

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
NEWNAN DIVISION**

TYLER MURKERSON, individually
and on behalf of a class of similarly
situated persons,

Plaintiff,

v.

FLOCK GROUP, INC. d/b/a FLOCK
SAFETY; COWETA COUNTY,
GEORGIA; WILLIAM FAULKNER,
individually; RANDALL S.
FAULKNER, individually;
JOHN DOES 1–3, individually;
SHERIFF LEONARD C. WOOD a/k/a
LENN WOOD, in his individual
capacity and in his official capacity as
SHERIFF OF COWETA COUNTY,
GEORGIA;

Defendants.

CIVIL ACTION FILE NO.

**CLASS ACTION COMPLAINT
FOR DAMAGES AND
INJUNCTIVE RELIEF**

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE
RELIEF**

Plaintiff Tyler Murkerson, individually and on behalf of a class of similarly situated persons, by and through undersigned counsel, files this Complaint for Damages and Injunctive Relief against the above-named Defendants, showing the Court as follows:

NATURE OF THE ACTION

1. This case is about what happened to a man who sued the police for violating his constitutional rights — and about what a surveillance system built without safeguards makes possible for anyone who sues the police, files a complaint against them, or otherwise draws their attention.

2. On February 6, 2023, Plaintiff Tyler Murkerson was arrested by Coweta County Sheriff's Office deputies following a stop in a gas station parking lot at the Charlie B. Johnson Road intersection in Coweta County, Georgia. Every charge against him was dismissed on June 26, 2023. He then did what the Constitution entitles him to do: on September 9, 2024, he filed suit against the two deputies who arrested him and against the Sheriff of Coweta County. That lawsuit — *Murkerson v. Teare, Brooks & Wood*, Civil Action No. 3:24-cv-00162-LMM (N.D. Ga.) — remained pending until it resolved in or about August 2026.

3. While that lawsuit was pending, deputies of the Coweta County Sheriff's Office used the Flock Safety automated license plate recognition ("ALPR") network, and associated state and federal law enforcement databases, to surveil Mr. Murkerson. According to Flock audit records obtained through public records requests and published at haveibeenflocked.com, his vehicle was the subject of a surveillance period spanning 197 days, from May 4, 2025 through November 18,

2025, with 167 days between the first and last recorded search. Five searches were attributed to the Coweta County Sheriff's Office, two of them by operators identified in the records as "r.fau" and "w.fau," and each reached across more than six thousand agency camera networks nationwide. Only two of the five searches have been disclosed; the details of the other three remain concealed.

4. The surveillance did not stay behind a screen. During the same period, Mr. Murkerson observed an unprecedented Sheriff's Office presence when driving, including on his routes home from work. Deputies parked within a quarter mile of his driveway on a dead-end road and in the parking lot of his business when he was there. The surveillance, upon information and belief, informed the Sheriff's Office of Mr. Murkerson's daily routine. As the civil rights lawsuit proceeded, Mr. Murkerson also experienced two roadblocks: one at the intersection where the underlying incident occurred and one, days later, on the road to his home, set up at a time that appears calculated to intercept him on his commute.

5. Mr. Murkerson told his wife he believed he was being followed and watched by the Coweta County Sheriff's Office. She suggested he was imagining it. He came to doubt his own perception, worried that he was "going crazy," and gave up a six-year business relationship servicing a neighboring police

department's vehicles because he no longer believed he was safe doing that work. He was not imagining it. The audit trail proves it.

6. What happened to Mr. Murkerson was not an aberration, and this case is not only about him. It was the predictable output of a surveillance system built without the one control that would have prevented it: a requirement that the officer running a search identify the investigation the search was for. Georgia law permits access to captured license plate data only for a "law enforcement purpose," which the General Assembly defined narrowly as "the investigation of an offense or activity initiated by a law enforcement agency." O.C.G.A. § 35-1-22(a)(4), (b). Yet throughout the relevant period Flock's platform required only that some text be entered in a free-form field, and it accepted whatever was typed — "investigation" and, on twenty separate occasions at one department, "hehehe." The only justifications entered for the searches of Mr. Murkerson's vehicle were "info" and "37." Neither corresponds to any investigation, case, incident, or call for service. A search recorded that way documents no investigation. It documents only that someone typed something.

7. Flock has since conceded, by its own conduct, that its platform should have required a verifiable law enforcement justification before executing a search. In August 2026 — after these searches, after the Georgia Bureau of Investigation

began arresting Georgia officers for misusing the system, and after investigative reporting exposed dozens of cases of abuse — Flock announced that case codes and its misuse-detection tool would become mandatory for its law enforcement customers by the end of 2026, that it had already made multifactor authentication mandatory at the beginning of that month, and that its default data retention period would be cut from thirty days to seven. Flock Safety, Flock Updates Privacy, Accountability, Security, and Transparency Safeguards (Aug. 13, 2026); see Jason Koebler, Cops Keep Getting Arrested for Using Flock to Stalk People, 404 Media (June 10, 2026); Drew Harwell, Douglas MacMillan & Aaron Schaffer, How Rogue Officers Turned a Nationwide Camera Network into a Tool for Stalking, Wash. Post (Aug. 2, 2026). Every one of those measures was available to Flock before Mr. Murkerson's vehicle license plate was ever searched.

8. Running a citizen's license plate and identity through law enforcement databases for a non-law-enforcement purpose is a crime in Georgia, O.C.G.A. § 35-1-22(d)(1); examining another person's personal data through a computer network without authority is a felony, O.C.G.A. § 16-9-93(c); and obtaining personal information from a motor vehicle record for an impermissible purpose is independently actionable under federal law, 18 U.S.C. § 2724.

9. The Coweta County Sheriff's Office knows the law prohibits those acts. In or about August 2026 — the same month Mr. Murkerson's civil rights lawsuit concluded — the Coweta County Sheriff's Office announced that an internal audit of its Flock Safety usage had flagged employee accounts, that three employees had resigned before the audit was completed, and that it had asked the Georgia Bureau of Investigation to conduct an independent investigation of those employees' conduct.

10. Defendant Flock Group, Inc. built the offending instrument and knew of its misuse before Mr. Murkerson was searched. It designed, sold, hosted, and operated the platform; it configured the retention and network-sharing settings that made a months-long nationwide lookback possible; and it accepted "info" and "37" as sufficient justification to execute a search. Flock waited until April 2026 to make available a product designed to detect exactly this kind of operator misuse — proof that the safeguard was feasible, available, and known to Flock, and that the misuse was foreseeable to Flock, Coweta County, and Sheriff Wood alike.

11. Plaintiff brings this action individually and, as set forth in the Class Action Allegations below, on behalf of a Class of persons whose vehicles were searched on Flock's platform in exactly the same undocumented way — where neither Flock's audit record for the search nor the searching agency's own records

reflect any case, incident, call for service, or official investigation to which the search corresponds, or where a law enforcement agency has itself determined that the search lacked a lawful purpose — two Subclasses, and a class seeking declaratory and injunctive relief only. Membership in that Class is determined from Flock's own database and agency records; it requires no inquiry into any class member's circumstances and no adjudication of any officer's state of mind. Against the Officer Defendants, Plaintiff asserts claims under the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–2725; 42 U.S.C. § 1983 for violations of the First, Fourth, and Fourteenth Amendments; the Georgia Racketeer Influenced and Corrupt Organizations Act, O.C.G.A. § 16-14-1 et seq.; the Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-90 et seq.; and Georgia common law. Against Sheriff Wood, he asserts claims under 42 U.S.C. § 1983 for supervisory liability and, individually and on behalf of the Coweta Subclass, for policymaker liability arising from the procurement, renewal, and continuation of the Flock Safety contract — the latter pleaded in the alternative against Coweta County. Individually and on behalf of the Class, he sues Flock for negligence, for breach of the legal duties imposed by O.C.G.A. § 35-1-22 and enforceable under O.C.G.A. § 51-1-6, and for invasion of privacy. He seeks compensatory, liquidated, treble, and punitive damages, attorney's fees, and injunctive relief requiring that unlawfully obtained records be purged, that his and Class members' identifiers be removed

from any active alert or watch list, and that Flock be required to validate search justifications in Georgia going forward.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over Plaintiff's federal claims pursuant to 28 U.S.C. § 1331 (federal question) and 28 U.S.C. § 1343(a)(3) (civil rights), and pursuant to 18 U.S.C. § 2724(a), which authorizes a civil action in a United States district court.

13. This Court has supplemental jurisdiction under 28 U.S.C. § 1367(a) over Plaintiff's Georgia law claims and over the Georgia law claims asserted on behalf of the Class in Counts X, XI, and XII. Those claims derive from a common nucleus of operative fact with Plaintiff's federal claims — the same Flock Safety platform, the same search and audit architecture, and the same design and operational decisions by Flock — and are such that Plaintiff would ordinarily be expected to try them in one judicial proceeding. Plaintiff does not invoke jurisdiction under 28 U.S.C. § 1332(d), because Flock is a citizen of Georgia by reason of its principal place of business and the proposed Class is limited to searches conducted by Georgia law enforcement agencies.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because all Defendants reside in this District — Flock maintaining its headquarters and principal place of business in Fulton County, Georgia — and because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District.

15. This Court has personal jurisdiction over Flock because Flock maintains its headquarters and principal place of business in Georgia, is registered to do business in Georgia, contracts with Georgia law enforcement agencies including the Coweta County Sheriff's Office, owns and operates ALPR cameras throughout Georgia and specifically within Coweta County, and purposefully collects, stores, and makes searchable the vehicle location data of Georgia residents. Plaintiff's claims arise out of and relate to those Georgia contacts.

16. Assignment to the Newnan Division is proper because the acts complained of occurred in Coweta County, Georgia, which lies within the Newnan Division.

17. Plaintiff has suffered a concrete injury sufficient to confer Article III standing. Defendants did not merely violate a statute in the abstract: they obtained, viewed, and used Plaintiff's personal information and the record of his physical movements, and they did so repeatedly over a period of months. That injury bears

a close relationship to harms traditionally recognized at common law as providing a basis for suit — including intrusion upon seclusion, Restatement (Second) of Torts § 652B, a tort Georgia has recognized since *Pavesich v. New England Life Insurance Co.*, 122 Ga. 190, 50 S.E. 68 (1905). Plaintiff further suffered downstream harm, including fear, anxiety, loss of a longstanding business relationship, and alteration of his daily routines and movements.

PARTIES

18. Plaintiff Tyler Murkerson is a natural person and a citizen of the State of Georgia. He resides in Heard County, Georgia, near the road that forms the boundary between Heard County and Coweta County. At all relevant times he was the registered owner and principal operator of the vehicle bearing the license plate that is the subject of the surveillance records described herein.

19. Defendant William Faulkner is, or at all relevant times was, a deputy or employee of the Coweta County Sheriff's Office and an authorized user of the Flock Safety ALPR platform and of Georgia and federal law enforcement databases, identified in the Flock audit records as operator "w.fau." He is sued in his individual capacity.

20. Defendant Randall S. Faulkner is, or at all relevant times was, a deputy or employee of the Coweta County Sheriff's Office and an authorized user of the Flock Safety ALPR platform, identified in the Flock audit records as operator "r.fau." He is sued in his individual capacity.

21. Defendants John Does 1, 2, and 3 are the individual operators who conducted the three searches of Plaintiff's vehicle identifier that appear in the Flock Safety audit record for identifier 78fee87f but whose operator name, date, time, and stated reason were withheld from public disclosure. Each is identifiable by a unique, machine-generated audit log entry, maintained by Flock and by the Coweta County Sheriff's Office, that records the operator account, the date and time of the query, the terminal or originating agency identifier, and the reason entered; each entry corresponds to exactly one human being. Upon information and belief, each of John Does 1 through 3 is or was a deputy, employee, or other authorized user of the Coweta County Sheriff's Office, or of an agency with which that office shares Flock Safety network access. They are sued in their individual capacities.

22. Upon information and belief, the details of those three searches were withheld from public disclosure because they are the subject of the ongoing Georgia Bureau of Investigation inquiry into Coweta County Sheriff's Office employees' Flock usage described below — the searchers being among the

employees whose accounts were flagged in the agency's August 2026 internal audit, who resigned before that audit was completed, and/or whose conduct was referred for criminal investigation — or because they were conducted by or shared with an agency outside Georgia not subject to the Georgia Open Records Act.

23. Defendant Sheriff Leonard C. Wood a/k/a Lenn Wood ("Sheriff Wood") is, or at all relevant times was, the duly elected Sheriff of Coweta County, Georgia, and the final policymaker for the Coweta County Sheriff's Office with respect to the acquisition, configuration, use, auditing, supervision, and discipline of employee access to the Flock Safety ALPR platform and to state and federal law enforcement databases. He was the Sheriff on February 6, 2023, and was personally named as a defendant, in his individual capacity, in the Underlying Action described below. He is sued in his individual capacity for damages on theories of supervisory liability (Count V) and policymaker liability (Count XIII), and in his official capacity solely for prospective declaratory and injunctive relief.

24. Defendant Flock Group, Inc. d/b/a Flock Safety ("Flock") is a corporation organized under the laws of the State of Delaware with its headquarters and principal place of business at 1160 Howell Mill Road NW, Suite 210, Atlanta, Fulton County, Georgia. Flock designs, manufactures, markets, sells, hosts, configures, and operates the automated license plate recognition cameras,

databases, search software, network-sharing architecture, access controls, audit logging, and misuse-detection functionality at issue in this action. Flock may be served through its registered agent, Registered Agents Inc., located at 8735 Dunwoody Place, Suite R, Atlanta, GA 30350.

25. Defendant Coweta County, Georgia ("the County") is a body corporate and a political subdivision of the State of Georgia. The County acts through its governing authority, the Coweta County Board of Commissioners, which is the County's final policymaker with respect to the procurement, funding, approval, renewal, and termination of contracts to which the County is a party. The County may be served through the Chairman of the Coweta County Board of Commissioners.

26. Plaintiff asserts no claim under Georgia law against the County. The claims asserted against the County arise under 42 U.S.C. § 1983.

27. Defendants William Faulkner, Randall Faulkner, and John Does 1 through 3 are referred to collectively as the "Officer Defendants." At all relevant times, each Officer Defendant, and Defendant Sheriff Wood, acted under color of the statutes, ordinances, regulations, customs, and usages of the State of Georgia and Coweta County. Each Officer Defendant accessed the Flock Safety platform and the law enforcement databases at issue using credentials, terminals, originating

agency identifiers, and authority conferred upon him solely by virtue of his employment as a law enforcement officer. No Officer Defendant could have accessed any of these systems as a private citizen. No claim under 42 U.S.C. § 1983 is asserted against Flock.

