Mass Surveillance Constitutional Defense

A Grassroots Legal and Tactical Framework

Executive Summary

Mass surveillance through Automated License Plate Readers (ALPRs), facial recognition, and public-private data networks operates in a constitutional gray zone—technically legal under existing judicial frameworks, yet increasingly vulnerable to Fourth Amendment challenges post-*Carpenter v. United States* (2018)[1]. This document outlines both grassroots activism strategies and a sophisticated Supreme Court litigation strategy that remain legally compliant while systematically dismantling the surveillance infrastructure.

Key Strategic Finding: The government's surveillance programs are NOT constitutionally bulletproof. The vulnerabilities center on: (1) warrantless mass collection, (2) third-party doctrine erosion, (3) chilling effects on First Amendment activity, and (4) inadequate statutory safeguards.

PART I: GRASSROOTS LEGAL COUNTERMEASURES

Non-Violent, Lawful Resistance Methods

1. Public Records Disclosure & Transparency Warfare

Legal Basis: FOIA (federal), state Public Records Acts, and state FOIA equivalents

Strategy:

- File comprehensive FOIA/public records requests for:
  - All Flock Safety camera locations and installation dates
  - Contracts between municipalities and surveillance vendors (Flock, Amazon Rekognition, etc.)
  - Usage logs, search queries, and retention policies
  - Federal agency access agreements
  - Cost-sharing arrangements and federal funding sources
  - Agreements regarding data sharing with federal agencies

Execution:

- Use **MuckRock.com** and **RecordTrac** for coordinated FOIA campaigns
- Request data in machine-readable format (CSV, JSON, database exports)
- Appeal denials through administrative channels
- Hire FOIA attorneys if municipalities wrongfully withhold records (they often lose)

Example Success: Washington state court (November 2025) ruled that Flock ALPR data IS public record, overturning municipalities' secrecy claims[2]

Impact: Transparency creates political pressure and identifies constitutional vulnerabilities

---

2. Legislative Advocacy & Democratic Participation

Non-litigation path:

Federal Level:

- Support bills requiring warrant authorization for ALPR/facial recognition searches
- Advocate for federal legislation explicitly overruling third-party doctrine for digital data
- Push for §2.022-style statutory solutions (creating private right of action for surveillance abuses)

State/Local Level:

- Campaign for local ban ordinances (similar to San Francisco's surveillance tech ban)
- Advocate for surveillance impact assessment requirements before deployment
- Support mandatory warrant requirements for ALPR/facial recognition searches
- Push for data minimization, retention limits, and audit logs

Participation:

- City council testimony during surveillance tech procurement votes
- Coalition building with civil rights organizations (ACLU, EFF, CCR)
- Direct outreach to elected officials with constituent letters

Recent Examples:

- Eugene, OR: ACLU lawsuit forced disclosure of Flock camera locations (2025)[3]
- Multiple states enacted warrant requirements for cellular tracking post-*Carpenter*

---

3. Corporate Accountability Campaigns

Target: Flock Safety's investor base and vendor relationships

Tactics:

- Public pressure on institutional investors (CalPERS, pension funds)
- Demand shareholder resolutions on privacy impact assessment
- Support customer defections (cities leaving Flock)
- Document and publicize surveillance harms through

data analysis

Example: Norfolk, Virginia litigation (2025) challenged 170+ Flock cameras; legal pressure mounted over tracking of protesters and activists[4]

---

4. Community Documentation & Data Analysis

Crowdsourced Intelligence:

- Coordinate public records requests across multiple jurisdictions
- Build databases of:
  - Surveillance camera locations (open-source mapping)
  - Vendor contracts and pricing
  - Federal agency access patterns
  - Documented misuse instances (false arrests, chilling effects on protest)

Tools & Platforms:

- Mapbox/Leaflet for surveillance mapping
- Document tracking via DocumentCloud
- Collaborative database building (Airtable, open databases)

Publication Strategy:

