiff is subjected to surveillance by Flock cameras. Upon information and belief, even if she were to alter her route, she would not be able to avoid Flock surveillance.

73. Every day, Plaintiff and Class members are forced to travel through the Flock camera areas of capture to reach their places of employment and school, and to engage in basic everyday activities such as grocery shopping or simply engaging in activities for leisure. Notwithstanding their doing nothing to warrant law enforcement surveillance, they nevertheless are aggressively and pervasively surveilled, with their likenesses and vehicle information captured, stored and disseminated.

74. In addition to invading Plaintiff and Class members' privacy, this surveillance subjects them to the systemic errors and misuse described above. As a result, Plaintiff and Class members have suffered harm.

CLASS ACTION ALLEGATIONS

75. Plaintiff seeks certification of the following Class under Rule 23 of the Federal Rules of Civil Procedure:

> All individuals in the United States whose license plate data was collected by Flock using an automated license plate recognition system operated by Flock since January 1, 2024.

76. Excluded from the Class are Flock; its officers, directors and employees; any entity in which Flock has a controlling interest; the judge assigned to this action and

members of the judge's immediate family; and any person who timely and validly requests exclusion from any certified damages class.

77. Plaintiff reserves the right to modify or amend the definition of the Class and/or add Subclass(es) before the Court determines whether certification is appropriate.

78. The Class meets the criteria for certification under Rule 23.

79. **Numerosity**. The members of the Class are sufficiently numerous that joinder is impracticable. Documented incidents already involve multiple agencies and numerous law enforcement officers and employees accused, charged, disciplined or terminated for non-law enforcement Flock searches. Several matters identify multiple personal targets or repeated searches of the same target. Upon information and belief, additional Class members are identifiable from Flock and agency audit records, which record the user, date, time, stated purpose and query information associated with searches. The precise number and identities of Class members are principally within Flock's records.

80. **Common questions of law and fact predominate.** Common questions of law and fact predominate, including whether Flock knew or should have known that users could use legitimate Flock access for non-law enforcement purposes; what portions of the access, search, justification, sharing, logging, auditing and misuse-safeguard architecture Flock designed, supplied, operated or materially controlled; whether Flock exercised reasonable care in designing and operating those controls; what abnormal use monitoring and intervention functions Flock controls; whether disclosures or warnings

Flock provides to agencies concerning the limits of its safeguards are sufficient; whether Flock facilitated unauthorized access through the challenged architecture; and whether Flock's conduct was reckless, willful or wanton. Additional common questions include whether Flock's conduct caused or contributed to actual unauthorized access to Class members' ALPR information; and whether Class members are entitled to common forms of relief under applicable law.

81. **Typicality.** Plaintiff's claims are typical because, upon information and belief, her ALPR information has been recorded, retained and shared through the Flock network.

82. **Adequacy**. Plaintiff will fairly and adequately protect the interests of the Class. Her interests are aligned with those of the Class, and she has retained counsel experienced in complex and class litigation.

83. **Superiority.** A class action is superior to individual litigation. The core liability questions concern common Flock architecture, controls, knowledge and safeguards. Many Class members will have no reason to know their information was improperly searched because user queries are not visible to the person being searched, while Flock and agency audit records record the activity. Separate actions would duplicate that inquiry and risk inconsistent adjudications concerning the same Flock-controlled mechanisms.

84. Flock acted or failed to act on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole. The

prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Flock. Such individual actions would create a risk of adjudications which would be dispositive of the interests of other Class members and impair their interests. Flock has acted and/or refused to act on grounds generally applicable to the Class as a whole, making final injunctive relief or corresponding declaratory relief appropriate.

COUNT I — INVASION OF PRIVACY

(On Behalf of Plaintiff and the Class)

85. Plaintiff repeats and realleges every allegation contained in paragraphs 1 through 84 as if set forth fully herein.

86. Plaintiff and Class members have a reasonable privacy interest in their movements, routines, associations and other private affairs that can be revealed through the systematic collection and aggregation of vehicle location information.