FACTUAL ALLEGATIONS

A. The Flock Safety ALPR Network and What It Reveals

28. Flock designs, manufactures, sells, and operates a nationwide network of automated license plate recognition cameras and the software platform through which law enforcement agencies search the resulting data.

29. Unlike a traffic camera, which activates only upon detecting a violation, a Flock ALPR camera photographs every vehicle that passes within its field of view. It captures the license plate, converts it to machine-readable text, and records the date, time, and precise location of the sighting, together with vehicle characteristics such as make, color, and distinguishing features. It frequently captures images of drivers and passengers as well.

30. The captured data is uploaded to Flock's centralized databases, where it becomes searchable. A single camera establishes that a vehicle was at one place at

one time. A network of cameras, searched together and over time, produces a history of where a vehicle has been — and therefore where its driver has been.

31.Flock markets that aggregation as a product feature. Its platform offers statewide and nationwide search capability reaching thousands of participating agency networks, and Flock promotes tools designed to identify recurring locations, common appearances, and travel associations.

32.Flock's platform does not merely return a list of discrete sightings. Flock markets analytic tools that operate on its stored data, including "Investigations Manager," which analyzes movement patterns to flag vehicles as suspicious; "Multi-State Insights," which alerts users when a vehicle has been detected in multiple states; "Linked Vehicles" or "Convoy Search," which identifies vehicles frequently seen together; and "Multiple locations search," which identifies vehicles seen at multiple locations. Jay Stanley, Surveillance Company Flock Now Using AI to Report Us to Police if It Thinks Our Movement Patterns Are "Suspicious," ACLU (July 23, 2025) (quoting Flock marketing materials); see also Flock Safety, The Future of Investigations: How Flock's New AI-Powered Tools Are Transforming Vehicular Evidence (Feb. 14, 2025) (Multi-State Insights). Each of these tools converts stored sightings into an analysis of where a particular vehicle goes, how often, and in whose company.

33. A single query on Flock's platform can simultaneously reach hundreds of other agencies' Flock networks, and once an agency grants another agency access to its network, the outside agency can search that data without seeking approval for any individual search. Tomo Chien, *California Cops Are Breaking Surveillance Laws. Who's Going to Stop Them?*, S.F. Standard (July 23, 2025). An agency that enables Flock's nationwide sharing both shares its data with, and can search the data of, every other agency nationwide that has done the same. Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, ACLU of Massachusetts (Oct. 7, 2025). And Flock generates "instant alerts when a vehicle matches a customer-defined or NCIC hot list." Flock Safety, Flock LPR (product page) (visited Sept. 29, 2026). Through that architecture, license plate data captured by Georgia agencies is exposed to searches by agencies the capturing Georgia agency never selected, including agencies outside Georgia that are beyond the practical reach of the audit and enforcement mechanisms of O.C.G.A. § 35-1-22.

34. Because vehicle travel is not random, aggregated ALPR data is revealing in a way that a single sighting is not. A vehicle's repeated presence at particular locations reflects where its owner lives, works, shops, worships, socializes, seeks medical care, and travels. Searched across months, the resulting record is a map of a person's life.

35. Georgia law recognizes the sensitivity of this data and restricts its use. O.C.G.A. § 35-1-22(b) provides that captured license plate data "shall be stored immediately upon collection and not accessed except for a law enforcement purpose"; § 35-1-22(a)(4) defines "law enforcement purpose" narrowly as "the investigation of an offense or activity initiated by a law enforcement agency"; § 35-1-22(e) requires every agency deploying an ALPR system to "maintain policies for the use and operation of such system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data consistent with this Code section"; and § 35-1-22(d)(1) makes it a misdemeanor of a high and aggravated nature for "[a]ny person" to "knowingly request[], use[], obtain[], or attempt[] to obtain captured license plate data of a law enforcement agency under false pretenses or for any purpose other than for a law enforcement purpose."

36. By 2018, therefore, Georgia law gave every law enforcement officer in this State fair and clear warning that captured license plate data may be accessed only to investigate an offense or activity initiated by a law enforcement agency, and that accessing it for any other purpose is a crime. That prohibition is specific, categorical, and directed at the precise conduct alleged in this Complaint. No reasonable officer could have believed, at any time after 2018, that querying a

private citizen's vehicle identifier with no investigation, no case, no incident, and no call for service was lawful.

37. The Flock platform requires an operator to enter text in a "reason" field before it will execute a search, but — as alleged below — it did not require that the text identify any investigation, case, or incident. The platform logs each search, including the operator's username, the date and time, the stated reason, and the identifier searched. Those audit logs are the record of who looked, when, and why.

B. The Risk of Misuse Was Known and Legislated Against Long Before 2025

38. The risk that a law enforcement officer with access to a license plate reader system would use it to track a spouse, a former partner, a neighbor, or an adversary was identified, documented, and addressed by professional associations, federal agencies, state legislatures, and state auditors more than a decade before the searches at issue in this action.

39. In September 2009, the International Association of Chiefs of Police published a privacy impact assessment for license plate readers recognizing that any organization maintaining records of personal data "must take precautions to prevent misuse of the data," and advising that "[c]reating tamper-proof audit trails as well as conducting real-time monitoring and analyzing LPR system usage can

all function to protect the public's privacy interests." Int'l Ass'n of Chiefs of Police, Privacy Impact Assessment Report for the Utilization of License Plate Readers (Sept. 2009).

40. In September 2012, the International Association of Chiefs of Police, under a grant from the National Institute of Justice, published operational guidance reporting that agency ALPR policies typically "[r]estrict and audit queries of the ALPR dataset," and finding that only 48 percent of responding agencies (19 agencies) reported having a policy addressing ALPR use and operations. David J. Roberts & Meghann Casanova, Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement (Int'l Ass'n of Chiefs of Police, Sept. 2012) (NIJ Grant No. 2007-MU-MU-K004; NCJ 239604).

41. On February 20, 2013, the Minnesota Office of the Legislative Auditor reported that "88 law enforcement personnel misused DVS data" in fiscal year 2012 and that, although query records were maintained, "neither division does much monitoring of the records to identify misuse." Office of the Legislative Auditor, State of Minnesota, Law Enforcement's Use of State Databases (Feb. 20, 2013).

42. On July 17, 2013, the American Civil Liberties Union published a national report warning that "[a]nyone with access to these systems could track his

boss, his ex-wife, his romantic or workplace rivals, friends, enemies, neighbors, family, and so forth." Am. Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements* (July 2013).

43. In 2015 — two years before Flock was founded — the Minnesota Legislature enacted Minn. Stat. § 13.824, which conditions access to ALPR data on a "legitimate, specified, and documented law enforcement purpose," requires that each access record "include a record of the factual basis for the access and any associated case number, complaint, or incident," requires that all queries "be recorded in a data audit trail," and requires an "independent, biennial audit" of those records.

44. On September 28, 2016, the Associated Press reported the results of a nationwide review of law enforcement misuse of confidential databases, including criminal-history and driver databases, finding that between 2013 and 2015 officers and employees "were fired, suspended or resigned more than 325 times" for such misuse and "received reprimands, counseling or lesser discipline in more than 250 instances."

45. In February 2017 — the same year Flock was founded — the Bureau of Justice Assistance of the United States Department of Justice published a model

License Plate Reader Policy Development Template for Use in Intelligence and Investigative Activities, providing that every query be logged with "[t]he authorized law enforcement or public safety justification for access, including a relevant case number if available," that agencies conduct "periodic random auditing" of system use, and that misuse be sanctioned up to referral "for criminal prosecution."

46. In 2018, the Georgia General Assembly enacted O.C.G.A. § 35-1-22, restricting access to captured license plate data to a law enforcement purpose, making misuse a crime, and requiring every agency operating an ALPR system to "maintain policies for the use and operation of such system, including . . . policies for the training of law enforcement officers." Ga. L. 2018, p. 758, § 1/HB 79. From that date forward, Flock — headquartered in Georgia — and every Georgia law enforcement officer were on notice, by criminal statute, that accessing captured license plate data for any other purpose was unlawful.

47. According to published accounts of the statements of the bill's sponsor, Representative John Pezold, the Georgia Sheriffs' Association — of which the Sheriff of Coweta County was at all relevant times a member — participated in negotiating the terms of House Bill 79, objecting to a shorter data-retention period and seeking the 30-month period ultimately enacted. Kevin Angell, Georgia Saw

the License Plate Reader Problem Coming, Now Georgia (Aug. 19, 2026); Two Peachtree City Officers Gone After Flock Misuse: Reform Is Needed, The Citizen (Sept. 10, 2026). The criminal penalty for misuse was enacted in the same bill. O.C.G.A. § 35-1-22(d)(1); Ga. L. 2018, p. 758, § 1. Upon information and belief, the Sheriff of Coweta County was at all relevant times a member of the Georgia Sheriffs' Association; Georgia's sheriffs therefore cannot maintain that the risk of misuse of captured license plate data was unknown to Georgia law enforcement leadership when that leadership helped to write the statute addressing it.

48. On February 13, 2020, the California State Auditor reported that none of the law enforcement ALPR programs it reviewed "had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate," while noting that, when conducting a search, staff "are prompted to enter a case number and the purpose of the search, and they may do so by typing in text" — underscoring that a justification requirement is only as good as the validation behind it. California State Auditor, Report 2019-118, Automated License Plate Readers: To Better Protect Individuals' Privacy, Law Enforcement Must Increase Its Safeguards for the Data It Collects (Feb. 13, 2020).

49. From January 2022 through December 2025, a lieutenant of the Fort Bend County, Texas Sheriff's Office used Flock cameras to search two license

plates 41 and 148 times, respectively, including the plate of a vehicle owner with whom, according to the Sheriff's Office's internal affairs records, he had a "very contentious familial relationship," and received a two-day suspension. Lileana Pearson, Fort Bend County Sheriff's Office Lieutenant Admits to Improper Use of Flock Cameras, Per Docs, ABC13 Houston (July 17, 2026).

50. On October 30, 2022, a lieutenant of the Kechi, Kansas Police Department was arrested for using the Wichita Police Department's Flock system to track his estranged wife, and was charged with stalking and unlawful acts concerning computers. Joe Baker, Kechi Police Lieutenant Arrested for Using Police Technology to Stalk Wife, KWCH (Oct. 31, 2022).

51. On November 4, 2022, Flock's Vice President of External Affairs, Josh Thomas, publicly acknowledged both that Flock's system could be abused and that preventing abuse was Flock's own responsibility: "We believe it is our responsibility to make it as difficult as possible to abuse systems like this and to make it as easy as possible to catch anybody if there is an abuse." Shawn Logging, Kechi Police Lieutenant's Arrest Puts Flock Technology Under Scrutiny, KWCH (Nov. 4, 2022).

52. On or about August 18, 2024 — nine months before the first search of Plaintiff's vehicle identifier — it was publicly reported that the former Chief of

Police of Sedgwick, Kansas had used Flock license plate readers to conduct approximately 164 searches of his former girlfriend's vehicle and 64 searches of her new partner's vehicle, recording them as investigations into "a missing child, drug use and suspicious activity" — demonstrating that Flock's free-text reason field did not prevent misuse but concealed it, because a justification field that accepts and records whatever the operator types is not a control. Cameron Burnett, Sedgwick Police Chief Tracked Ex-Girlfriend 164 Times Using License Plate Cams, KAKE (Aug. 18, 2024).

53. Upon information and belief, further instances of law enforcement personnel using Flock's platform to track private individuals for personal reasons occurred beginning in 2024 at the Orange City, Florida Police Department, the Riverside County, California Sheriff's Department, the Stow, Massachusetts Police Department, and the Haines City, Florida Police Department, where an officer searched Flock for his estranged wife's vehicle 717 times between September 2024 and June 2026. See "Dumb as Hell": Orange City Officer Accused of Stalking Woman Using License Plate Readers, WKMG (Feb. 5, 2025); Desert Sun (Nov. 18, 2024) (reporting charges against former Riverside County deputy); Mass. Officer Accused of Misusing Flock System Has Resigned, Boston.com (Aug. 26, 2026); Haines City Officer Arrested for Misusing Flock Cameras to Track Estranged Wife, Officials Say, FOX 13 Tampa Bay (Aug. 11, 2026).

54. Upon information and belief, other Georgia agencies operating the same platform under the same statute audit their personnel's Flock usage as a matter of routine — the Avondale Estates Police Department weekly and the DeKalb County Police Department every two weeks, whose audits in a single seven-month period identified eight employees who had violated agency policy, five of whom had conducted searches without any legitimate law enforcement purpose — while the Coweta County Sheriff's Office undertook no such audit until August 2026. Flock Misuse: 8 Metro Atlanta Officers Suspended over Policy Violations, WSB-TV (Aug. 7, 2026); Jamie Godin, Avondale Police Defend Flock Use Amid Resident Concerns, Decaturish (Aug. 27, 2026).

55. Upon information and belief, Georgia law enforcement personnel were misusing the Flock Safety platform before the searches of Plaintiff's vehicle began: publicly reported Flock audit logs indicate that the searches for which the Chief of Police of Braselton, Georgia was arrested in November 2025, as alleged below, began in or about October 2024, and a deputy of the Coffee County, Georgia Sheriff's Office used the Flock system and other law enforcement databases to track a woman for personal rather than law enforcement purposes in April and May 2024; he was terminated when the investigation began and was indicted by a Coffee County grand jury and arrested in May 2026 following an investigation by the Georgia Bureau of Investigation. Max Chun, Georgia Police Chief Arrested for

Using Flock Cameras for Stalking and Harassment Searched Capitola Data Earlier This Year, Lookout Santa Cruz (Dec. 3, 2025); Taylor Lewis, Former Coffee Co. Deputy Accused of Tracking Woman Through Law Enforcement Systems, WALB (May 8, 2026).

56. Accordingly, by the time Flock designed, sold, configured, hosted, and operated the system deployed in Coweta County, and by the time that system was procured and its contract renewed, the risk that operators would use it to surveil private citizens for personal purposes had been described by a professional association, studied by a federal research agency, quantified by a state auditor, enacted into the law of at least one State, published in a model policy by the Department of Justice, criminalized by the Georgia General Assembly, demonstrated by criminal prosecutions arising from Flock's own platform, and conceded by Flock itself — and a Georgia sheriff or county governing authority exercising ordinary diligence knew or should have known all of it.

C. Coweta County's Flock Deployment

57. Coweta County, Georgia has a population of approximately 160,000 residents. U.S. Census Bureau, QuickFacts: Coweta County, Georgia (July 1, 2025 estimate: 160,240). There are 76 Flock ALPR cameras in Coweta County.

58. At that density, a resident of Coweta County (or someone employed in Coweta County) cannot conduct ordinary daily life — commuting to work, taking children to school, buying groceries, attending church, visiting a doctor — without being repeatedly recorded. Plaintiff cannot reach his home or his place of business without passing Flock cameras, and could not avoid them by altering his route.

