

How does the deployment of Flock Safety's invasive camera networks reshape municipal accountability and alter human agency within public spaces by shifting surveillance power from democratic oversight to private corporate control?

August 26, 2026 | SnugLab Research

Executive Summary

The deployment of Flock Safety's camera networks significantly reshapes municipal accountability and alters human agency within public spaces by shifting surveillance power from democratic oversight to private corporate control. Evidence suggests that the proprietary nature of Flock's technology, its centralized data architecture, and cross-jurisdictional data sharing without explicit local consent bypass traditional democratic oversight, as elected officials' contractual control often proves insufficient for ensuring transparency or preventing misuse [1, 7, 9, 10, 13, 14]. While Flock has introduced new safeguards like reduced default data retention and mandatory audit tools, critics argue these are "cosmetic fixes" that do not fundamentally return control to democratic processes or address the inherent opacity of the system [4, 5, 12, 15, 16]. The key unresolved uncertainty lies in whether these corporate-imposed reforms, or future legislative actions, can genuinely re-establish democratic control over a privately-owned, nationwide surveillance infrastructure.

Key Findings

Shift of Surveillance Power to Private Corporate Control

The operational architecture of Flock Safety's network fundamentally shifts surveillance power from democratic oversight to private corporate control. Democratic oversight, in this context, requires direct public and legislative access to proprietary data models and algorithms, as contractual control alone is insufficient to ensure transparency or prevent corporate dominance [1, 7, 9, 10, 14]. Flock's software and cloud-based data management are proprietary, preventing public and local agencies from independently verifying surveillance practices or detecting misuse [7, 9].

While municipalities can negotiate terms or terminate contracts, these agreements are often made outside public view [9, 10]. Furthermore, despite Flock's claim that customers "own" their data, the nationwide network allows cross-jurisdictional sharing that diffuses accountability beyond local administrative rulemaking [5, 14]. Flock's active resistance to public-records scrutiny, including characterizing FOIA requests as a "coordinated attack," further demonstrates that contractual presence does not guarantee transparent oversight [7, 13]. This opacity means that elected officials' contractual control remains a superficial layer over private corporate control, particularly concerning how AI tools like OS Investigate generate suspicion or process movement data [1, 7, 9, 10, 14].

Limited Effectiveness of Local Oversight and Statutory Retention Limits

Court rulings and municipal audits reveal mixed effectiveness for statutory Automated License Plate Reader (ALPR) retention limits in preventing data misuse or corporate overreach. While some legislative interventions have succeeded, enforcement gaps and judicial interpretations often undermine these limits.

Court Rulings on Transparency and Privacy Limits: California appellate decisions highlight the impact of transparency. In *Bartholomew v. Parking Concepts* (February 2026), the California Court of Appeal ruled that failing to provide a required ALPR privacy policy constituted a legally recognized injury, establishing a basis for consumers to sue [21]. Conversely, *Mata v. Digital Recognition Network* (July 2026) favored the vendor because it maintained a publicly available privacy policy, suggesting compliance protects companies even with extensive data collection [21]. Other rulings show judicial reluctance to broadly apply privacy protections to ALPR data. The Ninth Circuit's decision in *U.S. v. Yang* (2020) limited individuals' ability to challenge government access to private ALPR databases, and the Massachusetts Supreme Judicial Court's ruling in *Commonwealth v. McCarthy* (2020) found that widespread ALPR use did not violate a reasonable expectation of privacy during limited surveillance [20]. Additionally, *Green v. City and County of San Francisco* (Ninth Circuit, 2014) demonstrated that retention policies alone do not prevent misuse stemming from technological inaccuracy, as a device malfunction led to a wrongful traffic stop [20].