87. Flock intentionally designed, operates and maintains a nationwide surveillance system that automatically collects vehicle and license plate information together with the time and location at which vehicles are detected, retains that information in searchable databases and enables vehicle location information collected across multiple cameras and jurisdictions to be searched and aggregated.

88. Through that system, Flock collects, maintains and disseminates information concerning Plaintiff's and Class members' movements without their consent and without regard to whether they are suspected of criminal activity.

89. The systematic collection, retention and aggregation of that information permits Flock's system to reveal information concerning where Plaintiff and Class members travel, the places they frequent and, depending upon the frequency and location of detections, aspects of their routines and associations.

90. Flock's collection and aggregation of vehicle location information on this scale and its creation and maintenance of searchable records capable of revealing individuals' movements and private affairs constitute a substantial intrusion that would be highly offensive to a reasonable person.

91. Plaintiff and the Class have been subjected to Flock surveillance during their ordinary activities.

92. Flock knew that its system is designed to and in fact systematically collects and aggregates vehicle location information concerning persons who are not suspected of criminal activity and knew or should have known that the resulting searchable records could reveal information concerning their movements, routines and associations.

93. The access and surveillance would be highly offensive to a reasonable person.

94. As a direct and proximate result of Flock's conduct, Plaintiff and Class members have suffered invasion of their privacy and loss of control over information

concerning their movements, activities, routines and associations and have suffered damages.

COUNT II — NEGLIGENCE

(On Behalf of Plaintiff and the Class)

95. Plaintiff repeats and realleges every allegation contained in paragraphs 1 through 84 as if set forth fully herein.

96. Flock designed, supplied, operates and materially controls portions of the collection, retention, search, sharing, logging, auditing and misuse-safeguard functions through which law enforcement agencies obtain and use vehicle location information.

97. Flock knew or should have known that its system creates searchable records associating vehicles with particular locations and that access to those records could be misused for personal or other non-law enforcement surveillance.

98. Flock further knew or should have known from recurring misuse incidents, audit information, customer communications and its own product development that authentication, user-supplied search reasons and retrospective auditing alone did not eliminate the risk of improper use.

99. Flock owed Plaintiff and similarly situated citizens a duty to exercise reasonable care in the Flock-controlled functions governing collection, retention, access, sharing, auditing and safeguards against foreseeable misuse of their vehicle location information.

100. Flock breached that duty by failing to exercise reasonable care in the design, implementation and operation of reasonable safeguards governing access to and use of vehicle location information, including reasonable preventive controls, timely identification or surfacing of improper or abnormal use and reasonable response and intervention mechanisms.

101. Upon information and belief, Flock also failed to exercise reasonable care in the retention, sharing and access settings applicable to vehicle location information to the extent those settings exposed information beyond what was reasonably necessary for legitimate law enforcement purposes.

102. Flock's failure to exercise reasonable care was reckless and willful.

103. Plaintiff and the Class are therefore entitled to damages, including punitive damages, caused by Flock's conduct in an amount to be proven at trial.

COUNT III — NEGLIGENT DESIGN

(On Behalf of Plaintiff and the Class)

104. Plaintiff repeats and realleges every allegation contained in paragraphs 1 through 84 as if set forth fully herein.

105. Flock had a duty to exercise reasonable care in selecting and implementing the design of Flock-controlled functionality relevant to the foreseeable risk that law enforcement users would use legitimate access for personal or other unauthorized purposes.

106. Flock's relevant design choices included search-purpose requirements, access and sharing controls, audit logging, tools capable of excluding prohibited searches, functionality capable of identifying abnormal or suspicious search activity and mechanisms for review, escalation, restriction or interruption when potential misuse is surfaced.

107. Flock's own products demonstrate that improper-use safeguards are technically cognizable. Flock has implemented search-term exclusion, case-number functionality, sharing controls and automated monitoring that analyzes recorded activity and surfaces atypical search patterns.

108. Flock has not publicly stated that the absence or limits of such controls during the relevant period resulted from technological infeasibility.

109. Plaintiff alleges that a reasonably designed safeguard architecture could have included reasonable preventive controls against defined improper access, reasonable mechanisms to identify or surface abnormal or repetitive user activity for timely review and reasonable mechanisms to respond to identified misuse before it continued unchecked.