59. The Coweta County Sheriff's Office is authorized by Flock as a user of the Flock Safety platform and participates in Flock's regional and national data-sharing networks.

D. The Underlying Civil Rights Action

60. On February 6, 2023, Plaintiff was stopped and arrested by Coweta County Sheriff's Office deputies in the parking lot of the BP gas station located at 4849 Georgia Highway 34, Newnan, Coweta County, Georgia 30263, at or near the intersection of Charlie B. Johnson Road. He was initially charged with a seatbelt violation and obstruction of an officer.

61. The deputies who stopped and arrested Plaintiff were Coweta County Sheriff's Office Deputies Christopher James Teare and Radford Stark Brooks. Neither Teare nor Brooks is named as a Defendant in this action.

62. Plaintiff asserts no claim in this action arising from the February 6, 2023 stop and arrest. Those events were the subject of the Underlying Action and have been resolved. They are alleged here only to the extent necessary to identify the protected activity for which Plaintiff was retaliated against and the persons with a motive to retaliate. Every claim asserted in this Complaint arises from the Flock Safety searches, the associated database queries, and the physical surveillance that occurred after the Underlying Action was filed on September 9, 2024, and from the design, policy, and procurement decisions that made them possible — conduct committed by persons and entities who were not parties to the Underlying Action or, as to Sheriff Wood, in a capacity and through conduct not at issue in it.

63. In summary, the Underlying Action alleged that the stop occurred entirely on private property, where Georgia's seat safety belt statute does not apply; that Plaintiff complied with the deputies' instructions and did not resist; and that the deputies nonetheless took Plaintiff to the ground, tased him, and arrested him.

64. Plaintiff was released on bond and retained criminal defense counsel. The day after counsel's notice of appearance was filed, an accusation was filed adding two additional counts of obstruction of an officer, bringing the total to four charges. On June 26, 2023, the State Court of Coweta County dismissed all four charges.

65. In or about September 2023, Plaintiff retained civil rights counsel. On September 9, 2024, Plaintiff filed a civil action under 42 U.S.C. § 1983 arising from the February 6, 2023 stop and arrest, styled *Murkerson v. Teare, Brooks & Wood*, Civil Action No. 3:24-cv-00162-LMM, in the United States District Court for the Northern District of Georgia, Newnan Division (the "Underlying Action").

66. The Underlying Action asserted four claims: excessive force in violation of the Fourth and Fourteenth Amendments against Deputy Teare (Count One); excessive force in violation of the Fourth and Fourteenth Amendments against Deputy Brooks (Count Two); deprivation of civil rights under color of law against Sheriff Wood, premised on his hiring, training, supervision, and discipline of the deputies (Count Three); and liability of Sheriff Wood for the misconduct of his deputies under O.C.G.A. § 15-16-24 (Count Four).

67. The Underlying Action remained pending from its filing on September 9, 2024 until it was resolved in or about August 2026 and dismissed with prejudice. Neither the resolution of the Underlying Action nor any release given in connection with it encompassed the claims asserted here. The conduct on which this action is based was not pleaded in the Underlying Action, was not within its subject matter, and did not arise from the incident in the Underlying Action.

68. The filing and prosecution of the Underlying Action was activity protected by the First Amendment to the United States Constitution, under both the Free Speech Clause and the Petition Clause. The Officer Defendants and Defendant Sheriff Wood knew of the Underlying Action. Christopher James Teare, then a deputy of the Coweta County Sheriff's Office, and Defendant Sheriff Leonard C. Wood were each named parties to it. The Officer Defendants are or were employees of the Coweta County Sheriff's Office, the agency whose hiring, training, and supervisory practices the Underlying Action placed at issue.

E. Retaliation Following the Filing of the Underlying Action

69. Since Plaintiff filed the Underlying Action, two or three Sheriff's Office vehicles have been stationed at the gas station at the Charlie B. Johnson Road intersection on an almost daily basis — a presence that Plaintiff, who travels past that location every workday, had seldom observed before. That pattern continues.

70. Defendant William Faulkner drives a distinctive vehicle — a Dodge Hellcat — that is the only one of its kind operated by the Coweta County Sheriff's Office and is immediately recognizable. During the pendency of the Underlying Action, Plaintiff repeatedly observed that vehicle stationed at the gas station at the time that his typical schedule causes Plaintiff to pass the gas station.

F. The Flock Surveillance: What the Audit Record Shows

71. After the Underlying Action resolved, Plaintiff first learned that he had been the subject of Flock ALPR surveillance through haveibeenflocked.com, a publicly accessible website that aggregates Flock Safety audit logs obtained from law enforcement agencies through public records requests and permits an individual to search for records associated with a license plate or vehicle identifier.

72. The Flock audit record associated with Plaintiff's vehicle, a 2024 Toyota Camry XSE registered under Mr. Murkerson's name, searched under identifier 78fee87f, reflects the following:

- a. Searching agency: Coweta County, Georgia Sheriff's Office.
- b. Surveillance period: May 4, 2025 through November 18, 2025.
- c. Surveillance duration: 197 days.
- d. Elapsed time between the first and last recorded search: 167 days.
- e. Total searches: five.
- f. Distinct days with recorded activity: two (at minimum).
- g. Operators: two, identified as "r.fau" and "w.fau."

h. Stated reasons: "info" and "37."

i. Networks searched: a minimum of 6,397, an average of 6,459, and a maximum of 6,521.

73. The operator identifiers "r.fau" and "w.fau" recorded for the two disclosed searches correspond to Defendant Randall Faulkner and Defendant William Faulkner, respectively, deputies or employees of the Coweta County Sheriff's Office.

74. The "networks searched" figures reflect that each query of Plaintiff's vehicle was propagated across more than six thousand participating law enforcement camera networks nationwide. Defendants did not merely ask where Plaintiff's vehicle had been in Coweta County. They asked where it had been anywhere in the United States that Flock cameras operate.

75. Upon information and belief, the 197-day surveillance duration reflects that Plaintiff's vehicle identifier was placed on a persistent alert, hot list, or standing watch entry within the Flock system, such that the network was configured to notify the operator each time Plaintiff's vehicle passed any participating camera, rather than merely returning the results of a one-time historical query; the searches reached back into stored location data extending materially beyond the default retention period applicable to standard Flock scans,

indicating that Defendants accessed long-term archived location data in order to reconstruct Plaintiff's movements over many months; and, because the details of three of the searches are withheld, the surveillance period to which Plaintiff was subjected was likely longer than the period shown in the incomplete audit record.

76.The surveillance period of May 4, 2025 through November 18, 2025 falls squarely within the pendency of the Underlying Action.

G. The Stated Reasons Were Pretextual

77.The Flock platform will not execute a search unless the operator enters a reason. The reasons recorded for the searches of Plaintiff's vehicle were "info" and "37."

78.Neither "info" nor "37" is a law enforcement purpose. Neither identifies an offense. Neither identifies an activity initiated by a law enforcement agency. Neither references a case number, an incident number, a call for service, or any investigation; and neither references that a case, or investigation, or law enforcement purpose exists.

79.A review of the search history of Defendant William Faulkner reflects that he entered the identical entry — "37" — for most searches he conducted on the platform, without regard to the subject or purpose of the search. William

Faulkner made thousands of searches, but only 4 of the searches had a case number entered with the query. An entry made reflexively and identically across unrelated searches conveys no information about purpose and is not a reason at all. It is a keystroke used to satisfy a software prompt.

80. At no time between May 4, 2025 and November 18, 2025 was Plaintiff the subject of any criminal investigation by the Coweta County Sheriff's Office or any other law enforcement agency. He was not suspected of any offense; no warrant was outstanding for him; no case was opened, no incident was recorded, and no call for service concerned him; he was not a witness to any crime under investigation; and all charges arising from the February 6, 2023 arrest had been dismissed nearly two years earlier. The Flock audit record of the searches of Plaintiff's vehicle contains no case number, no incident number, and no computer-aided-dispatch identifier because no such number existed to be entered. There was no law enforcement purpose for any search of Plaintiff's vehicle identifier, and Defendants knew it.

H. The Three Concealed Searches

81. Although the audit record reflects five total searches of Plaintiff's vehicle identifier, the details of only two have been disclosed. The operator name, date,

time, and stated reason for the remaining three were withheld from the records released to the public.

82. Those three searches were nonetheless made, each by an identifiable operator using a named credential at a recorded date and time, and each is memorialized in an audit log entry that Flock and the Coweta County Sheriff's Office maintain and can retrieve. Those operators are Defendants John Does 1, 2, and 3. For the reasons alleged in paragraph 22 above, the concealed searches are likely to reflect misconduct: the two disclosed searches were supported by nothing more than "info" and "37," and whatever justification was recorded for the three that were withheld has not been permitted to see daylight.

83. Flock removed core fields from the "Network Audit" reports through which an agency sees searches of its data by other agencies. Flock announced that "Network Audits will no longer include officer name, specific plates searched, vehicle fingerprint, and open text search reason," leaving little more than the searching agency, the date, and an offense category. H.C. van Pelt, Flock Decides Cops Can't Be Trusted with Cop Data, Footnote4a (Dec. 29, 2025, updated Jan. 7, 2026) (quoting Flock); DeFlockILM, The Flock Records That Caught Police Abuse Are Going Dark (Sept. 5, 2026) (describing Flock's Dec. 9, 2025 notice to customers, effective Jan. 31, 2026). Flock thus eliminated the record of who

searched and why — the information an audit exists to preserve. The complete record of who conducted each of the three concealed searches of Plaintiff's vehicle identifier, and the reason entered for each, is therefore in Flock's possession and control.

I. Physical Surveillance and Presence at Plaintiff's Home and Business

84. The database surveillance was accompanied by physical surveillance.

85. Joe Stevens Road forms the boundary between Coweta County and Heard County. Plaintiff's residence sits approximately one-eighth to one-quarter of a mile from that boundary, on a dead-end road, such that any vehicle stationed near the boundary must be passed by Plaintiff coming and going.

86. On multiple occasions, Coweta County Sheriff's Office deputies parked and remained at a storage facility located directly across from Plaintiff's road, within approximately one-eighth to one-quarter of a mile of his driveway. In the years Plaintiff lived at that property before the conduct described in this Section began, law enforcement vehicles were almost never present at that location.

87. On multiple occasions, Coweta County Sheriff's Office deputies parked and remained in the parking lot of Plaintiff's place of business during business hours. The surveillance, upon information and belief, informed the Sheriff's Office

of Mr. Murkerson's daily routine. And as the civil rights lawsuit proceeded, Mr. Murkerson also experienced two roadblocks: one at the intersection where the underlying incident occurred and one, days later, on the road to his home. These roadblocks appeared to Mr. Murkerson to be set up at a time calculated to intercept him on his commute. Upon information and belief, the Officer Defendants participated in, directed, or coordinated the physical surveillance described in this Section.

J. The August 2026 Audit, Resignations, and GBI Investigation

88. In or about August 2026, the Coweta County Sheriff's Office publicly disclosed that it had conducted an internal audit of its employees' use of the Flock Safety system; that several employee accounts had been identified for further review; that three employees met with their department heads and resigned before the audit process was completed; and that the agency had requested that the Georgia Bureau of Investigation conduct an independent investigation into those employees' conduct. The Sheriff's Office stated publicly: "We expect every employee with access to these systems to use them in a manner that is lawful, ethical and in accordance with agency policy," and "[p]rotecting the integrity of these systems and maintaining the trust of the community is a responsibility we take very seriously"; it further stated that it would provide additional training to all

authorized users on agency policy, appropriate system use, and employee accountability. 3 Former Sheriff's Office Employees Accused of Misusing Flock Safety System After Audit, WSB-TV (Aug. 4, 2026); Coweta County Sheriff's Office Employees Resign After Internal Audit of Flock Cameras, Officials Say, CBS News Atlanta (Aug. 5, 2026); Three Coweta sheriff's employees resign after audit flags flock safety access, Clay Neely, The Newnan Times-Herald (Aug. 4, 2026).

K. Procurement, Renewal, and the Failure to Terminate

89. The Flock Safety system deployed in Coweta County was acquired, funded, approved, and renewed pursuant to a written contract. Upon information and belief, that contract was negotiated, executed, and thereafter renewed by Defendant Sheriff Wood or, in the alternative, by Defendant Coweta County acting through its Board of Commissioners. Whichever of them held that authority held it as a final policymaker: the decisions to acquire, configure, and fund the system, to renew the contract, and not to terminate it were decisions of that policymaker, and the policy they established governed whether the Flock Safety platform would continue to operate in Coweta County at all.

90. When the contract was negotiated and when it was renewed, the Sheriff or, in the alternative, the County knew or should have known that the Flock Safety

system as designed lacked any requirement that an operator identify an investigation before executing a search, accepted free text of any kind in place of a case number, validated nothing, permitted nationwide propagation of a single query, and therefore permitted, and predictably produced, searches conducted for purposes other than law enforcement purposes — and that those design deficiencies had already resulted in actual deprivations of constitutional rights, in Georgia and nationally. That knowledge was available not as specialized literature but as the ordinary professional environment in which a Georgia sheriff's office operates, as set forth in Section B above. Neither the Sheriff nor the County needed to await the August 2026 internal audit to learn that the Flock Safety system could be, and was being, used to surveil private citizens without any law enforcement purpose.

91. By no later than the time of the August 2026 internal audit — which flagged the Flock Safety accounts of employees of the Coweta County Sheriff's Office, precipitated three resignations, and resulted in a referral to the Georgia Bureau of Investigation for criminal investigation — the Sheriff and, in the alternative, the County had actual knowledge that the system was being misused by persons with access to it in Coweta County.

92. Upon acquiring that knowledge, the Sheriff or, in the alternative, the County should have terminated the Flock Safety contract, or should have conditioned its continuation upon the implementation of controls sufficient to prevent searches conducted without a law enforcement purpose. Neither did so. Instead, upon information and belief, the contract was renewed or permitted to continue, and the system remained in operation, without any requirement that an operator identify an investigation, any validation of entered justifications, any routine audit, or any mechanism to interrupt an abusive pattern of searching.

93. Other public bodies confronted with the misuse of Flock's platform in violation of their own State's law chose to end, suspend, or condition their relationships with Flock. Termination, suspension, or conditioning of a Flock contract upon learning of misuse was thus a known, available, and actually exercised choice for a local policymaker. The Sheriff or, in the alternative, the County made none of those choices after the August 2026 audit.