Municipal Audit Findings on Compliance and Overreach: Audits consistently show that the mere existence of retention limits or internal policies does not guarantee prevention of misuse. A 2020 California State Auditor report found that the Sacramento Police Department shared ALPR data with over 1,000 agencies nationwide, indicating

that existing regulations did not prevent extensive inter-agency sharing [19]. Similarly, an audit of the Marin County Sheriff's Office revealed that confusing vendor settings allowed three Immigration and Customs Enforcement (ICE) agencies to access ALPR data despite local efforts to limit such sharing [20]. Internal compliance failures are also common, with quarterly audits of the Lexington Police Department's Flock Safety system in 2023 showing officers using vague search justifications like "123456" or "investigation" [22]. A 2023 third-party audit of the Minneapolis Police Department uncovered outdated operational accounts for former personnel, indicating a failure in access control policies [22]. Systemic mismanagement was also highlighted in a July 2020 City Auditor Report for Brownsville, Texas, which found that records were disposed of without committee approval, suggesting ALPR data would be susceptible to mishandling [18].

Effectiveness of Statutory Retention Limits: While many audits show enforcement failures, robust legislative interventions have demonstrated immediate prevention. Washington State's SB 6002 (effective March 30, 2026) imposed strict location-based restrictions and a general 21-day retention limit [8, 13]. This law immediately prevented potential overreach by forcing police departments in Seattle and Kent to deactivate mobile ALPRs because they could not ensure compliance [23]. Other states, such as New Hampshire since 2016, have implemented stringent limits requiring purging records within three minutes unless a match results in an arrest or citation [4, 6, 9].

Corporate-Imposed Safeguards and Their Limitations

As of August 26, 2026, Flock's "Evidence Mode" has not yet been activated by any U.S. municipalities, as it was unveiled in August 2026 and is expected to roll out in the coming weeks [1, 4, 8, 17]. Therefore, there are no documented changes in police discretion or data retention policies directly following its implementation.

However, Flock introduced a broader suite of mandatory policy and product changes in August 2026 to tighten oversight and alter police discretion [4, 7, 10, 17]. Key documented changes include:

- **Data Retention:** Flock shifted its default data retention period from 30 days to 7 days, though existing customers retain their democratically approved periods unless they opt into the new recommendation [2, 3, 4, 5, 7, 8].
- **Police Discretion:** Searches now require a specific case code from records management systems to tie queries to active criminal cases, replacing the previously optional requirement [4, 7, 8, 10, 12, 15].

- **Accountability Tools:** An automated Audit Assistance Tool with proactive lockouts for abnormal search activity became mandatory for all customers by year-end [4, 7, 8, 10, 11, 12].

- **Data Sharing Controls:** Communities gained enhanced offense filtering to block specific crime categories like immigration enforcement, and federal data sharing was set to "default off" for local departments [4, 7, 10, 12, 15, 17].

Critics argue these corporate-imposed reforms are merely "cosmetic fixes" or "window dressing" that do not resolve the fundamental dangers of mass surveillance or shift power back to democratic oversight [4, 5, 12, 15, 16]. More than 50 agencies or communities have canceled, suspended, or rejected a Flock contract or deactivated their cameras since the beginning of 2026, according to one grassroots group [2].

Implications

The findings imply a significant erosion of traditional municipal accountability, as the operational control and data governance of public space surveillance increasingly reside with a private vendor rather than democratically elected bodies. This shift diminishes human agency by subjecting individuals to pervasive, opaque surveillance where the parameters of data collection, retention, and sharing are largely determined by corporate policy and proprietary algorithms. While municipalities retain some contractual leverage, the structural nature of Flock's network means that true democratic oversight, defined by transparency into and control over the underlying technology, remains elusive. This creates a tension between public safety objectives and civil liberties, necessitating robust legislative action and direct access to proprietary systems to rebalance power.