- Investigative journalism partnerships (ProPublica model)
- Academic research utilizing FOIA data
- Civil rights organization reports

Recent Success: EFF analysis of Flock searches revealed 50+ federal/state/local agencies searched national database in connection with protest activity; some specifically targeted activist groups (November 2025)[5]

---

5. Constitutional Test Case Development

Strategy: Identify and support sympathetic individual plaintiffs with strong Fourth Amendment claims

Selection Criteria:

- Individuals tracked extensively through ALPR network without warrant
- Documented chilling effect on First Amendment activity (protesters, activists, journalists)
- Clear privacy injury and traceable government action
- Potential for interlocutory appeal (faster Supreme Court path)

Execution:

- Coordinate with civil rights law firms (IJ, CCRJ, ACLU)
- Document surveillance chain of custody
- Preserve evidence (FOIA discovery, witness statements)

Example Case: Norfolk driver tracked 526 times in 4 months without warrant—strong damages/injunction claim[6]

---

6. Administrative Defund Campaigns

Grassroots Tactics:

- Public records requests revealing surveillance program costs
- Calculate cost-per-crime-solved analyses
- Lobby budget committees for defunding
- Support ballot initiatives limiting police surveillance budgets

Information Warfare:

- Demonstrate fiscal waste (expensive technology with marginal crime-fighting benefit)
- Highlight vendor lock-in and predatory contracts
- Show disparate impact on minority communities

PART II: SUPREME COURT CLASS ACTION LITIGATION STRATEGY

I. Constitutional Foundations

A. Fourth Amendment Framework Post-*Carpenter*

Holding: *Carpenter v. United States* (2018) established that warrantless seizure of sensitive location data is a Fourth Amendment search[7]

Key Language:

> "The fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection... Given the unique nature of cell-site location information, the Government's acquisition of the records was a search within the meaning of the Fourth Amendment."

Application to ALPR/Flock:

- Flock captures systematic location data on entire populations
- Far more comprehensive than cell-site data
- Creates permanent records of movement patterns
- Enables retroactive tracking without probable cause

Vulnerability: Courts have NOT yet applied *Carpenter*'s reasoning to ALPR systems, creating Supreme Court cert opportunity

B. Unconstitutional Warrantless Mass Search

Theory: ALPR surveillance performs warrantless searches on the public en masse

Doctrine:

- General warrants (colonial America) prohibited precisely this: searching all to find some
- Fourth Amendment requires individualized suspicion or warrant
- Systematic tracking without warrant = unconstitutional seizure

Authority: *Kyllo v. United States* (thermal imaging); *Jones v. United States* (GPS tracking); *Carpenter* (cell-site data)

C. First Amendment Chilling Effect

Theory: Mass surveillance on protesters/activists chills First Amendment rights

Facts Developed by EFF (2025):

- 50+ agencies searched Flock network for protest-related activity
- Known activist groups specifically targeted
- Clear surveillance of First Amendment-protected activity

Constitutional Doctrine:

- Government cannot suppress First Amendment rights through surveillance
- *Ashcroft v. Free Speech Coalition*: chilling effect on protected speech is injury cognizable in court
- *National Association for Advancement of Colored People v. Alabama*: compelled disclosure of membership chills association rights

Application: Systematic tracking of protesters' movements violates associational privacy and chills political protest

D. Due Process/Fifth Amendment (Taking of Privacy Interest)

Theory: Warrantless seizure of location data is uncompensated taking of privacy property interest

Framework:

- Privacy in movement is constitutionally protected interest (*Carpenter*, *Jones*, *Kyllo*)
- Seizure without warrant or just compensation violates Fifth Amendment
- Systematic, permanent recordation aggravates taking

II. Class Definition & Standing

A. Class Definition

Proposed Classes:

Class 1: Vehicular Movement Tracking (Primary Class)

- All persons whose vehicles were photographed by Flock ALPR network cameras without warrant
- From [Date network implemented] to present
- Across [Multi-state jurisdiction or nationwide]
- Regardless of whether data was searched/accessed by police