94. In procuring, renewing, and continuing the contract with the knowledge alleged in paragraphs 90 and 91, the Sheriff or, in the alternative, the County acted with deliberate indifference to the known and obvious consequence that persons within the reach of the Flock Safety network — including Plaintiff and members of the Coweta Subclass — would be searched without any law enforcement purpose

and thereby deprived of rights secured by the Constitution. Those decisions were the moving force behind the deprivations alleged herein: had the contract been declined at procurement or renewal, or conditioned on the controls described above, the searches of Plaintiff and of Coweta Subclass members conducted without any recorded investigative justification could not have occurred as they did.

95. The August 2026 audit demonstrates that the misuse of the Flock platform by Coweta County Sheriff's Office personnel was detectable through an audit, and that the audit tools necessary to detect it were available to Defendant Sheriff Wood throughout the period of Plaintiff's surveillance. The Coweta County disclosures came amid a documented statewide pattern: from July through August 2026, the Georgia Bureau of Investigation announced arrests of current and former law enforcement and public-safety personnel across Georgia for misuse of license plate reader systems, including in Albany, Conyers, Polk County, Paulding County, Savannah, and Covington, and on or about November 19, 2025 — one day after the last search of Plaintiff's vehicle identifier reflected in the audit record — it announced the arrest of the Chief of Police of Braselton, Georgia on charges of Violation of Oath by a Public Officer, Stalking, Harassing Communications, and multiple counts of Misuse of Automated License Plate Recognition Systems, following a multi-month investigation. Ga. Bureau of Investigation, Press Releases

(July 6, 2026) (Albany); (July 23, 2026) (Conyers); (Aug. 7, 2026) (Polk County); (Aug. 12, 2026) (Paulding County); (Aug. 21, 2026) (Savannah); (Aug. 27, 2026) (Covington); (Nov. 19, 2025) (Braselton). Upon information and belief, Defendant Sheriff Wood was aware of that pattern.

96. Upon information and belief, prior to August 2026, the Coweta County Sheriff's Office maintained no adequate policy, practice, or protocol requiring: (a) that operators enter a meaningful, verifiable case number or investigative justification before searching the Flock platform; (b) routine or periodic audit of employee search activity; (c) supervisory review of searches lacking a corresponding call for service or case file; (d) any restriction on searching the identifiers of persons known to be adverse to the agency in pending litigation; or (e) discipline for searches conducted without a law enforcement purpose.

L. Flock Designed, Operated, and Controlled the Instrument of the Surveillance

97. Flock does not merely manufacture roadside cameras. It sells an integrated service in which Flock-manufactured cameras capture vehicle information, Flock-controlled software converts that information into searchable records, and a Flock-hosted cloud platform permits users to retrieve, aggregate, and share those records.

98. Flock designs and controls the functionality through which every search at issue in this case was executed, including: the search interface; the reason-entry field and what inputs it will accept; the retention period applicable to captured data; the network-sharing configuration that determines how many outside agency networks a single query reaches; the account provisioning and deprovisioning process; the audit logging architecture; and the tools, if any, that detect and surface anomalous or abusive search activity.

99. Flock retains continuing control over its platform after installation. Flock's own Terms and Conditions expressly reserve to Flock the authority to restrict or suspend customer access in specified circumstances. Flock Safety, Terms and Conditions §§ 2.2–2.3 (last updated Aug. 21, 2026). Upon information and belief, the terms in effect during the period of the searches of Plaintiff's vehicle contained materially similar provisions. Flock therefore performs ongoing access and control functions, and possesses the technical capability to terminate an abusive user's access, at all times.

M. Flock Knew That Operators Were Using Its Platform to Surveil Private Citizens

100. The misuse of Flock's platform by individual law enforcement operators for personal, retaliatory, and other non-law-enforcement purposes was

known to Flock, was extensively documented publicly, and was foreseeable to Flock, well before and throughout the period of Plaintiff's surveillance. Upon information and belief, by August 2026 national reporting had identified at least fifty law enforcement officers nationwide charged with or accused of misusing automated license plate reader systems; Flock's system was used in forty-six of those fifty cases, and in twenty-six of them investigators or prosecutors concluded that the officer used the technology to surveil a wife, girlfriend, former partner, a former partner's new partner, or a woman he sought to approach; and at least twenty Georgia officials had been arrested for misusing the Flock database by mid-2026, including those described in paragraph 95 above. Drew Harwell, Douglas MacMillan & Aaron Schaffer, *How Rogue Officers Turned a Nationwide Camera Network into a Tool for Stalking*, Wash. Post (Aug. 2, 2026); Autumn Billings, *Georgia Has Arrested At Least 20 Officials for Misusing the Flock Surveillance Database*, Reason (July 31, 2026).

101. By November 2025, public analysis of Flock audit logs had documented use of Flock's platform to search in connection with activity protected by the First Amendment. The Electronic Frontier Foundation reported that "more than 50 federal, state, and local agencies ran hundreds of searches through Flock's national network of surveillance data in connection with protest activity." Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to*

Surveil Protesters and Activists, Elec. Frontier Found. (Nov. 20, 2025). Audit logs published at haveibeenflocked.com — the same source through which Plaintiff learned of the searches of his own vehicle — reflect searches with stated reasons such as "Mosque," "protester," and "activist recording." First Amendment Report, Have I Been Flocked? (haveibeenflocked.com).

102. Flock's audit logs have also recorded search reasons that were improper on their face, and Flock's platform executed those searches anyway. The Electronic Frontier Foundation documented that more than 80 law enforcement agencies entered language perpetuating harmful stereotypes against Romani people as the stated reason for Flock searches, including single searches that reached as many as 1,233 agency networks and 14,467 cameras. Rindala Alajaji & Dave Maass, License Plate Surveillance Logs Reveal Racist Policing Against Romani People, Elec. Frontier Found. (Nov. 3, 2025). A platform that records such language as the justification for a search, and executes the search, does not validate justifications at all.

103. Stated reasons may also be false. In 2025, a Texas sheriff's office searched Flock's nationwide network for a woman who had self-managed an abortion. Flock and the sheriff's office publicly characterized the search as a search for a missing person; records later showed that deputies had opened a death

investigation and consulted prosecutors about charging her. Dave Maass & Rindala Alajaji, Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation., Elec. Frontier Found. (Oct. 7, 2025). Like the searches recorded as investigations into "a missing child" in Sedgwick, Kansas (§ 52), that episode shows that a free-text reason field records whatever an operator chooses to say and verifies nothing.

104. Flock has publicly described its historical safeguard — a retrospective audit process — as "reactive." In or about April 2026, Flock publicly introduced a product it markets as "Audit Assistance," which Flock describes as a trust and compliance tool that continuously monitors system activity and "surfaces search patterns that fall outside an agency's typical usage" so that administrators can see when activity warrants a closer look. Flock Safety, Press Release (Apr. 14, 2026) (announcing Audit Assistance). That product is dispositive of feasibility: a company does not design, build, and market a tool to detect operator misuse of its platform unless it knows such misuse occurs, knows it is detectable, and possesses the technical capability to detect it. Flock's own product line establishes that the safeguards Plaintiff alleges were owed to him were technologically feasible and a marketable reality.

N. Flock's Search-Justification Architecture Accepted Anything

105. Flock alone designed and controlled what a law enforcement operator was required to supply before the platform would execute a search of a private citizen's vehicle identifier. Throughout the period during which Plaintiff's vehicle was searched, and for years before, that requirement was a free-form text field: the operator typed something, and the platform ran the search. Flock did not require the entry to identify an offense, an investigation, a case, an incident, a call for service, or anything else, and did not validate the entry against any record of the searching agency.

106. In July 2025, Flock added an optional "case code" field but, upon information and belief, did not require it to be completed or validate it against any agency records; Flock did not introduce a standardized offense-category dropdown drawn from the National Incident-Based Reporting System until the week of December 10, 2025, after every search of Plaintiff's vehicle identifier reflected in the audit record; and did not announce until August 2026 that case codes would become mandatory, with compliance required of its law enforcement customers only by the end of 2026. Flock Safety, Flock Updates Privacy, Accountability, Security, and Transparency Safeguards (Aug. 13, 2026); Flock Safety, Offense Type Dropdown: A Simpler, More Accurate Audit (Dec. 10, 2025). An offense

category is not an investigation — selecting "theft from a motor vehicle" from a menu identifies a genre of crime, connects the search to no case, and can be verified against nothing, and upon information and belief operators simply selected the nearest available category whether or not it described the actual purpose of the search. Even now, Flock does not undertake to verify that an entered case number corresponds to a real investigation, or that the person whose identifier was searched has any connection to it.

107. The consequences of that design were documented and public. Upon information and belief, at agencies across the country officers defeated the search-reason requirement by entering generic text such as "investigation" — the only reason the Medford, Oregon Police Department gave for 111 searches of another city's Flock data — or, on twenty separate occasions by the same department, "hehehe," and in each instance the platform executed the search. Alan Torres, Medford PD Searched Eugene's Flock Data. The Reason? "hehehe", Eugene Register-Guard (reprinted at <https://www.aol.com/articles/medford-pd-searched-eugenes-flock-120347510.html>). The reasons recorded for the searches of Plaintiff's vehicle, "info" and "37," are of that character. Upon information and belief, "37" is not a Flock code, because at the time of the searches Flock maintained no code set at all; it is a string an operator typed into a field that would accept any string.

108. The misuse of Flock against Mr. Murkerson reflects the same pattern seen across Flock's customer base: agencies running searches with no case number and no stated reason beyond a generic placeholder. See ¶ 107.

109. Computer-aided-dispatch records are maintained by Georgia law enforcement agencies and their dispatch centers independently of Flock. They record, contemporaneously, every call for service and every officer-initiated activity and investigation, together with the officer assigned and the times of assignment and clearance. Those records are capable of establishing whether an officer who executed a search was engaged in any law enforcement activity at the moment of the search. Upon information and belief, the computer-aided-dispatch records of the Coweta County Sheriff's Office will show that the Officer Defendants were engaged in no call for service and no assigned or self-initiated activity concerning Plaintiff at the times the searches of his vehicle were executed.

O. Reasonable Alternative Designs Existed and Were Available to Flock

110. At all relevant times, reasonable alternative designs were available to Flock which would have prevented, interrupted, or timely surfaced the searches of Plaintiff's vehicle, and which were technologically feasible, commercially marketable, and capable of implementation without impairing the platform's

legitimate utility or unreasonably increasing its cost. These include, without limitation:

- a. Requiring entry of a verifiable case number, incident number, or computer-aided-dispatch identifier — validated against the agency's own records management system — before a search will execute, rather than accepting free text such as "info" or "37";
- b. Rejecting or flagging reason entries that are facially non-responsive, repeated verbatim across unrelated searches, or identical to an operator's every prior entry;
- c. Automated anomaly detection surfacing, in real time or near real time, repeated queries directed at a single plate that is not the subject of any hot list, warrant, or open case;
- d. Rate limiting and supervisory pre-approval for queries that reach beyond the searching agency's own camera network into statewide or nationwide networks;
- e. Automated expiration and mandatory supervisory re-authorization of any persistent alert, hot list entry, or standing watch on an individual plate, rather than permitting such an entry to persist for 197 days;

- f. Restricting the historical lookback window available to a single query to the platform's default retention period absent documented supervisory authorization;
- g. Automatic deprovisioning of operator accounts upon separation from the contracting agency;
- h. Contemporaneous notification to a designated agency compliance officer when the foregoing controls are triggered; and
- i. The misuse-detection functionality Flock itself designed, built, and marketed as "Audit Assistance," made a default and mandatory feature rather than an optional add-on.

111. Flock has never publicly asserted that the absence or limitation of such controls during the relevant period resulted from technological infeasibility, nor could it. The requirement that a query be tied to a documented factual basis and case number, be recorded in an audit trail, and be subject to periodic independent audit was codified in Minnesota law in 2015, two years before Flock was founded, and published as a model policy by the United States Department of Justice in February 2017; the ALPR systems reviewed by the California State Auditor prompted users to enter a case number and the purpose of each search by 2020 (§ 48); and validating an entry against a system of record, rate limiting,

flagging anomalous access patterns, expiring standing authorizations, deprovisioning departed users, and requiring multifactor authentication were all ordinary, well-established practices in the design of sensitive database systems long before 2025. Flock's adoption of them in 2026 did not make them feasible. It confirmed that they always had been.

112. Throughout the period of the searches of Plaintiff's vehicle, Flock did not require multifactor authentication for its existing law enforcement users. Flock enabled multifactor authentication by default only for new customers beginning in November 2024, and made it mandatory for everyone logging into its platform only in August 2026 (¶ 7). Letter from Sen. Ron Wyden & Rep. Raja Krishnamoorthi to the Fed. Trade Comm'n (Nov. 3, 2025) ("Flock does not require its law enforcement customers to use multi-factor authentication."); TechCrunch (Nov. 3, 2025) (quoting Flock's chief legal officer); Flock Safety, Flock Updates Privacy, Accountability, Security, and Transparency Safeguards (Aug. 13, 2026).

113. Had any of the foregoing designs been implemented, the searches of Plaintiff's vehicle — five searches of a single private citizen's plate, by at least two identified operators, supported by "info" and "37," reaching more than six thousand networks, sustained across 197 days, with no case number, no call for

service, and no open investigation — would have been blocked at the point of entry or surfaced for supervisory review long before the surveillance ran its course.

P. Flock Controlled How Long the Data Was Kept

114. Flock designs, sets, and administers the retention period applicable to captured license plate data on its platform; a customer agency selects among the retention options Flock makes available, and Flock implements and enforces the selection. Upon information and belief, Flock's default retention period was thirty days throughout the period relevant to this action, Flock reduced that default to seven days on or about August 13, 2026, and, in Flock's words, "[e]xisting customers will keep their current, democratically approved retention periods." Flock Safety, Flock Updates Privacy, Accountability, Security, and Transparency Safeguards (Aug. 13, 2026).

115. Flock's published License Plate Reader Policy states that "LPR data is hard deleted on a rolling 30-day basis by default," but that retention "may be increased or decreased on a case-by-case basis if a different schedule is required by a customer's law or policy." Flock Safety, License Plate Reader Policy (last updated Nov. 13, 2025) (superseded by version last updated June 30, 2026). Flock therefore implements each customer's retention period and possesses the records

establishing the retention period applied to the Coweta County Sheriff's Office's data during the period of the searches of Plaintiff's vehicle.

116. O.C.G.A. § 35-1-22(b) requires that "[a]ll such data collected shall be destroyed no later than 30 months after such data were originally collected unless such data are the subject matter of a toll violation or for a law enforcement purpose," and by operation of § 35-1-22(d)(2) a person who contracts with a law enforcement agency "to hold and maintain captured license plate data for such law enforcement agency" — which is precisely what Flock contracts to do — is subject to the policies of that agency and to the prohibition in § 35-1-22(d)(1). The exception for data that is "the subject matter of . . . a law enforcement purpose" has no application to Plaintiff or, upon information and belief, to the Class: where no law enforcement purpose existed for the access in the first instance, none existed to excuse continued retention.