Limitations and Caveats

The report's conclusions are drawn from available evidence, which includes municipal audits, court rulings, and company announcements. However, direct public and legislative access to Flock Safety's proprietary data models and algorithms remains limited. The full impact of newly introduced features like "Evidence Mode" and other policy changes, unveiled in August 2026, has not yet been empirically observed in municipal deployments. While the original question was scoped globally, specific quantitative data and detailed case studies are predominantly from U.S. municipalities, limiting the ability to draw definitive global conclusions.

Sources

- [1] [wiki] Flock Safety - en.wikipedia.org - https://en.wikipedia.org/wiki/Flock_Safety
- [2] Flock Safety Tightens Safeguards As States Cities Question S - stateline.org - <https://stateline.org/2026/08/14/flock-safety-tightens-safeguards-as-states-cities-question-surveillance-network/>
- [3] Know Your Tech Flock - aclu-or.org - <https://www.aclu-or.org/know-your-tech-flock/>
- [4] Effs Investigations Expose Flock Safety's Surveillance Abuses - eff.org - <https://www.eff.org/deeplinks/2025/12/effs-investigations-expose-flock-safety-s-surveillance-abuses-2025-review>
- [5] Flock Releases Accountability Features - asisonline.org - <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/august/Flock-Releases-Accountability-Features/>
- [6] [peer-reviewed] Stable - jstor.org - AUTHORS UNAVAILABLE - <https://www.jstor.org/stable/27317055>
- [7] Who Is Flock Safety - maryvilleprivacy.org - <https://www.maryvilleprivacy.org/maryville-residents-for-privacy/who-is-flock-safety/>
- [8] Flock Safety Camera System FAQ - cityofbartlesville.org - <https://www.cityofbartlesville.org/flock-safety-camera-system-faq/>
- [9] The Private Companies Quietly Building A Police State - campaignzero.org - <https://campaignzero.org/the-private-companies-quietly-building-a-police-state/>
- [10] State And Surveillance - cigionline.org - <https://www.cigionline.org/articles/state-and-surveillance/>
- [11] Flock Announces Security Amid Data Privacy Concerns 13561939 - goodmorningamerica.com - <https://www.goodmorningamerica.com/news/story/flock-announces-security-amid-data-privacy-concerns-13561939>
- [12] [gov] Show Public Doc - ecf.ksd.uscourts.gov - https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2024cr10010-48+
- [13] [news] Flock Contracts Canceled Immigration Surveillance Concerns - npr.org - <https://www.npr.org/2026/02/17/nx-s1-5612825/flock-contracts-canceled-immigration-surveillance-concerns>
- [14] Flocks Terms And Conditions - aclu.org - <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flocks-terms-and-conditions>
- [15] Restrictions Flock Cameras - mrsc.org - <https://mrsc.org/stay-informed/mrsc-insight/april-2026/restrictions-flock-cameras>
- [16] Jul 2126 4 - emeraldbook.org - <https://emeraldbook.org/news/jul-2126-4/>
- [17] [blog] Customers Own And Control Their Flock Data - flocksafety.com - <https://www.flocksafety.com/blog/customers-own-and-control-their-flock-data>
- [18] 6030740 Civil Liberties Backlash Ai Surveillance - thehill.com - <https://thehill.com/policy/technology/6030740-civil-liberties-backlash-ai-surveillance/>
- [19] [blog] Flock Guardrails Address Lpr Privacy Concerns And Police Tra - flocksafety.com - <https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency>
- [20] [gov] Crs Product - congress.gov - <https://www.congress.gov/crs-product/IF13068>
- [21] Flock Safety Credibility Lost As It Repeatedly Lies To City - aclu.org - <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-departments-and-public-across-the-country>
- [22] Privacy Vs Public Records The Politicization Of Alpr Data - policerecordsmanagement.com - <https://policerecordsmanagement.com/privacy-vs-public-records-the-politicization-of-alpr-data/>
- [23] Alpr Data Privacy Eliminate Data Misuse Fears - platesmart.com - <https://platesmart.com/alpr-data-privacy-eliminate-data-misuse-fears/>