Class 2: First Amendment Injury (Protest/Activist Subclass)

- All persons engaged in lawful protest/activist activity whose location data was captured and searched by law enforcement

Class 3: Disparate Impact (Civil Rights Subclass)

- All persons from racial/ethnic minorities disproportionately tracked through Flock network

Class Certification Strengths:

- Numerosity: Millions of vehicles photographed daily
- Commonality: Uniform technology, uniform policy, systematic injury
- Typicality: Named plaintiffs' injuries representative of class
- Adequacy: Civil rights organizations with proven track record as representatives

B. Standing Arguments

Injury in Fact:

- Violation of Fourth Amendment privacy right in movement
- Permanent record of location data without consent or warrant
- Concrete, particularized harm: loss of privacy, chilling of conduct, dignitary harm

Causation:

- Government (via Flock contract and access) directly caused injury through systematic data collection

Redressability:

- Injunction: cease warrantless ALPR operation, delete retroactively collected data
- Damages: statutory damages per violation + actual damages
- Declaratory judgment: ALPR surveillance unconstitutional

Overcome Justiciability Challenges:

- *Clapper v. Amnesty International* requires "certainly impending" injury
- Sustained ALPR photography with permanent database storage = certainly impending injury (not speculative)
- Every moment vehicle operates on public road, photograph likely captured and retained

---

III. Defendant Parties

Federal Defendants:

- DOJ/FBI (access and usage patterns, FOIA shows widespread federal access)[8]
- DHS (use in immigration enforcement)
- Other federal agencies accessing Flock national database

State/Local Defendants:

- State Attorneys General (indirect authorization through state law)
- Municipalities operating Flock networks
- Police departments authorized to conduct searches

Third-Party Defendant:

- Flock Safety, Inc. (private surveillance contractor; potential §1983 liability as state actor; FDCPA violations)

Liability Theories:

- Direct constitutional violation by government entities
- Conspiracy to violate civil rights (42 U.S.C. §1985)
- Private party liability as state actor (Flock operates government surveillance function)

IV. Legal Arguments

A. Primary: Fourth Amendment Warrantless Search/Seizure

Briefing Strategy:

Motion: Extend *Carpenter* beyond cell-site to ALPR location data

Argument:

1. *Carpenter* established that modern location tracking requires warrant
2. ALPR system captures far MORE granular location data than cell-site info
3. Data is permanent, searchable, and accessible to multiple agencies
4. Systematic collection without warrant = per se Fourth Amendment violation

Distinguishing Government Arguments:

- "Photos of vehicles are public": *Yes, individual photos; no, systematic permanent database of all movements*
- "Already decided in Richmond federal court, upheld Flock": Judge applied outdated Third Circuit precedent pre-*Carpenter*; DC Circuit likely reversed on appeal
- "Different from cell-site because not telecom data": Logically irrelevant; *Carpenter* applied analysis to third-party data generally, not just telecom

Proposed Holding:

> "Systematic, warrantless capture and retention of comprehensive location data through ALPR technology violates Fourth Amendment when searched by law enforcement. Government must obtain warrant supported by probable cause prior to searching database for individual's location history."

B. Secondary: First Amendment Chilling Effect

Briefing Strategy:

Motion: Recognize that systematic protest surveillance violates First Amendment

Argument:

1. EFF documented 50+ agencies searching Flock for protest-related activity
2. Known activist groups specifically targeted (Direct Action Everywhere case)
3. Surveillance of protest activity has well-documented chilling effect on First Amendment exercise

Authority:

- *NAACP v. Alabama* (compelled disclosure chills associational rights)

- *Ashcroft v. Free Speech Coalition* (government action creating chilling effect is justiciable)
- *City of Ladue v. Gilleo* (surveillance can chill expressive rights)

Unique Injury: Protesters injured not by direct government interference with speech, but by mass surveillance enabling targeting

Proposed Holding:

> "Systematic warrantless surveillance of protest activity through ALPR networks, used to track and potentially prosecute protesters, creates unconstitutional chilling effect on First Amendment. Class of First Amendment-injured persons has justiciable claim for injunction and damages."