117. To the extent the searches of Plaintiff's vehicle identifier returned location data spanning the months-long surveillance period, that data was necessarily retained beyond Flock's thirty-day default retention period. Upon information and belief, the Coweta County Sheriff's Office was configured for a materially longer retention period, or the data was preserved in an archival or evidentiary state outside the ordinary retention cycle, or both, and Flock retained,

or permitted the Coweta County Sheriff's Office to retain, captured license plate data concerning Plaintiff and Class members for periods exceeding those permitted by O.C.G.A. § 35-1-22(b), by the written policies the contracting agency was required to maintain under § 35-1-22(e), or by both.

118. The longer that data is retained, the more revealing it becomes. A record spanning days establishes that a vehicle passed a camera. A record spanning months permits the reconstruction of where its driver lives, works, worships, seeks medical care, and travels, and with whom. Flock's retention settings therefore determined the depth of the intrusion that each search could accomplish.

Q. Injury to Plaintiff

119. Before he learned of the Flock records, Plaintiff perceived that he was being followed and monitored but could not prove it; his wife told him he must be mistaken, and he came to doubt his own perception of reality, describing a belief that he was "going crazy." Upon learning that Defendants had in fact obtained real-time and historical data on his location for a period of 197 days, Plaintiff experienced, and continues to experience, fear, anxiety, humiliation, and apprehension for his safety and the safety of his family.

120. Plaintiff terminated a business relationship of approximately six years under which he serviced the vehicles of a neighboring municipal police

department, because he no longer believed it was safe to continue that work while he was being surveilled and monitored by the Coweta County Sheriff's Office in the manner described in this Complaint. He suffered a corresponding loss of income.

121. Plaintiff altered his routines, his routes, and his conduct in response to the surveillance. He has incurred and will incur costs and expenses in investigating, documenting, and attempting to obtain the records of Defendants' surveillance of him, and has expended money to retain counsel to investigate this matter and to seek an end to the surveillance, intimidation, and misuse of the Flock system directed at him, including an attorney retention fee and the filing fee for this lawsuit.

122. Defendants' conduct would deter a person of ordinary firmness from filing or prosecuting a civil rights action against law enforcement officers.

CLASS ACTION ALLEGATIONS

123. Plaintiff brings Counts X, XI, and XII individually and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4), on behalf of the Class defined below. Plaintiff brings Counts I, VII, and VIII individually and on behalf of the Officer Defendant Subclass, and Count IV individually for

damages and on behalf of the Officer Defendant Subclass for declaratory and injunctive relief only. Plaintiff brings Count XIII individually and on behalf of the Coweta Subclass. Counts II, III, V, VI, IX, XIV, and XV are asserted by Plaintiff individually only. Plaintiff further brings Counts X, XI, and XII on behalf of the Placeholder Injunctive Class defined below, for declaratory and injunctive relief only, pursuant to Federal Rule of Civil Procedure 23(b)(2).

A. Class Definitions

124. Plaintiff proposes the following Class:

All natural persons whose license plate number or other vehicle identifier was queried on the Flock Safety platform by a Georgia law enforcement agency or its employees at any time during the Class Period where: (1) neither Flock's audit record for the query nor the searching agency's records-management or computer-aided-dispatch records reflect any case, incident, call for service, or official investigation activity to which the query corresponds; or (2) a Georgia or federal law enforcement agency has determined that the query was made without a "law enforcement purpose" within the meaning of O.C.G.A. § 35-1-22(a)(4) and (b) (the "Class").

125. Plaintiff proposes the following Subclasses:

All members of the Class whose license plate number or other vehicle identifier was queried by the Coweta County Sheriff's Office or its employees (the "Coweta Subclass").

All members of the Class whose license plate number or other vehicle identifier was queried by one or more of the Officer Defendants (the "Officer Defendant Subclass").

126. Plaintiff further proposes the following class, for declaratory and injunctive relief only under Federal Rule of Civil Procedure 23(b)(2):

All natural persons whose license plate number or other vehicle identifier was queried on the Flock Safety platform by a Georgia law enforcement agency or its employees at any time during the Class Period where the reason recorded for the query in Flock's audit record (1) contained no case, incident, or computer-aided-dispatch number and (2) consisted solely of a generic, non-responsive, or placeholder entry — such as "investigation," "inv," "crime," "info," a single word, character, or punctuation mark, or a numeric or alphanumeric string that does not correspond to any case, incident, or call-for-service identifier in the searching agency's records (the "Placeholder Injunctive Class").

127. The Officer Defendant Subclass is defined by reference to the searches the Officer Defendants themselves conducted because the claims asserted in Counts I, IV, VII, and VIII are claims against those individual Defendants for their own conduct. The operator account that executed each search is recorded in the Flock Safety audit record, so membership in each Subclass is determinable from the same records that determine Class membership.

128. The "Class Period" is the period beginning four years before the filing of this Complaint and continuing through the date of judgment.

129. Membership in the Class is determined by objective criteria recorded in Flock's own business records and the business records of the Georgia law enforcement agencies that conducted the queries. It does not depend upon, and cannot be determined by, any adjudication of the merits of any Class member's claim, of the lawfulness of any search, or of any operator's state of mind. Membership in the Placeholder Injunctive Class is determinable from the reason and case-number fields of Flock's own audit records, which Flock generates for every search.

130. Excluded from the Class and Subclasses are: Flock and its officers, directors, employees, and agents; any entity in which Flock has a controlling interest; the Officer Defendants; the judge to whom this action is assigned and members of the judge's immediate family; any person who timely and validly requests exclusion from any certified damages class; and any claim for personal injury or wrongful death.

131. Plaintiff reserves the right to modify or amend the definitions of the Class and Subclasses, and to add or refine subclasses, before the Court determines whether certification is appropriate.

B. The Class Is Defined by Searches, Not by Image Capture

132. Membership in the Class is defined by the fact that a person's vehicle identifier was affirmatively searched on the Flock Safety platform. It is not defined by the passive capture of a vehicle's image by a Flock camera.

133. That distinction is deliberate, and it matters for three reasons.

- a. Ascertainability. A search is a discrete, timestamped, attributable event that Flock itself records. Every search generates an audit log entry identifying the operator account, the searching agency, the date and time, the identifier searched, and the reason entered. Class membership is therefore determinable by objective criteria from Flock's own business records and the searching agencies' records-management and computer-aided-dispatch records, without individualized inquiry into any class member's state of mind or circumstances.
- b. Concreteness of injury. A search is an affirmative human act of retrieval and examination. When an operator queries a plate, a person's accumulated location history is assembled and displayed to another human being. That is the traditional harm of intrusion upon seclusion — the prying itself — and not a bare procedural or statutory

violation. Every member of the Class has therefore suffered a concrete injury bearing a close relationship to a harm traditionally recognized at common law as providing a basis for suit. See Restatement (Second) of Torts § 652B; *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021).

- c. Cohesion. Every member of the Class was subjected to the same operative conduct: retrieval of that person's location history through the platform Flock designed, configured, hosted, and controlled, under the same access-control architecture and the same search-justification requirements, or absence of them.

C. Numerosity — Rule 23(a)(1)

134. The members of the Class are so numerous that joinder of all members is impracticable. Flock reports that its network processes more than 20 billion vehicle reads each month and that its platform is used by thousands of law enforcement agencies. Georgia agencies conduct search volumes of a corresponding magnitude: upon information and belief, based on published audit-log data, a single Coweta County Sheriff's Office operator conducted approximately 2,600 searches on the platform within a single year, and 76 Flock ALPR cameras are deployed in Coweta County alone (§ 57).

135. Upon information and belief, the number of Class members is in the tens of thousands at minimum. The precise number and the identity of each member are ascertainable from Flock's audit records and from the records of the Georgia law enforcement agencies that conducted the searches, all of which are within Defendants' or their customers' possession, custody, or control.

136. Class membership is ascertainable by objective criteria. Flock generates and maintains an audit record for every search executed on its platform. Upon information and belief, that record includes discrete fields for the searching agency, the operator account, the date and time of the query, the identifier searched, the stated reason, and the case number, and is exportable in comma-separated-value format from the administrative interface Flock provides to each customer agency. Class membership may therefore be determined by applying a filter to records Flock already produces on demand and comparing the results against the searching agencies' records-management and computer-aided-dispatch records.

D. Commonality and Predominance — Rules 23(a)(2) and 23(b)(3)

137. There are questions of law and fact common to the Class that are capable of classwide resolution and that predominate over any questions affecting only individual members. Those common questions include:

- a. Whether Flock's platform permitted Georgia law enforcement agencies to execute searches without any recorded case number, incident number, or computer-aided-dispatch identifier;
- b. Whether Flock owed a duty of reasonable care in the design, configuration, and operation of the access controls, search-justification requirements, retention settings, network-sharing settings, persistent-alert controls, anomaly detection, and audit functionality of its platform;
- c. Whether Flock's design was unreasonable when the risks inherent in it are weighed against its utility;
- d. Whether reasonable alternative designs were technologically feasible, commercially marketable, and available to Flock during the Class Period;
- e. Whether Flock knew or reasonably should have known that operators were using its platform to search private citizens for purposes other than law enforcement purposes, and when Flock acquired that knowledge;

- f. Whether Flock had reasonable grounds for apprehending that such misuse would occur;
- g. Whether Flock is a "person" within the meaning of O.C.G.A. § 35-1-22(a)(5) that contracts with Georgia law enforcement agencies to hold and maintain captured license plate data within the meaning of O.C.G.A. § 35-1-22(d)(2);
- h. Whether a Flock search to which no case, incident, call for service, or official investigation activity in the searching agency's records corresponds reflects "the investigation of an offense or activity initiated by a law enforcement agency" within the meaning of O.C.G.A. § 35-1-22(a)(4);
- i. Whether Flock designed and operated a platform that executed searches of Georgia residents' vehicle identifiers without capturing any verifiable identifier of an investigation;
- j. Whether Flock retained captured license plate data, or permitted it to be retained, beyond the period authorized by O.C.G.A. § 35-1-22(b) or by the policies of the contracting law enforcement agency;

- k. Whether O.C.G.A. § 35-1-22 imposes upon Flock a legal duty enforceable under O.C.G.A. § 51-1-6, and whether Class members fall within the class of persons that statute was enacted to protect;
- l. Whether Flock breached that duty;
- m. Whether the retrieval and display of Class members' stored location data to law enforcement operators, through a platform Flock designed and controlled, in searches to which no case, incident, call for service, or official investigation corresponds, constitutes an intrusion that would be highly offensive and objectionable to a reasonable person;
- n. Whether Flock's conduct showed that entire want of care which would raise the presumption of conscious indifference to consequences, so as to warrant punitive damages;
- o. The nature and scope of the injunctive and declaratory relief to which the Class is entitled.

138. As to the Officer Defendant Subclass and the Coweta Subclass, the common questions further include:

- a. Whether the Officer Defendants obtained personal information from Georgia motor vehicle records maintained by the Georgia Department

of Revenue, Motor Vehicle Division, and the Georgia Department of Driver Services for a purpose not permitted under 18 U.S.C. § 2721(b);

- b. Whether an Officer Defendant who queried a vehicle identifier to which no case, incident, call for service, or official investigation in the searching agency's records corresponds did so "without authority" within the meaning of O.C.G.A. § 16-9-92;
- c. Whether the retrieval of an individual's stored vehicle location history through a query of the Flock Safety platform constitutes a search within the meaning of the Fourth Amendment;
- d. Whether the Officer Defendants are entitled to qualified immunity on the claims asserted in Counts I and IV;
- e. Whether the retrieval of an individual's accumulated vehicle location history without any recorded investigative justification is an intrusion that would be highly offensive and objectionable to a reasonable person; and
- f. Whether the decision to acquire, renew, and continue the Flock Safety contract in Coweta County without controls sufficient to prevent

searches conducted without a law enforcement purpose was made with deliberate indifference to the known or obvious consequence that such searches would occur.

139. These questions turn on the Defendants' own conduct, design decisions, knowledge, and records. They do not vary from one Class member to another. Their resolution will drive the resolution of the litigation for every member of the Class in a single stroke.

140. Individualized questions concerning the amount of each Class member's damages do not defeat predominance. Liability may be established on common proof, and damages may be determined thereafter by claims administration, formula, subclassing, or individual proceedings as the Court directs.

E. Typicality — Rule 23(a)(3)

141. Plaintiff's claims against Flock are typical of the claims of the Class. Like every Class member, Plaintiff's vehicle identifier was searched on the Flock Safety platform by a Georgia law enforcement agency; that search was executed through the same architecture Flock designed and controlled; and the same alleged design and operational failures permitted it.

142. Plaintiff's claims against the Officer Defendants, Sheriff Wood, and the County arise from the same searches. They are asserted individually and, where so designated, on behalf of the Officer Defendant Subclass or the Coweta Subclass, and not on behalf of the Class. Those claims do not conflict with the interests of the Class. Plaintiff's interest in establishing that Flock designed and operated a platform that permitted searches without a law enforcement purpose is identical to the interest of every Class member.

F. Adequacy — Rule 23(a)(4)

143. Plaintiff will fairly and adequately protect the interests of the Class. He has no interest antagonistic to or in conflict with the Class. He has retained counsel experienced in complex and class litigation and in civil rights litigation, who are competent to prosecute this action and who will vigorously do so.

G. Rule 23(b)(2) — Injunctive and Declaratory Relief

144. Flock has acted and refused to act on grounds that apply generally to the Class. Its design decisions, access-control architecture, search-justification requirements, retention settings, network-sharing configuration, and audit practices are uniform across its Georgia customers and were applied to every Class member alike.

145. Final injunctive relief and corresponding declaratory relief are therefore appropriate respecting the Class as a whole, including relief requiring Flock to validate search justifications against agency records, to implement and enforce anomaly detection and supervisory review, to limit persistent alerts and retrospective lookback windows, to preserve and make available to searched individuals the audit records of searches of their own identifiers, and to purge data retained in violation of O.C.G.A. § 35-1-22. Certification of the Placeholder Injunctive Class under Rule 23(b)(2) is independently appropriate. Every member of that class was searched through a platform that accepted a placeholder in lieu of any investigative justification; membership turns on the uniform content of Flock's own audit records; and a single injunction requiring Flock to validate search justifications before executing searches for Georgia agencies would provide relief to each member of the class at once.

H. Superiority — Rule 23(b)(3)

146. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The core liability questions concern Flock's common design, knowledge, and conduct. Litigating them separately would duplicate that inquiry thousands of times over and would risk inconsistent adjudications establishing incompatible standards of conduct for Flock.

