COMMENTARY

A response to Brandon del Pozo, ALPRs and the Principles of Democratic Public Safety (July 2026)

The Infrastructure We Haven't Consented To: Why Flock's ALPR Network Remains a Fourth Amendment Problem

[Wylie Stecklow, Wylie Stecklow PLLC]

Brandon del Pozo brings twenty-three years of policing experience and a PhD in philosophy to this debate, and his paper deserves engagement on the merits, not dismissal as industry talking points. To his credit, the Flock Safety funding relationship is disclosed candidly on the title page, along with a stated condition of editorial independence and peer review.

And to be clear, I like and respect Brandon del Pozo. I even agree with one of del Pozo's central arguments: collecting a license plate on a public road is not, under current case law, a Fourth Amendment search. The paper's focus avoids the less defensible position that ALPRs are always fine, and focuses more on how that data gets aggregated, queried, and shared. And again, we agree that this is the point where the real debate starts. Unsurprisingly, we don't finish the debate agreeing.

Where del Pozo's framework is right, I say so. Where it falls short, I try to show why, often using the paper's own data and sources against its conclusions. I also draw heavily on an August 2026 report by the Surveillance Technology Oversight Project (S.T.O.P.) and LatinoJustice PRLDEF, Flock Favors: Police Across New York Search Flock on Behalf of ICE, which tests del Pozo's governance model against real search logs from the same state and months he writes about.

Where the Paper Is Right, and Why the Concession Isn't the End of the Analysis

Del Pozo is correct, under existing precedent, a license plate on a public road carries no independent expectation of privacy, and most courts haven't treated ALPR collection, on its own, as a search. ALPR data, read in isolation, is narrower than a phone's contents, a browsing history, or a financial record as it doesn't reveal who was driving, why, or what they did next. And real governance including role-based access, documented purpose codes, search limits, retention caps, and independent audits, would meaningfully reduce the risk of misuse, if vendors, administrators or legislative bodies actually put it in place.

But conceding that baseline isn't the same as endorsing it and showing that safeguards could reduce misuse isn't the same as showing that they do. My response takes up both of these points.

The paper's own escalation ladder concedes more than it appears to

Del Pozo identifies a four-stage model for ALPR - collection, storage, querying, and aggregation. The paper then places the constitutional trigger at the point ALPR data is combined with an outside source: financial records, cell-site data, and so on. I disagree that the constitutional line is drawn at ALPR data being combined with other data, and the very caselaw authority cited in support of the combination requirement, in fact, doesn't require that combination. *Commonwealth v. McCarthy*, 484 Mass. 493, 506 (2020), the Massachusetts high court decision the paper leans on, opines that "with enough cameras in enough locations," ALPR location data alone could invade a reasonable expectation of privacy. The court ruled network density and duration could be sufficient on their own to trigger constitutional protections. *McCarthy* ruled in favor of law enforcement because it only involved four fixed cameras on two bridges. Flock's network now runs more than 120,000 cameras across 6,000-plus communities in 49 states, capturing roughly 20 billion scans a month. Del Pozo cites *McCarthy* for his framework, but the holding can easily be the seed of the opposite argument: enough aggregated tracking data ("mosaic theory," *Id.* at 504) violates the framers' aim "to place obstacles in the way of a too permeating police surveillance," *Id.* at 499.

Carpenter does not condition its holding on combining unlike data sources

Carpenter v. United States, 585 U.S. 296 (2017), held that cell-site data revealing "the whole of a person's physical movements" is constitutionally protected. Full stop. The Court never made the protection contingent upon a subsequent cross-reference with banking records, and I don't think that qualifier can be read into the decision. What worried the Court was the totalizing nature of the record itself; not how many different types of data went into building it. A dense enough ALPR network builds exactly that kind of record using just one data type, and that's all *Carpenter* actually requires. The paper's framework assumes something more: that ALPR data needs to be combined with a second category of data, financial records, cell-site pings, before any privacy interest kicks in. I don't see that requirement in *Carpenter*.

The paper's anchor precedent is the one now being retested

There is also a precedential issue that has arisen since January 2026, when *Schmidt v. City of Norfolk*, 819 F.3d 492 (E.D. Va. 2026), the case the paper treats as the clearest sign that ALPR deployments survive Fourth Amendment scrutiny, was decided. It is now on appeal to the Fourth Circuit. In the interim, the Supreme Court decided in *Chatrie v. United States*, 609 U.S. __ (2026), a related location-tracking case, that people do have a reasonable expectation of privacy in cell-phone location data. It also rejected the government's fallback argument that a search is fine as long as it only draws a narrow slice out of a much bigger retained dataset. That matters for the retention argument I make below, because it tells courts to look at what a system is capable of doing, not how big a slice an officer happened to ask for in one case. While Mr. del Pozo could not have anticipated it, the ground has shifted under him, and his anchor case is now being reconsidered in light of *Chatrie*.