C. Tertiary: Civil Rights/Disparate Impact (If Developed)

Briefing Strategy:

Motion: ALPR surveillance employed with discriminatory effect violating Civil Rights Act

Argument:

1. Facial recognition + ALPR disproportionately impacts minorities (documented algorithmic bias)[9]
2. Police departments in majority-minority neighborhoods deploy Flock cameras at higher rates
3. Pattern of targeting minorities for ALPR searches (develop through discovery)
4. 42 U.S.C. §1983 + Title VI disparate impact claim

V. Procedural Pathway to Supreme Court

A. Litigation Staging

Phase 1: District Court (Year 1-2)

- File class action complaint in favorable jurisdiction (D.C., N.D. California, or E.D. Virginia for constitutional venue)
- Move for class certification
- Government moves to dismiss (inevitably denied on Fourth Amendment claim post-*Carpenter*)
- Discovery phase: obtain all Flock contracts, federal access logs, agency search patterns

Phase 2: Preliminary Injunction (Year 1-3)

- Move for preliminary injunction halting warrantless ALPR searches
- Argue: (1) likelihood of success on Fourth Amendment merits, (2) irreparable harm (ongoing privacy violation), (3) balance of equities (public interest in Fourth Amendment compliance)
- GOAL: Obtain preliminary injunction to create circuit split pressure

Phase 3: Summary Judgment (Year 2-3)

- Move for summary judgment on Fourth Amendment claim

- Argue: unconstitutional as matter of law (no fact question about whether warrantless mass tracking violates Fourth Amendment post-*Carpenter*)

Phase 4: Appeal/Circuit Decision (Year 3-4)

- Anticipate government appeal
- Target circuit with active Fourth Amendment docket

B. Supreme Court Cert Strategy

Timing: File cert petition after circuit decision (even if favorable to plaintiffs, to consolidate law)

Cert Factors Supporting Acceptance:

- **Circuit Split:** Fourth, Fifth Circuits allow ALPR without warrant; *Carpenter* logic suggests Second, Ninth might disagree
- **Constitutional Significance:** Major Fourth Amendment expansion to emerging technology
- **Acute Practical Importance:** 30,000+ police departments now using surveillance technology
- **Question Presented:** "Whether systematic, warrantless capture and retention of comprehensive location data through automated license plate readers violates Fourth Amendment absent warrant supported by probable cause"

Precedent Momentum:

- *Carpenter* (2018) already signaled openness to Fourth Amendment digital privacy
- New justices may be more protective of privacy than 2010s court
- Congress has shown interest in statutory solutions (*Carpenter* itself prompted legislative proposals)

VI. Damages Framework

A. Statutory Damages

42 U.S.C. §1983 (Civil Rights Act):

- Per-violation damages for constitutional deprivation
- Standard: $1,000-$2,000 per violation (baseline; increased for egregious conduct)

Calculation Examples:

- If Flock photos person's car 10x/year for 5 years, warrantless = 50 separate Fourth Amendment violations × $2,000 = $100,000 per person
- Class of 5,000,000 persons = $500 trillion theoretical class exposure (forces settlement)
- More conservative $500/violation × 50 million photos/person × millions of people = still $billions+

Equitable Enhancement:

- Punitive damages if malicious/reckless (targeting protesters, activists)
- Multipliers for egregious conduct (federal access without warrant, targeting protected activity)

B. Injunctive Relief

Primary: Cease warrantless ALPR searches; require warrant for any access to Flock database

Secondary: Data deletion of all retroactively collected photos without warrant

Tertiary: Prospective oversight: independent auditor, monthly reporting to court, sanctions for unauthorized searches

Monitoring: Three-year court oversight of ALPR operations post-injunction

---

VII. Discovery Strategy

Critical Depositions:

1. **Flock Safety executives:** business model, federal agency relationships, data retention, access controls
2. **Federal agency officials (FBI, DHS):** usage patterns, search protocols, targeting criteria, training
3. **Municipal police chiefs:** policy on ALPR searches, retention practices, audit logs
4. **Technology experts:** accuracy rates, false positive rates, retention capacity

Document Requests:

- All Flock contracts with government agencies
- Federal agency MOUs with Flock/municipalities for data access
- Logs of federal agency searches (FOIA-obtained + discovery requests)
- Internal communications regarding ALPR targeting
- Cost-benefit analysis documents (crime solved vs. people surveilled)
- All data breaches, security incidents involving Flock platform

Key Evidence to Develop:

- Targeting of activists/protesters (EFF research shows pattern)
- Racial disparities in ALPR search patterns
- Federal access to data without warrant
- Retention policies (permanent vs. temporary)
- Interagency data-sharing without safeguards

PART III: Political/Legislative Alternatives

If Litigation Path Blocked:

A. Congressional Action (Federal Level)

Model Legislation:

- **"Location Privacy Protection Act"**: Require warrant for government access to comprehensive location data from any source
- **"Data Minimization Act"**: Prohibit government from retaining systematic tracking data unless directly connected to individualized investigation

- **"Third-Party Doctrine Reform"**: Statutory extension of Fourth Amendment to third-party digital data (legislative work-around to case law limitations)
- **"Facial Recognition Moratorium"**: Ban federal funding for facial recognition until privacy safeguards enacted

B. State Constitutional Claims

Backup pathway: Many state constitutions have MORE protective privacy clauses than Fourth Amendment

Target States:

- California (Prop 13)
- New York
- Massachusetts
- Washington (already led on Flock transparency)

State-Level Litigation: Class actions in state courts using state constitutions may succeed even if federal suit fails

---

PART IV: Anticipated Counterarguments & Responses

Government Argument 1: "Third-Party Doctrine Still Applies"

Response:

- *Carpenter* explicitly rejected third-party doctrine for comprehensive digital data
- ALPR goes beyond cell-site data in granularity and comprehensiveness
- Third-party doctrine cannot survive modern technology reality

Government Argument 2: "Photos Taken in Public Have No Privacy Interest"

Response:

- Individual photos in public ≠ systematic database of all movements
- *Carpenter* explicitly holds that aggregated location data has privacy interest even though individual data points public
- Composition and aggregation creates new constitutional interest

Government Argument 3: "Law Enforcement Needs These Tools"

Response:

- Warrant requirement does NOT prevent law enforcement use; it just requires probable cause
- Tools should not be used in ways that violate Constitution
- Fourth Amendment exists precisely to constrain government in name of security

Government Argument 4: "ALPR Doesn't Search Until Police Actually Query Database"

Response:

- Seizure occurs at moment government captures and permanently retains data
- Search is subsequent accessing, but seizure is the capture itself
- Analogous to wiretap: government can't tap and record everything, then claim no search until call is played back

---

PART V: Organizations & Resources

Civil Rights Law Firms (Proven Track Record)

1. **Institute for Justice (IJ)**
   - Leading Flock litigation (Norfolk case)
   - Weak on federal cases but strong on local challenges
2. **ACLU**
   - Extensive surveillance litigation portfolio
   - Strong First Amendment angle capacity
   - Currently litigating Eugene/Stanwood Flock cases
3. **Center for Constitutional Rights (CCR)**
   - Experienced mass surveillance challenges
   - Strong on Third Amendment/state actor theory
   - COINTELPRO history
4. **Electronic Frontier Foundation (EFF)**
   - Leading research and FOIA on Flock
   - Expertise in ALPR networks
   - Coordination with academic researchers
5. **Visible Law**
   - Emerging civil rights firm
   - Co-counsel on Eugene litigation