147. Most Class members do not know they were searched. A Flock search is invisible to its subject: the platform provides no notice to the person whose identifier is queried, and captured license plate data is exempt from public disclosure under O.C.G.A. § 35-1-22(f), an exemption agencies have invoked to withhold search records. Many Class members therefore have no practical means of discovering their claims, and few would have the resources or incentive to pursue individual actions. Class treatment is the only realistic mechanism by which their rights can be adjudicated.

148. Plaintiff is aware of *Schulte v. Flock Group, Inc.*, No. 1:26-cv-04843-MLB (N.D. Ga. filed Aug. 25, 2026), which seeks to represent a nationwide class of all individuals whose license plate data Flock has collected since January 1, 2024, on claims of invasion of privacy, negligence, negligent design, failure to warn, and intentional infliction of emotional distress. The operative *Schulte* complaint defines its class by the collection of license plate data, not by any search; asserts no claim under O.C.G.A. § 35-1-22 or O.C.G.A. § 51-1-6; and names no law enforcement officer, sheriff, or county as a defendant. This action, by contrast, is defined by affirmative searches conducted by Georgia agencies without any recorded investigative justification, and asserts claims that depend on the search itself. Plaintiff is also aware of litigation pending in the Northern District of California concerning Flock's sharing of California license plate data

with federal and out-of-state agencies under California's ALPR statute, *In re Flock Group Inc. Automated License Plate Reader Litigation*, No. 3:26-cv-02375-VC (N.D. Cal.), and *Javorsky v. Flock Group, Inc.*, No. 3:26-cv-02382-VC (N.D. Cal.); Plaintiff believes those actions are limited to California residents and California law. Plaintiff is aware of no other litigation concerning this controversy already commenced by members of the Class as defined herein. Concentrating the litigation in this forum is desirable because Flock is headquartered in this District, the searches at issue were conducted by Georgia agencies, and the governing law is the law of Georgia.

I. Rule 23(c)(4) — Issue Certification in the Alternative

149. In the alternative, and to the extent the Court determines that individualized issues concerning damages or causation preclude certification of a damages class under Rule 23(b)(3), Plaintiff seeks certification under Rule 23(c)(4) of the particular common issues identified above, including duty, breach, foreseeability, the availability of reasonable alternative designs, and Flock's knowledge, with damages to be determined in subsequent individual proceedings.

J. The Limitations Period Is Tolled

150. The applicable statutes of limitation are tolled as to the Class by the discovery rule and by Flock's concealment of the facts giving rise to these claims.

151. A search of a person's identifier on the Flock Safety platform is, by design, invisible to the person searched: neither Flock nor the searching agency notifies the subject, the subject has no means of detecting the search when it occurs and no ordinary channel through which to inquire, and captured license plate data is expressly exempt from public disclosure, O.C.G.A. § 35-1-22(f) — an exemption agencies have invoked to withhold search records, including, upon information and belief, three of the five searches of Plaintiff's own identifier. It was only through the recent publication of Flock audit logs obtained by third parties through public records requests, and their aggregation at haveibeenflocked.com, that any member of the Class acquired a practical means of learning that his or her identifier had been searched. Plaintiff himself learned of the searches of his vehicle in that manner, and not before. Flock has compounded that concealment. Upon information and belief, after its audit reports were produced in response to public records requests, Flock removed from its Network Audit reports the identity of the officer who conducted each search, the plate searched, and the reason entered,

rather than redacting the identities of the persons searched while preserving the record of who searched and why. See ¶ 83.

152. Accordingly, the claims of Plaintiff and the Class did not accrue, and the limitations period did not begin to run, until each Class member discovered or in the exercise of reasonable diligence should have discovered that his or her identifier had been searched.

COUNT I

VIOLATION OF THE DRIVER'S PRIVACY PROTECTION ACT

18 U.S.C. §§ 2721–2725

**(On Behalf of Plaintiff and the Officer Defendant Subclass, Against
Defendants William Faulkner, Randall Faulkner, and John Does 1–3,
individually)**

153. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

154. The Driver's Privacy Protection Act ("DPPA") provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724(a).

155. Querying a license plate to identify its registered owner, and thereby obtaining that person's name, address, and other identifying information from state motor vehicle records, is the knowing obtaining and use of personal information from a motor vehicle record within the meaning of 18 U.S.C. § 2724(a).

156. "Personal information" includes "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information," 18 U.S.C. § 2725(3), and "motor vehicle record" means "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles," 18 U.S.C. § 2725(1).

157. Each Defendant named in this Count is a natural person and therefore a "person" within the meaning of 18 U.S.C. § 2725(2). None is a State or an agency thereof.

158. Each Defendant named in this Count knowingly obtained, disclosed, or used personal information pertaining to Plaintiff from Georgia motor vehicle records maintained by the Georgia Department of Revenue, Motor Vehicle Division, and the Georgia Department of Driver Services, including by querying

Plaintiff's license plate to identify him as the registered owner, and by obtaining his name, address, driver identification number, and photograph.

159. These acts include, without limitation, the registration and driver record queries conducted, upon information and belief, in connection with each of the five Flock searches reflected in the audit record between May 4, 2025 and November 18, 2025, and such further queries as discovery may reveal.

160. None of these acts was for a purpose permitted under 18 U.S.C. § 2721(b), the exceptions to which are construed narrowly and turn on the predominant purpose of the obtaining or use. *Maracich v. Spears*, 570 U.S. 48 (2013). In particular, none was "use by any government agency, including any court or law enforcement agency, in carrying out its functions" within the meaning of § 2721(b)(1). Surveilling an adverse party in pending litigation against one's own agency is not an agency function. It is the abandonment of one.

161. Defendants acted knowingly. They knew they were obtaining Plaintiff's personal information, they knew the identity of the person whose information they were obtaining, and they knew they had no investigative reason to obtain it.

162. Plaintiff is entitled to recover, and hereby seeks: actual damages, but not less than liquidated damages in the amount of \$2,500 for each violation,

pursuant to 18 U.S.C. § 2724(b)(1); punitive damages upon proof of willful or reckless disregard of the law, pursuant to § 2724(b)(2); reasonable attorney's fees and other litigation costs reasonably incurred, pursuant to § 2724(b)(3); and such other preliminary and equitable relief as the Court determines to be appropriate, pursuant to § 2724(b)(4).

163. Plaintiff need not prove actual damages to recover liquidated damages under the DPPA. *Kehoe v. Fidelity Federal Bank & Trust*, 421 F.3d 1209, 1216–17 (11th Cir. 2005).

164. As to the Officer Defendant Subclass, this Count is limited to those Subclass members whose personal information was obtained from a Georgia motor vehicle record maintained by the Georgia Department of Revenue, Motor Vehicle Division, or the Georgia Department of Driver Services in connection with a query described in the Subclass definition. Each such violation carries liquidated damages of not less than \$2,500 without proof of actual damages, so Subclass damages are determinable by the number of violations rather than by individualized proof.

COUNT II

42 U.S.C. § 1983 — FIRST AMENDMENT RETALIATION

(Against Defendants William Faulkner, Randall Faulkner, and John Does 1–3, individually)

165. Plaintiff incorporates by reference paragraphs 1 through 122 above as if fully set forth herein.

166. Plaintiff's filing and prosecution of the Underlying Action was constitutionally protected activity under the Free Speech Clause and the Petition Clause of the First Amendment. Access to the courts to seek redress for the violation of constitutional rights lies at the core of the right to petition the government for a redress of grievances.

167. Defendants subjected Plaintiff to a campaign of surveillance in retaliation for that protected activity, including: placing his vehicle under persistent ALPR monitoring for 197 days; conducting nationwide searches of his location history reaching more than six thousand camera networks; obtaining his motor vehicle and driver records without a law enforcement purpose; and, upon information and belief, participating in or coordinating the stationing of Sheriff's Office vehicles at the site of his arrest on his route home, at his place of business, and within a quarter mile of his driveway.

168. This conduct would likely deter a person of ordinary firmness from the exercise of First Amendment rights. *Bennett v. Hendrix*, 423 F.3d 1247, 1250, 1254 (11th Cir. 2005). In *Bennett*, the Eleventh Circuit recognized that a retaliatory campaign including surveillance and the use of "government databases to obtain confidential information on the plaintiffs" states a First Amendment retaliation claim.

169. There is a causal connection between Plaintiff's protected activity and Defendants' retaliatory conduct. Among other things: the surveillance period falls entirely within the pendency of the Underlying Action; Defendant Sheriff Wood was himself a named defendant in the Underlying Action, and the Underlying Action placed at issue both the conduct of deputies of the Coweta County Sheriff's Office and the Sheriff's own hiring, training, supervision, and discipline of them; the physical surveillance concentrated at the precise location of the underlying incident; there was no law enforcement purpose for any of the conduct; and the stated reasons for the searches were pretextual.

170. Defendants acted under color of state law. They accessed the Flock platform and law enforcement databases using credentials, terminals, and authority conferred upon them solely by virtue of their employment as deputies. A private

citizen cannot query these systems. Defendants abused the position given to them by the State. *Griffin v. City of Opa-Locka*, 261 F.3d 1295, 1303 (11th Cir. 2001).

171. The unlawfulness of Defendants' conduct was clearly established at the time it occurred. The right to be free from retaliation for petitioning the courts, and the rule that a campaign of surveillance and database queries undertaken because a citizen sued law enforcement officers violates the First Amendment, were clearly established in this Circuit no later than *Bennett* in 2005. Although the constitutional right, not any statute, is the source of Defendants' liability, O.C.G.A. § 35-1-22(d)(1), which made the searches themselves criminal, and 18 U.S.C. § 2721, which prohibited the associated motor vehicle record queries, confirm that no reasonable officer could have believed that searching an adverse litigant's records was within his legitimate duties. See *Hope v. Pelzer*, 536 U.S. 730, 741 (2002). No reasonable officer could have believed that such conduct was lawful.

172. As a direct and proximate result, Plaintiff suffered the injuries described herein.

COUNT III

42 U.S.C. § 1983 — FOURTEENTH AMENDMENT

DEPRIVATION OF THE RIGHT TO INFORMATIONAL PRIVACY

**(Against Defendants William Faulkner, Randall Faulkner, and John Does 1–
3, individually)**

173. Plaintiff incorporates by reference paragraphs 1 through 122 above as if fully set forth herein.

174. The Due Process Clause of the Fourteenth Amendment protects an individual interest in avoiding disclosure of personal matters. *James v. City of Douglas*, 941 F.2d 1539, 1543 (11th Cir. 1991).

175. Georgia law compels its residents, as a condition of lawfully operating a motor vehicle, to furnish the State with their name, address, date of birth, photograph, and identifying numbers, and to display a registration plate that links their vehicle to that record. The State in turn restricts the use of that information to law enforcement purposes. O.C.G.A. § 35-1-22(b); 18 U.S.C. § 2721.

176. The constitutional interest in avoiding disclosure of personal matters was recognized in this Circuit no later than 1991, *James*, 941 F.2d at 1543, and an intrusion on that interest supported by no governmental interest whatsoever fails any balancing. Those statutory restrictions, while not the source of the right,

confirm that no reasonable officer could have believed that obtaining and examining Plaintiff's personal information and location history for a purpose other than a law enforcement purpose was lawful. The unlawfulness of Defendants' conduct was therefore clearly established at the time it occurred.

177. Defendants obtained and examined Plaintiff's personal information and the record of his movements for no legitimate governmental purpose whatsoever, but instead to monitor an adversary in litigation.

178. No governmental interest justified that intrusion, and Defendants can identify none.

179. As a direct and proximate result, Plaintiff suffered the injuries described herein.

COUNT IV

42 U.S.C. § 1983 — FOURTH AMENDMENT

UNREASONABLE SEARCH

(Against Defendants William Faulkner, Randall Faulkner, and John Does 1–3, individually, and against Defendant Sheriff Wood in his official capacity for prospective declaratory and injunctive relief only)

180. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

181. Plaintiff asserts this Count individually for damages, and on behalf of the Officer Defendant Subclass for declaratory and injunctive relief only. Plaintiff's claims against Defendant Coweta County, Georgia arising from the same searches are asserted in Count XIII.

182. Each query of Plaintiff's vehicle identifier on the Flock Safety platform was a search within the meaning of the Fourth Amendment. Plaintiff does not challenge the photographing of his vehicle by any Flock camera on a public road, or the collection and storage of such images. The search alleged in this Count is the government's affirmative retrieval, from a stored database, of a compiled record of a specific, identified person's past locations. That act of retrieval is what the Supreme Court held to be a search in *Carpenter v. United States*, 585 U.S. 296, 316 (2018) (holding that the government's acquisition of historical cell-site records was a search), and what the en banc Fourth Circuit held to be a search in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 346 (4th Cir. 2021) (en banc) (holding that police access to stored aerial surveillance data was a search). Where stored location data is protected, a search occurs regardless of how much of that data the government retrieves. *Chatrie v. United States*, 609 U.S. ___, 146 S. Ct. 2193, 2210, 2215 (2026) (holding that police conduct a search when they access a person's stored location history, and that "[i]t does not matter if the time period scrutinized was only two hours").

183. Defendants did not observe Plaintiff's vehicle at a single place and time. Upon information and belief, each query returned every capture of Plaintiff's vehicle held within the retention window available to the searching account across more than six thousand agency camera networks nationwide, including captures along the routes to and from Plaintiff's home and his place of business, which Plaintiff cannot reach without passing Flock cameras (§ 58), and, as alleged in paragraph 75, captures retained beyond the platform's default retention period.

184. Upon information and belief, the Coweta County Sheriff's Office's Flock subscription included one or more of the analytic features described in paragraph 32, so that the queries of Plaintiff's vehicle identifier returned not merely scattered sightings but an analysis of the patterns of his movements — which locations he visits, how often, and in the company of which other vehicles.

185. Upon information and belief, Defendants also placed Plaintiff's vehicle identifier on a persistent alert, hot list, or standing watch entry that notified them in real time whenever his vehicle passed a participating camera during the 197-day period (§ 75). Months-long, real-time monitoring of a single identified individual is not the passive, generalized collection of images of passing traffic that courts have upheld; it is the targeted, long-term tracking of a particular person that a majority of the Supreme Court has recognized impinges on reasonable

expectations of privacy. *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring). The records Defendants retrieved and the alerts they received revealed the privacies of Plaintiff's life — where he lives, where he works, when he departs and returns, and where he travels — in a manner categorically different from the observation of a vehicle on a public road.

186. Plaintiff's expectation that the stored record of his movements would not be retrieved absent an investigation is one that society is prepared to recognize as reasonable, and in Georgia society has said so by statute. The General Assembly has provided that captured license plate data "shall be stored immediately upon collection and not accessed except for a law enforcement purpose," O.C.G.A. § 35-1-22(b), has defined that purpose as "the investigation of an offense or activity initiated by a law enforcement agency," *id.* § 35-1-22(a)(4), and has made access for any other purpose a crime, *id.* § 35-1-22(d)(1). Plaintiff does not contend that a violation of Georgia law is, by itself, a violation of the Fourth Amendment. He alleges that these democratically enacted limits are evidence of the expectation of privacy Georgians reasonably hold in these records.