The "pattern-of-life" scoring exercise undercounts by construction

Figure 1 gives ALPR records a "pattern of life" score of 17 percent, against 92 percent for browsing history and 83 percent for cell-phone data. But look at what's actually being measured: a single, isolated ALPR read, not the retrievable, aggregated output of a network of 120,000-plus always-on cameras queried across a chosen date range. Score a single credit-card swipe or a single cell-tower ping in isolation and you'd get a low number too. That's exactly the point of *Carpenter*: a lot of low-information points, stacked up over time, add up to a high-information result. Scoring one plate read instead of what an agency can actually retrieve and reconstruct misses exactly what *Carpenter's* "whole of a person's physical movements" holding was written to catch. Id. at 297, 310.

Governance Theater: What the Model Policy Promises vs. What New York Agencies Actually Did

This is where the S.T.O.P./LatinoJustice PRLDEF findings matter most. They take del Pozo's oversight claims, the documented purpose codes, the role-based access, the audits, and test them against real search logs instead of policy language.

A documented reason is not a safeguard if agencies can write anything, or nothing at all

The paper's own recommended controls identify "a legitimate reason for every search" and "regular oversight and auditing" among six core levers. Yet, in New York logs reviewed by S.T.O.P. and LatinoJustice PRLDEF (that were only obtained through hard fought public-records requests), officers in Nassau County, Beacon, Glen Cove, and Cheektowaga entered reasons like "Immigration (civil/administrative)," "ICE," and "Wanted by ICE" for drivers suspected of no crime; one State Police search tied to the same plate as a DHS query was logged only as "Investigation." Because officers can enter any reason, **or none,** the report's authors note that the immigration-tagged searches they found are likely a small percentage of the true total. A reason-code requirement is only a safeguard if someone reviews it before the harm occurs. Here it functioned, at best, as a paper trail discoverable months later through outside litigation in a state whose *Local Cops, Local Crimes Act* (N.Y. Exec. Law § 170-k (McKinney 2026)) exists specifically to prohibit this kind of cooperation with ICE.

A separate NYCLU review backs up the S.T.O.P./LatinoJustice findings. When Syracuse police "inadvertently" opted into Flock's confederate (interagency, interjurisdictional) network, outside jurisdictions searched Syracuse drivers' data 4.4 million times between June 2024 and July 2025, 2,097 of them labeled immigration related. Denver's audit logs show searches run on behalf of ICE more than 1,400 times in that same period, and in June 2025 California agencies shared ALPR data with ICE over 100 times, in direct violation of state law. Three different jurisdictions. Three separate audits. And in each one, the same result: exactly what the paper's oversight framework was supposed to prevent (NYCLU, *How License Plate Readers Track Your Every Move*, May 2026).

Confederated search reach is not a hypothetical — it appears in del Pozo's own footnotes

The paper's own citations acknowledge that agencies nationwide have queried distant jurisdictions' Flock data hundreds of thousands of times, and that both Ventura County and San Francisco audits documented flows reaching federal immigration authorities. Del Pozo's read is that this volume "reflects the automation of the process rather than the intentions of the agencies involved." That's the critics' point, not a rebuttal: a system that routes one officer's query into every participating jurisdiction's database by default functions as a general-warrant system regardless of intent. The paper's own cited University of Washington research documents direct, back-door, and on-behalf-of searches of Washington ALPR data by federal immigration authorities, and a Texas agency using the network in connection with an out-of-state abortion investigation. These aren't edge cases. This is the network doing exactly what its confederation design lets it do.

Vendor self-regulation arrived after press exposure, and covers only one company

The paper cites Flock's August 2026 policy changes with shorter retention, mandatory search-category tagging, and automated anomaly detection, as proof the system can self-correct and Flock can self-police. Those changes followed a Washington Post investigation into officers using the network to track romantic partners, published days earlier, per the S.T.O.P. / LatinoJustice report. Stricter governance that a company adopts in response to bad press, and which they can quite obviously unilaterally alter or revoke whole cloth isn't democratic regulation, and it does nothing for jurisdictions switching to competitors like Axon with no comparable safeguards. A governance model that depends on one company's PR incentives can be a durable check on state surveillance.

This is not a governance gap. It is the system working as designed.

The paper treats every documented failure here, the concealed ICE searches, the system search sprawl, the safeguards that only kicked in after press exposure, as proof that governance is incomplete, not that it's impossible. That distinction matters a lot, and I think the short history we actually have points the other way. This isn't a knock-on Mr. del Pozo's scholarship. It's a challenge to the premise underneath the white paper: that a commercial, confederated network like Flock's can be governed into compliance at all.