110. Flock failed to exercise reasonable care in selecting and implementing a safeguard design reasonably adequate to address the foreseeable user misuse mechanism alleged herein across prevention, detection and response.

111. Flock's failure to exercise reasonable care was reckless and willful.

112. As a direct and proximate result of Flock's negligent design, Plaintiff and Class members suffered actual unauthorized access to or use of their ALPR information, loss of privacy and confidentiality and resulting damages in an amount to be proven at trial.

COUNT IV — FAILURE TO WARN

(On Behalf of Plaintiff and the Class)

113. Plaintiff repeats and realleges every allegation contained in paragraphs 1 through 84 as if set forth fully herein.

114. Upon information and belief, Flock knew or should have known that law enforcement users could misuse otherwise legitimate Flock access for personal and other non-law enforcement purposes, including stalking, tracking and repeated personal surveillance.

115. Upon information and belief, Flock knew or should have known that search-reason requirements and retrospective audit logs alone did not eliminate that risk and that customer agencies required adequate warnings, instructions and guidance concerning the risk of user misuse and the need to configure, monitor, audit and respond to Flock usage in a manner reasonably calculated to prevent or timely identify such misuse.

116. Upon information and belief, because Flock designed, supplied and operated material portions of the relevant access, search, logging, auditing and safeguard architecture and possessed knowledge concerning recurring misuse and the operation and limitations of its own safeguards, Flock had a duty to provide reasonable and adequate

warnings and instructions concerning known or reasonably foreseeable risks associated with improper user access and the measures reasonably available to address those risks.

117. Upon information and belief, Flock failed to provide law enforcement customers with warnings, instructions or guidance reasonably adequate to communicate the nature and extent of the recurring user misuse risk, the limitations of relying on user-entered search reasons and retrospective auditing and the need for appropriate preventive, monitoring, audit, configuration and intervention measures.

118. Upon information and belief, adequate warnings and instructions would have caused law enforcement agencies to adopt, enable, configure, use or enforce additional safeguards or review practices that would have prevented, identified, limited or interrupted at least some improper searches of Plaintiff and Class members.

119. Upon information and belief, Flock's failure to provide adequate warnings and instructions caused or materially contributed to the occurrence, continuation or delayed identification of improper user searches of Plaintiff and Class members.

120. Flock's failure to warn was reckless and willful.

121. As a direct and proximate result, Plaintiff and Class members suffered unauthorized access to or use of their ALPR information and resulting damages, including punitive damages, in an amount to be proven at trial.

COUNT V — INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

(On Behalf of Plaintiff and the Class)

122. Plaintiff repeats and realleges every allegation contained in paragraphs 1 through 84 as if set forth fully herein.

123. Flock operates a powerful law enforcement surveillance system capable of creating searchable records of a person's movements and has continued to operate and expand that system despite recurring incidents in which Flock access was used for personal surveillance.

124. Flock's continued facilitation of broad vehicle location collection and searching without safeguards reasonably sufficient to prevent or timely surface known categories of personal misuse constitutes, upon information and belief, reckless, willful and wanton disregard for the privacy and security of persons whose movements are recorded through the system.

125. Under the circumstances alleged, Flock's reckless, willful and wanton conduct was extreme and outrageous.

126. Flock's architecture facilitated the unlawful surveillance, and its alleged failure to employ adequate safeguards caused or materially contributed to the unauthorized access, its continuation or both.

127. As a result, Plaintiff and the Class have suffered severe and continuing emotional distress and lasting impairment of their well-being and quality of life.

128. Therefore, Plaintiff and the Class are entitled to damages, including 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 the Class under Rule 23, appoint Plaintiff as Class Representative and appoint her counsel as Class Counsel;

B. Enter judgment in favor of Plaintiff and the Class on Counts I through V;

C. Award compensatory and consequential damages;

D. Award punitive damages;

E. Award the expenses of litigation and attorneys' fees;

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

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

JURY DEMAND

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

Respectfully submitted, this 25th day of August, 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

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Class Action Lawsuit Alleges Flock Enables Law Enforcement Personnel to Misuse Vehicle Location Info for Surveillance, Stalking

---