187. Each search was conducted without a warrant, without probable cause, without reasonable suspicion, and without consent. No exception to the

warrant requirement applied, and none could: Plaintiff was not the subject of any investigation, no exigency existed, and no case, incident, or call for service concerned him (§ 80). Because the searches served no law enforcement purpose at all, they were unreasonable under any standard, including any balancing of the governmental interest against the intrusion on Plaintiff's privacy.

188. The unlawfulness of those searches was clearly established. By 2018 it was settled that the government's warrantless acquisition of a stored record of an identified person's past movements is a search, *Carpenter*, 585 U.S. at 316, and it has long been settled that a search supported by no warrant, no exception, and no governmental interest whatsoever is unreasonable. Defendants can identify no decision of any court holding that an officer may retrieve a private citizen's stored location history for no law enforcement purpose. Where, as here, a search serves no legitimate governmental purpose of any kind, the Fourth Amendment's prohibition applies with obvious clarity, and no case directly on point is required. See *Hope v. Pelzer*, 536 U.S. 730, 741 (2002); *Vinyard v. Wilson*, 311 F.3d 1340, 1350–51 (11th Cir. 2002).

189. As a direct and proximate result, Plaintiff suffered the injuries described herein. Plaintiff further seeks prospective injunctive relief as set forth in the Prayer for Relief.

COUNT V

42 U.S.C. § 1983 — SUPERVISORY LIABILITY

(Against Defendant Sheriff Wood, individually)

190. Plaintiff incorporates by reference paragraphs 1 through 122 above as if fully set forth herein.

191. Defendant Sheriff Wood was at all relevant times the final policymaker for the Coweta County Sheriff's Office with respect to the acquisition, configuration, use, auditing, supervision, and discipline of employee access to the Flock Safety platform and to state and federal law enforcement databases.

192. Defendant Sheriff Wood maintained a custom or policy of permitting deputies unaudited and unsupervised access to the Flock Safety platform and to law enforcement databases; of accepting facially meaningless reason entries such as "info" and "37" in lieu of a genuine investigative justification; of failing to require any corresponding case number, incident number, or call for service; of failing to conduct any routine audit of search activity; and of failing to impose any restriction on the searching of persons known to be adverse to the agency in pending litigation.

193. That custom or policy resulted in deliberate indifference to the constitutional and statutory rights of persons whose data was accessible through those systems, including Plaintiff.

194. Defendant Sheriff Wood was on notice of the need to correct the deprivation. He knew or should have known: that O.C.G.A. § 35-1-22 restricted access to captured license plate data to law enforcement purposes and criminalized other use; that O.C.G.A. § 35-1-22(e) obligated his agency to maintain policies governing use and training; that Georgia Crime Information Center regulations, Ga. Comp. R. & Regs. r. 140-2-.04, limit use of disseminated information "to the purposes for which it was disseminated"; that 28 C.F.R. § 20.21 imposes parallel limits and mandates periodic audits; that his agency had been sued by Plaintiff and that his deputies had a motive to retaliate; and that misuse of license plate reader systems by law enforcement personnel, including Georgia personnel, was the subject of public reporting and criminal enforcement before and during the period of Plaintiff's surveillance, as alleged in Section B above. Each of those statutory and regulatory limits was clearly established law of which Sheriff Wood, as the chief law enforcement officer of Coweta County, was charged with knowledge.

195. Defendant Sheriff Wood's notice was personal and direct. He was himself a named defendant in the Underlying Action, sued in his individual

capacity precisely for his hiring, training, supervision, and discipline of Coweta County deputies, and he was personally defending against Plaintiff's claims throughout the 197-day period during which his deputies were searching Plaintiff on the Flock Safety platform. The August 2026 internal audit — which flagged employee accounts, precipitated three resignations, and resulted in a referral to the Georgia Bureau of Investigation — establishes that the means of detecting this misconduct were available to him at all relevant times and were not employed while Plaintiff was being surveilled.

196. There is a causal connection between Defendant Sheriff Wood's failures and the violations of Plaintiff's rights. Had any audit or supervisory review been conducted, a 197-day surveillance of a private citizen who was the plaintiff in a pending lawsuit against the agency, supported by nothing but the reason codes "info" and "37," would have been identified and stopped.

197. As a direct and proximate result, Plaintiff suffered the injuries described herein.

COUNT VI

**VIOLATION OF THE GEORGIA RACKETEER INFLUENCED AND
CORRUPT ORGANIZATIONS ACT**

O.C.G.A. § 16-14-4(b), (c); O.C.G.A. § 16-14-6(c)

**(Against Defendants William Faulkner, Randall Faulkner, and John Does 1–
3, individually)**

198. Plaintiff incorporates by reference paragraphs 1 through 122 above as if fully set forth herein.

199. The Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-90 et seq. (Article 6 of Chapter 9 of Title 16), is an enumerated predicate offense constituting "racketeering activity" under O.C.G.A. § 16-14-3(5)(A)(xix).

200. Each Defendant named in this Count committed computer invasion of privacy in violation of O.C.G.A. § 16-9-93(c), a felony chargeable by indictment under the laws of this State, by using a computer or computer network with the intention of examining personal data relating to Plaintiff with knowledge that such examination was without authority, as set forth more fully in Count VII below.

201. Defendants engaged in at least two such acts of racketeering activity. The audit record reflects five searches of Plaintiff's vehicle identifier by at least

two identified operators over a 167-day span, in addition to the motor vehicle record and criminal justice information queries alleged herein.

202. Those acts constitute a pattern of racketeering activity within the meaning of O.C.G.A. § 16-14-3(4)(A). They were undertaken in furtherance of one or more incidents, schemes, or transactions having the same or similar intents, results, accomplices, victims, and methods of commission: the same victim (Plaintiff), the same method (misuse of law enforcement database access), the same instrumentality (the Flock Safety platform and associated databases), the same participants, and the same intent (to monitor and intimidate an adverse litigant). They were not isolated incidents.

203. The pattern of racketeering activity was "motivated by or the effect of which is pecuniary gain or economic or physical threat or injury" within the meaning of O.C.G.A. § 16-14-2(b). Its purpose and effect were to threaten, intimidate, and physically confront Plaintiff — through persistent electronic tracking of his movements and armed deputies stationed within a quarter mile of his driveway and at his place of business — in order to deter him from prosecuting the Underlying Action, and its effect was also economic injury to Plaintiff, including the loss of a six-year business relationship and the costs of investigating

the surveillance. The Act "shall be liberally construed to effectuate the remedial purposes embodied in its operative provisions." O.C.G.A. § 16-14-2(b).

204. At all relevant times the Coweta County Sheriff's Office constituted an "enterprise" within the meaning of O.C.G.A. § 16-14-3(3), being a governmental entity and a group of individuals associated in fact within the meaning of that section. In the alternative, Defendants and such other persons as discovery may reveal constituted an association-in-fact enterprise. Upon information and belief, the members of that association shared a common purpose — to monitor, track, and intimidate Plaintiff, an adverse litigant in the Underlying Action against their own agency and its Sheriff — and pursued it through coordinated conduct, including repeated searches of Plaintiff's vehicle identifier under at least two operators' credentials and the stationing of Sheriff's Office personnel at the site of his arrest, near his home, and at his place of business. The association functioned as a continuing unit throughout the pendency of the Underlying Action, including at least from May through November 2025, a period sufficient to permit its members to pursue that purpose.

205. Defendants, being associated with and employed by that enterprise, conducted or participated in, directly or indirectly, the affairs of the enterprise

through a pattern of racketeering activity, in violation of O.C.G.A. § 16-14-4(b), and conspired to do so in violation of O.C.G.A. § 16-14-4(c).

206. Plaintiff was injured by reason of those violations. His injury flowed directly from the predicate acts, which were targeted at him by name and by license plate. Plaintiff is precisely the person at whom the predicate offenses were directed. The actual damages Plaintiff sustained by reason of those violations include: (a) the loss of income from the business relationship he terminated because of the surveillance; (b) the expenses he incurred in investigating, documenting, and attempting to obtain the records of the surveillance; (c) the costs of altering his routines, routes, and conduct in response to the surveillance; and (d) the fear, anxiety, humiliation, and apprehension for his safety and that of his family caused by the surveillance. O.C.G.A. § 16-14-6(c) affords a cause of action to "[a]ny person who is injured by reason of" a violation and is not limited to injury to business or property.

207. Pursuant to O.C.G.A. § 16-14-6(c), Plaintiff is entitled to recover three times the actual damages sustained, punitive damages, attorney's fees in the trial and appellate courts, and the costs of investigation and litigation reasonably incurred. Defendants acted with actual malice and with actual intent to cause

injury, as alleged in paragraph 220, and are not entitled to official immunity under Ga. Const. Art. I, Sec. II, Para. IX(d).

COUNT VII

VIOLATION OF THE GEORGIA COMPUTER SYSTEMS PROTECTION ACT

COMPUTER INVASION OF PRIVACY — O.C.G.A. § 16-9-93(c), (g)

(On Behalf of Plaintiff and the Officer Defendant Subclass, Against

Defendants William Faulkner, Randall Faulkner, and John Does 1–3,

individually)

208. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

209. O.C.G.A. § 16-9-93(c) provides that "[a]ny person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy."

210. Each Defendant named in this Count used a computer and a computer network — the Flock Safety platform, the Georgia Department of Revenue, Motor Vehicle Division, and Georgia Department of Driver Services databases, and/or the

Georgia Crime Information Center and National Crime Information Center systems.

211. Each did so with the intention of examining personal data relating to Plaintiff, including his license plate, the historical and real-time locations of his vehicle, his name, his address, his driver identification number, and his driver record.

212. Each did so with knowledge that the examination was without authority. Under O.C.G.A. § 16-9-92, "without authority" "includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." The owners of these systems granted Defendants permission to use them for law enforcement purposes only. That limitation is expressly imposed by O.C.G.A. § 35-1-22(b), by Ga. Comp. R. & Regs. r. 140-2-.04, by 28 C.F.R. § 20.21(c), and by the user agreements and agency policies that Defendants executed and were trained upon as a condition of receiving access. Defendants used these systems in a manner exceeding that permission.

213. Plaintiff's person and property were injured by reason of these violations. He sustained damages including lost income from the terminated

business relationship, expenses incurred in investigating and documenting the surveillance, and injury to his person.

214. Pursuant to O.C.G.A. § 16-9-93(g)(1), Plaintiff and the members of the Officer Defendant Subclass are entitled to recover the damages sustained and the costs of suit. Defendants acted with actual malice and with actual intent to cause injury, as alleged in paragraph 220, and are not entitled to official immunity under Ga. Const. Art. I, Sec. II, Para. IX(d).

COUNT VIII

INVASION OF PRIVACY — INTRUSION UPON SECLUSION

**(On Behalf of Plaintiff and the Officer Defendant Subclass, Against
Defendants William Faulkner, Randall Faulkner, and John Does 1–3,
individually)**

215. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

216. Georgia recognizes the tort of invasion of privacy by intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. No physical intrusion is required.

217. Sustained surveillance of an individual, including surveillance conducted in public places, is actionable where it is calculated to frighten, torment, or hound the plaintiff.

218. Defendants intruded upon Plaintiff's seclusion and private affairs by monitoring the whole of his movements for 197 days, by reconstructing months of his location history, by obtaining his personal identifying information without authority, and, upon information and belief, by participating in or coordinating the stationing of deputies near his home, at his business, and along his daily routes.

219. That intrusion would be highly offensive and objectionable to a reasonable person. It was undertaken by armed officers of the State against a citizen who had done nothing but sue them.

220. Defendants acted with actual malice and with actual intent to cause injury. Their conduct was not the negligent performance of a discretionary function; it was the deliberate commission of acts they knew to be wrongful and criminal, undertaken for the purpose of monitoring and intimidating an adverse litigant. Defendants are therefore not entitled to official immunity under Ga. Const. Art. I, Sec. II, Para. IX(d).

221. As a direct and proximate result, Plaintiff suffered the injuries described herein. To the extent the injury inflicted by that intrusion is to the peace,

happiness, and feelings of Plaintiff, Plaintiff is entitled to general damages in an amount determined by the enlightened consciences of impartial jurors, without proof of pecuniary loss. O.C.G.A. § 51-12-6.

COUNT IX

BREACH OF LEGAL DUTY — O.C.G.A. § 51-1-6

(Pleaded in the Alternative, Against Defendants William Faulkner, Randall Faulkner, and John Does 1–3, individually)

222. Plaintiff incorporates by reference paragraphs 1 through 122 above as if fully set forth herein. This Count is pleaded in the alternative to Counts VI through VIII.

223. O.C.G.A. § 51-1-6 provides that "[w]hen the law requires a person to perform an act for the benefit of another or to refrain from doing an act which may injure another, although no cause of action is given in express terms, the injured party may recover for the breach of such legal duty if he suffers damage thereby."

224. O.C.G.A. § 9-2-8(b) expressly preserves this theory of recovery notwithstanding the absence of an express private right of action.

225. O.C.G.A. § 35-1-22(b) and (d)(1) impose a legal duty to refrain from accessing or using captured license plate data for any purpose other than a law enforcement purpose. O.C.G.A. § 35-3-38 imposes a legal duty to refrain from

knowingly requesting or obtaining criminal history record information under false pretenses.

226. Plaintiff falls within the class of persons those provisions were enacted to protect — individuals whose license plate data is captured and whose criminal justice information is maintained — and the harm he suffered is precisely the harm those provisions were intended to guard against.

227. Defendants breached those duties, and Plaintiff suffered damage thereby. Defendants are not entitled to official immunity on this Count: the prohibition in O.C.G.A. § 35-1-22(b) and (d)(1) on accessing captured license plate data except for a law enforcement purpose leaves no room for the exercise of discretion and is therefore ministerial, and, in the alternative, Defendants acted with actual malice and with actual intent to cause injury, as alleged in paragraph 220.

COUNT X

NEGLIGENCE — NEGLIGENT DESIGN AND OPERATION

(On Behalf of Plaintiff and the Class, Against Defendant Flock Group, Inc.)

228. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

229. Under Georgia law, a manufacturer or designer has a duty to exercise reasonable care in selecting from among alternative designs so as to reduce reasonably foreseeable risks of harm posed by what it designs and places into use. Georgia law "does not recognize a blanket exception to a manufacturer's design duty in all cases of intentional or tortious third-party product misuse," and a design duty may run to an injured person "regardless of who — the injured person or a third party — was using the defectively designed product." *Maynard v. Snapchat, Inc.*, 313 Ga. 533, 870 S.E.2d 739 (2022).