A safeguard can only work if whoever can enforce it is willing to enforce it, even against its own interest. Local agencies have every operational reason to keep utilizing a network that helps them close cases, including using it for purposes their own state has banned. Flock has every commercial reason not to police its police customers aggressively: the agencies it would need to discipline are the ones paying for the service, and a vendor that restricts a paying customer risks losing them to a competitor with fewer guardrails. And the oversight bodies nominally in charge are not paying attention and the public has had to rely on what journalists, litigants, and public-records requesters happen to surface, leaving an unknown category of violations that no one inside the system ever finds.

The paper's framework isn't wrong because its safeguards are poorly specified. It's wrong because it assumes a governance environment of disinterested agencies, a vendor willing to

discipline its own customers, statutes enforced the moment they're violated. Every layer of governance in the paper relies on an actor in existence with both the incentive and the authority to execute the safeguards. No such actor has shown up in the record, and the paper doesn't explain why one would.

In a perfect world, ALPR bounded by real retention limits, real access controls, and real consequences for misuse might be defensible. We don't live there. Personally, I live in a state that passed a law specifically to stop this conduct. Yet, law enforcement departments kept doing it anyway, undetected until FOIL requests uncovered it. That isn't a bug in an otherwise sound system. It's the system working as designed.

Judging the technology by the governance regime that could theoretically exist, rather than the one that's actually been tried and has actually failed, is the paper's weakest pillar. The Fourth Amendment was written by people who'd lived under general warrants with blanket search powers and meant never to trust a government's promise of restraint. A surveillance architecture that can only be governed in theory, and has already failed in practice, is exactly what the Amendment exists to foreclose, not a technology awaiting better rules, but one at odds with the principle that citizens' privacy shouldn't depend on the discretion of the watchmen.

Retention: Paid for by the Company It Benefits

The paper leans on a Flock-commissioned analysis of 2024 FBI NIBRS clearance data to argue that even the vendor's new seven-day default retention period "strongly emphasizes privacy protections over the sheer efficacy of the technology," since a meaningful share of homicide, trafficking, and sex-offense arrests happen more than twenty-one days out. I'd take that with a grain of salt. A retention study funded by the company whose product gets more valuable with every extra day of data it's allowed to keep is not a neutral voice in a debate about how long to hold location data on people who've never been charged with anything. S.T.O.P. and LatinoJustice PRLDEF looked at the same question and came out somewhere very different: a 48-hour default, with exceptions for evidence and warrants, because in their view a longer window just means a longer window for misuse. Really, the disagreement isn't about whose numbers are right. It's about who pays the price for the false positives in a system that sweeps up thousands of people to occasionally find the one it's actually looking for.

Beyond Doctrine: Why We Shouldn't Build This, Even Where Courts Allow It

The paper is organized by framing its inquiry as "not whether ALPRs should exist … but how they should be governed." That framing is a decision, and I disagree that the first question is one that can simply be brushed past.

The chilling effect falls hardest on populations the paper's cost-benefit model does not weigh

The paper's analysis is built around clearance rates and equitable camera placement, and that's simply too narrow. It leaves out the chilling effect on immigrants, protesters, and people seeking or providing reproductive healthcare, who now have real, documented reasons to believe that driving through camera coverage creates a searchable, potentially ICE-accessible record. That's

not a hypothetical; it's what the S.T.O.P./LatinoJustice report found actually happening, in a state with a statutory ban on that exact cooperation. You don't need to be arrested for a surveillance system to harm you. The chill on protected movement and association is itself the harm the Fourth and First Amendments were written to prevent.

Verification doesn't fix staleness, and Caselaw doesn't require accuracy

The paper admits two aspects of ALPR failures that "subject innocent citizens to dangerous and stressful encounters with police" (p. 26): a misread plate, and a stale entry — a car reported stolen, later recovered, that stays flagged in the ALPR database until an officer updates the record and clears it. His suggested fix is to verify the plate reading before it's entered in the database, and to confirm the alert is "valid and actionable" before a stop (p. 34). While this may catch the first problem, it will not cure the second: an entry accurate the day it was entered will pass every check and still be wrong once someone else is driving the car. The same failure predates ALPR: it shows up wherever police use facial recognition software. That technology has supported wrongful arrests of Robert Williams, Randal Reid, Nijeer Parks, Michael Oliver, and several others — nearly all Black — some despite a department policy, like Hennepin County's, that a software hit alone shouldn't support an arrest. Fan, *Suspecting with Data*, 109 Minn. L. Rev. 2253, 2293–96, 2315–16 (2025). A verification rule on paper didn't stop the error from negatively impacting real people there, and there's no reason to expect it will here. A judicial backstop for errors in the system does not exist. In *Kansas v. Glover*, 589 U.S. 376 (2020), the Court upheld a stop based on a reasonable inference from a vehicle record even though it knew the inference would sometimes be wrong. In other words, reasonable is enough; accurate isn't required. Better recordkeeping lowers the error rate, it doesn't erase it, and the harm from what's left isn't spread evenly: for most drivers it stays ephemeral, the impact of a database check they may never feel; but for the one it lands on, it's concrete, a roadside stop and at a bare minimum, momentary deprivation of liberty. Moreover, that harm nearly always falls hardest on someone who already deals with police the most. None of that shows up in the paper's effectiveness metrics. That harm isn't rare. It's just uncounted.