Law School Clinical Programs

- Harvard Civil Rights-Civil Liberties Clinic
- Yale Civil Rights Clinic
- NYU Center for Law and Security
- Stanford Cybersecurity Law Institute

Academic Researchers

- Jonathan Mayer (Princeton): algorithmic surveillance expert
- Kiel Brennan-Marquez (University of Baltimore): law + tech surveillance scholar
- Conference presentations at Georgetown Tech Law conferences

Coalition Organizations

- Access Now
- Fight for the Future
- Freedom of the Press Foundation

IMPLEMENTATION TIMELINE

Year 1:

- Assemble legal team (identify lead counsel + co-counsel from law firms above)
- File FOIA requests strategically across multiple jurisdictions
- Identify plaintiff(s) with strong personal injury + First Amendment angle
- Begin media outreach, investigative journalism partnerships

Year 1-2:

- Draft complaint with maximum-impact facts
- File class action in optimal jurisdiction
- Move for class certification
- Begin preliminary injunction briefing

Year 2-3:

- Discovery (high-priority: federal agency search logs, targeting patterns)
- Motion practice (summary judgment on constitutional issues)
- Monitor for circuit appeals from other cases (create/accelerate cert readiness)

Year 3-4:

- Obtain favorable district or circuit ruling
- Begin cert petition drafting
- Engage Supreme Court amicus coordination (law professors, civil rights organizations)

Year 4-5:

- Cert petition filed
- Amicus brief coordination
- Oral argument preparation

CONCLUSION

Mass surveillance through ALPR networks operated by Flock and others is NOT constitutionally invulnerable. Post-*Carpenter*, the legal landscape has shifted decisively in favor of privacy protections. A well-coordinated campaign combining grassroots transparency efforts, political advocacy, and sophisticated Supreme Court litigation can systematically dismantle the surveillance state.

The path is clear. The vulnerabilities are documented. The time is now.

References

[1] Carpenter v. United States, 585 U.S. ___ (2018) (holding government acquisition of cell-site location information from third party is Fourth Amendment search).

[2] Washington Court Rules That Data Captured on Flock Safety Cameras Are Public Records, Electronic Frontier Foundation (Nov. 11, 2025), https://www.eff.org/deeplinks/2025/11/washington-court-rules-data-captured-flock-safety-cameras-are-public-records.

[3] ACLU of Oregon and partners sue City of Eugene for failing to disclose public records on Flock cameras, ACLU (Oct. 27, 2025), https://www.aclu-or.org/press-releases/aclu-oregon-and-partners-sue-city-eugene-failing-disclose-public-records-flock.

[4] Public Interest Law Firm Responds to Flock Safety Pausing Federal Access to License Plate Reader Camera Network, Institute for Justice (Aug. 27, 2025), https://ij.org/press-release/public-interest-law-firm-responds-to-flock-safety-pausing-federal-access-to-license-plate-reader-ca.

[5] How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists, Electronic Frontier Foundation (Nov. 20, 2025), https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists.

[6] Police cameras tracked one driver 526 times in four months, lawsuit says, NBC News (Sept. 18, 2025), https://www.nbcnews.com/tech/security/virginia-police-used-flock-cameras-track-driver-safety-lawsuit-surveil-rcna230399.

[7] Carpenter v. United States, 585 U.S. ___ (2018) (establishing that government acquisition of cell-site records was Fourth Amendment search requiring warrant).

[8] See generally EFF Transition Memo: Surveillance Programs Requiring Immediate Attention, at Section 702 discussion (Jan. 19, 2025), https://www.eff.org/wp/eff-transition-memo-incoming-trump-administration.

[9] Facial Recognition and the Fourth Amendment: Search, Seizure, and Constitutional Limits in the Age of Algorithmic Surveillance, International Journal of Forensic and Medico-Legal Research (Oct. 2, 2025), https://www.ijfmr.com/research-paper.php?id=56376 (documenting racial bias in facial recognition systems; discussing application to Fourth Amendment law).