230. Flock designed, built, configured, hosted, and operated an integrated surveillance system whose foreseeable and intended output is a searchable record of the movements of every person who drives past its cameras — including persons, like Plaintiff, who are suspected of nothing.

231. The risk that individual operators would use that system to surveil private citizens for personal, retaliatory, or other non-law-enforcement purposes was not merely foreseeable to Flock. It was known to Flock, documented publicly and repeatedly, the subject of criminal prosecutions in Flock's home state, and sufficiently concrete that Flock designed and marketed a commercial product for the express purpose of detecting it.

232. Flock therefore had reasonable grounds for apprehending that the very conduct alleged in this Complaint would be committed, and the intervening acts of the Officer Defendants do not insulate Flock from liability.

233. Flock owed Plaintiff a duty to exercise reasonable care in the design, configuration, and operation of the access controls, search-justification requirements, retention settings, network-sharing settings, persistent-alert controls, anomaly detection, audit functionality, and intervention mechanisms of the system it built and continues to control.

234. Flock breached that duty. Weighing the risks inherent in its design against the utility derived from it, and considering the availability, feasibility, marketability, and cost of the alternative designs identified above, Flock's design was unreasonable.

235. Flock further breached that duty by failing to exercise reasonable care in the ongoing operation of the platform, including by failing to detect, surface, interrupt, or terminate a 197-day surveillance of a private citizen supported by no case number, no call for service, and no investigative justification, notwithstanding that Flock possessed the audit data, the technical capability, and the contractual authority to do so.

236. As a direct and proximate result of Flock's negligence, Plaintiff suffered the injuries described herein.

COUNT XI

BREACH OF LEGAL DUTY — O.C.G.A. § 51-1-6

(On Behalf of Plaintiff and the Class, Against Defendant Flock Group, Inc.)

237. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

238. O.C.G.A. § 51-1-6, quoted in Count IX above, permits an injured party to recover for the breach of a legal duty imposed for his benefit "although no cause of action is given in express terms," and O.C.G.A. § 9-2-8(b) expressly preserves that theory of recovery. Plaintiff does not assert an implied private right of action under O.C.G.A. § 35-1-22; he asserts a claim under O.C.G.A. § 51-1-6 predicated on the legal duty that § 35-1-22 imposes.

239. O.C.G.A. § 35-1-22(a)(5) defines "person" to include a corporation, and § 35-1-22(d)(2) provides that a law enforcement agency may contract "with a person to hold and maintain captured license plate data for such law enforcement agency; provided, however, that such person shall be subject to the policies of the law enforcement agency and paragraph (1) of this subsection." Flock is such a person. It contracts with the Coweta County Sheriff's Office to hold and maintain

that agency's captured license plate data, and by operation of § 35-1-22(d)(2) it is subject to the policies of that agency and to the prohibition in § 35-1-22(d)(1) against requesting, using, obtaining, or attempting to obtain captured license plate data for any purpose other than a law enforcement purpose.

240. The General Assembly thus imposed upon Flock, by function and by express reference, the same statutory constraint it imposed upon the deputies: captured license plate data may be accessed only for a law enforcement purpose. O.C.G.A. § 35-1-22(b).

241. Plaintiff falls squarely within the class of persons that O.C.G.A. § 35-1-22 was enacted to protect — individuals whose license plate data is captured, stored, and made searchable — and the harm he suffered is precisely the harm the statute was intended to guard against, namely the use of that data for a purpose other than a law enforcement purpose.

242. Flock breached that duty by holding and maintaining Plaintiff's captured license plate data and by making it available for, and permitting it to be accessed for, purposes other than a law enforcement purpose; by failing to configure and operate the data it held in a manner consistent with the statutory limitation and with the policies of the contracting agency; and by failing to restrict

or suspend access when the data it held was being used for purposes the statute forbids.

243. Flock further breached that duty by retaining, and by permitting the contracting agency to retain, captured license plate data concerning Plaintiff and Class members beyond the period permitted by O.C.G.A. § 35-1-22(b) or beyond the period permitted by the policies of the contracting law enforcement agency, to which Flock is subject under O.C.G.A. § 35-1-22(d)(2). The statutory duty to destroy captured license plate data is a duty to "perform an act for the benefit of another" within the meaning of O.C.G.A. § 51-1-6.

244. Plaintiff suffered damage thereby.

COUNT XII

INVASION OF PRIVACY — INTRUSION UPON SECLUSION

(On Behalf of Plaintiff and the Class, Against Defendant Flock Group, Inc.)

245. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

246. Plaintiff has a reasonable expectation that the stored record of his movements, routines, and associations will not be retrieved and examined by others without a lawful purpose.

247. Flock intentionally designed, built, and operates a system through which the stored location records of private individuals who are suspected of no wrongdoing are retrieved and displayed to human operators on demand, and Flock alone determines what justification, if any, an operator must supply before that retrieval occurs.

248. Through the platform it designed, hosted, and controlled, Flock retrieved and displayed Plaintiff's stored vehicle location records to law enforcement operators in each of the searches described in this Complaint — without Plaintiff's knowledge or consent, without any recorded investigative justification, and with knowledge that its platform was being used by operators to conduct exactly such searches.

249. The retrieval and display of Plaintiff's stored location records to law enforcement operators, in searches supported by no recorded investigative justification, constitute a substantial intrusion into Plaintiff's seclusion and private concerns that would be highly offensive and objectionable to a reasonable person. Plaintiff does not contend that the capture of his vehicle's image on a public road, standing alone, is an actionable intrusion.

250. As a direct and proximate result, Plaintiff suffered the injuries described herein. To the extent the injury inflicted by that intrusion is to the peace,

happiness, and feelings of Plaintiff and Class members, they are entitled to general damages in an amount determined by the enlightened consciences of impartial jurors, without proof of pecuniary loss.

COUNT XIII

42 U.S.C. § 1983 — ENTITY AND POLICYMAKER LIABILITY

PROCUREMENT, RENEWAL, AND FAILURE TO TERMINATE

(On Behalf of Plaintiff and the Coweta Subclass, Against Defendant Sheriff Wood in his individual and official capacities or, in the alternative, Against Defendant Coweta County, Georgia)

251. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

252. This Count is pleaded in the alternative. If the authority to negotiate, execute, renew, and terminate the Flock Safety contract resided with the Sheriff, this Count is asserted against the Sheriff. If that authority resided with the County acting through its Board of Commissioners, this Count is asserted against the County.

253. Plaintiff seeks damages on this Count against Sheriff Wood in his individual capacity and, in the alternative, against the County. To the extent Sheriff Wood is deemed to have acted as an arm of the State of Georgia in exercising

authority over the Flock Safety contract, Plaintiff seeks against him in his official capacity only prospective declaratory and injunctive relief.

254. A local government is liable under 42 U.S.C. § 1983 where the execution of its own policy or decision inflicts the injury, *Monell v. Department of Social Services*, 436 U.S. 658 (1978), and, where the government's own act is not itself unconstitutional, where the policymaker acted with deliberate indifference to the known or obvious consequence that a constitutional violation would follow and the decision was the moving force behind the injury. The decision to acquire the Flock Safety system, the decision to renew the contract, and the decision not to terminate it upon actual knowledge of misuse were decisions of a final policymaker, made on behalf of the governmental entity that held contracting authority, and were official policy.

255. Those decisions were made with deliberate indifference to the known and obvious consequence that the system would be used to search persons for purposes other than law enforcement purposes, and that those persons would thereby be deprived of rights secured by the Fourth and Fourteenth Amendments to the United States Constitution, as alleged in Counts III and IV.

256. The deliberate indifference existed at procurement and at each renewal, by reason of the notice alleged in paragraph 90, and it is compounded as

to continuation after August 2026. By August 2026 the Sheriff and, in the alternative, the County possessed actual knowledge that employees with access to the Flock Safety system in Coweta County had misused it, that three had resigned rather than complete an audit, and that the Georgia Bureau of Investigation had been asked to investigate them criminally. Continuing the contract on unchanged terms with that knowledge was a conscious choice to accept the risk that the misuse would continue.

257. That policy was the moving force behind the deprivations suffered by Plaintiff and members of the Coweta Subclass. The searches at issue were possible only because the system was procured, funded, renewed, and permitted to operate without any requirement that an operator identify an investigation.

258. As a direct and proximate result, Plaintiff and members of the Coweta Subclass suffered the injuries described herein, and are entitled to compensatory damages, declaratory relief, and injunctive relief requiring that the Flock Safety system not be operated in Coweta County absent controls sufficient to prevent searches conducted without a law enforcement purpose.

259. Plaintiff does not seek punitive damages against Defendant Coweta County.

COUNT XIV

PUNITIVE DAMAGES — O.C.G.A. § 51-12-5.1

(Against All Individual Defendants and Defendant Flock Group, Inc.)

260. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

261. The actions of the Officer Defendants and of Sheriff Wood showed willful misconduct, malice, wantonness, oppression, and that entire want of care which would raise the presumption of conscious indifference to consequences, warranting an award of punitive damages under O.C.G.A. § 51-12-5.1(b).

262. The Officer Defendants acted with the specific intent to cause harm to Plaintiff. Accordingly, pursuant to O.C.G.A. § 51-12-5.1(f), there is no limitation on the amount that may be awarded as punitive damages against them.

263. Flock's conduct likewise showed that entire want of care which would raise the presumption of conscious indifference to consequences. Flock continued to operate, expand, and profit from a surveillance platform it knew was being used by law enforcement operators to surveil private citizens for personal and retaliatory purposes; it left the safeguards it knew to be feasible optional or unbuilt; and it did so with knowledge of a documented and escalating pattern of criminal misuse in its own home state.

264. Plaintiff further seeks punitive damages under 18 U.S.C. § 2724(b)(2), under O.C.G.A. § 16-14-6(c), and, against the individual Defendants, on his claims under 42 U.S.C. § 1983.

COUNT XV

ATTORNEY'S FEES AND EXPENSES OF LITIGATION

(Against All Defendants)

265. Plaintiff incorporates by reference paragraphs 1 through 152 above as if fully set forth herein.

266. Plaintiff is entitled to recover reasonable attorney's fees and costs pursuant to 42 U.S.C. § 1988(b), 18 U.S.C. § 2724(b)(3), and O.C.G.A. § 16-14-6(c).

267. Plaintiff further specially pleads and prays for the expenses of litigation pursuant to O.C.G.A. § 13-6-11, in that Defendants have acted in bad faith, have been stubbornly litigious, and have caused Plaintiff unnecessary trouble and expense.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that this Court:

- (a) Issue process and require Defendants to answer;

- (b) Certify the Class, the Subclasses, and the Placeholder Injunctive Class under Federal Rule of Civil Procedure 23, appoint Plaintiff as Class Representative, and appoint his counsel as Class Counsel;
- (c) Enter judgment in favor of Plaintiff, the Class, and the Subclasses and against Defendants on each Count as pleaded, including judgment against Defendant Sheriff Wood or, in the alternative, against Defendant Coweta County, Georgia, on Count XIII;
- (d) Award Plaintiff and the members of the Officer Defendant Subclass liquidated damages of not less than \$2,500 for each violation of the Driver's Privacy Protection Act pursuant to 18 U.S.C. § 2724(b)(1), or actual damages, whichever is greater;
- (e) Award Plaintiff, the Class, and the Subclasses compensatory damages in an amount to be proven at trial, including general damages pursuant to O.C.G.A. § 51-12-6 on Counts VIII and XII;
- (f) Award Plaintiff three times his actual damages pursuant to O.C.G.A. § 16-14-6(c);

(g) Award Plaintiff punitive damages in an amount to be determined by the enlightened conscience of an impartial jury, without limitation as to the Officer Defendants pursuant to O.C.G.A. § 51-12-5.1(f);

(h) Award Plaintiff, and the members of the Coweta Subclass on Count XIII, nominal damages on the claims under 42 U.S.C. § 1983; and award Plaintiff, the Class, and the Subclasses nominal damages pursuant to O.C.G.A. § 51-12-4 to the extent any injury is not capable of estimation in money;

(i) Grant declaratory relief adjudging that Defendants' conduct violated the Driver's Privacy Protection Act, the First, Fourth, and Fourteenth Amendments, and the laws of the State of Georgia;

(j) Grant prospective injunctive relief against Defendant Sheriff Wood in his official capacity requiring that he: (i) purge all records of Plaintiff obtained without a law enforcement purpose; (ii) remove Plaintiff's license plate, vehicle identifier, and personal identifiers from any active alert, hot list, or standing watch entry within the Flock Safety platform or any comparable system; (iii) preserve and produce the complete, unredacted audit record of every search of Plaintiff's identifiers; (iv) implement and enforce a policy requiring a verifiable case number or incident number for

every ALPR and database query; (v) implement routine supervisory audit of query activity; (vi) refrain from further searches of Plaintiff's identifiers absent a genuine law enforcement purpose documented contemporaneously; and (vii) as to the Coweta Subclass, refrain from operating the Flock Safety system in Coweta County absent controls sufficient to prevent searches conducted without a law enforcement purpose; and, in the alternative as to item (vii), grant the same relief against Defendant Coweta County, Georgia;

(k) Grant equitable relief against Defendant Flock Group, Inc. requiring that it preserve and produce the complete, unredacted audit record of every search of Plaintiff's identifiers across its platform, including the operator-identity, stated-reason, and case-number fields as originally recorded and without regard to any subsequent change Flock has made to its audit-reporting format, identify every operator who conducted such a search and every agency with which the results were shared, purge Plaintiff's captured license plate data obtained or retained in violation of O.C.G.A. § 35-1-22, remove Plaintiff's identifiers from any persistent alert, hot list, or standing watch entry, and, as to the Class and the Placeholder Injunctive Class, validate search justifications against agency records, implement and enforce anomaly detection and supervisory review, limit persistent alerts and

retrospective lookback windows, and purge data retained in violation of O.C.G.A. § 35-1-22;

(l) Award Plaintiff his reasonable attorney's fees and costs pursuant to 42 U.S.C. § 1988(b), 18 U.S.C. § 2724(b)(3), O.C.G.A. § 16-14-6(c), and O.C.G.A. § 13-6-11;

(m) Award pre-judgment and post-judgment interest as allowed by law; and

(n) 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 8th day of October 2026.

HALL & LAMPROS, LLP

/s/ Christopher B. Hall

Christopher B. Hall

Georgia Bar No. 318380

Andrew L. Lampros

Georgia Bar No. 432328

300 Galleria Parkway, Suite 300

Atlanta, Georgia 30339

Telephone: (404) 876-8100

chall@hallandlampros.com

alampros@hallandlampros.com

Attorneys for Plaintiff Tyler Murkerson