Infrastructure outlasts the intentions of the people who built it

The paper's history section reviews two decades of NYPD ALPR use in support of its assertion that there is no public record of political or religious tracking. But that misses the forest for the trees. The critique is not that today's operators intend to misuse the system. It's that a searchable, aggregated, nationally confederated tracking network, once built, stays available to whoever holds administrative access next, under whatever policy a future legislative body or administration adopts. It is much easier to rewrite private or public use policies than it is to remove a camera. New York is the clearest example of what will happen. A law was enacted designed to stop informal cooperation between New York law enforcement and ICE. Yet, within the year, documented searches continued, caught and published only by outside public-records requests, not by any of the paper's built-in safeguards.

Consent was never obtained at the scale the network now operates

It must also be remembered that many, if not all, of the 6,000+ communities within Flock's network procured cameras through routine police purchases, not legislative or public debate about joining a nationwide, cross-jurisdictionally searchable database. Del Pozo's own paper acknowledges that data has been shared "in ways the collecting community does not consent to"

— including, by his own citations, into immigration enforcement and reproductive-healthcare investigations a jurisdiction may have specifically chosen not to assist. A governance framework solely built on agency policy coupled with a vendor's terms of service does not equal community consent. A technology this far-reaching should have required such community support at the outset.

What communities do once they learn what they signed up for is its own hard evidence of the lack of consent in the first place. Tompkins County's legislature voted down its Flock renewal 12 to 1; Ithaca terminated its contract as incompatible with its sanctuary-city policy; residents in Troy, Scarsdale, Poestenkill, Saranac Lake, and Pine Plains have each pushed successfully to cancel or defund similar contracts. Communities do not organize to exit an arrangement they knowingly consented to in the first place (NYCLU, *How License Plate Readers Track Your Every Move,* May 2026, *See also,* NYCLU's suit on behalf of Westchester drivers suing the County over Mass Vehicle Surveillance System,*(* *https://www.nyclu.org/press-release/westchester-drivers-sue-county-police-department-over-mass-vehicle-surveillance-system*)).

Conclusion

Mr. del Pozo's paper may very well be the most intellectually honest and rigorous defense of Flock's governance model available, and he's right that ALPR data, in isolation, is a comparatively narrow category of information. But "narrow in isolation" isn't "narrow in aggregate," and the paper's own sources — the *McCarthy* dictum on camera density, the Washington confederated-search research (n. 10), the out-of-state audit findings (n. 9) — supply much of the evidence for the opposite conclusion once density, retention, and confederation are taken seriously instead of bracketed off as problems to solve later. The S.T.O.P./LatinoJustice findings show what "solved later" looks like: apparent cooperation with ICE continuing under a law written to prohibit it, surfaced only by outside records requests, with no enforcement against any agency involved.

None of this means Flock's use of ALPR technology has no legitimate use in the abstract. It means the Flock paper has evaluated the technology against the oversight needed that could *theoretically* exist, not the one that actually exists and has failed. A privately operated, nationally confederated, thinly audited surveillance network that is deployed faster than legislatures can regulate, and answerable only to whichever outside party happens to catch it, isn't a technology whose defects get cured by a better policy document. Del Pozo's critical thinking is apparent throughout the white paper, which sets forth the right governance questions. But our conclusions, perhaps, reflect where our backgrounds diverge. Brandon's twenty-three years in law enforcement[1] against my decades as a civil rights practitioner, and Flock's short history persuades me: governance, here, has been an illusion. This infrastructure is being built anyway, in an imperfect world of misaligned incentives and undisclosed violations — and that should trouble anyone who takes the Fourth Amendment seriously.

[1] Though law enforcement experience alone will not necessarily dictate a positive view of Flock and ALPRs. *See New York's Finest: Retired & Unfiltered Podcast, August 19, 2026, Flock Cameras: Public Safety or Mass Surveillance,* where ex-NYPD officers- John Macari, Eric Dym and Marlon Bethel, explain their concerns over Flock Cameras and government mass surveillance.

September 2026