

September 29, 2026

Chair Wasserman, Vice-Chair O'Connor, and Members of the Milwaukee County Board Committee on Parks and Culture:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide comments in support of File #26-640- A resolution directing removal of fixed Flock Condor and automated license plate reader (ALPR) camera equipment from Milwaukee County park property, and opposing the use of ALPR technology for tracking individuals' movements.

The proliferation of artificial intelligence-powered surveillance networks—perhaps most notably automated license plate readers (ALPRs) deployed by companies like Flock Safety—has sparked a fierce nationwide backlash that defies traditional partisan lines. At the end of August, Texas Governor Greg Abbott announced he was blocking state agencies from spending money on Flock cameras, Florida Governor Ron DeSantis ordered the state DOT to revoke ALPR permits on state roads, and Pennsylvania Governor Josh Shapiro said he would welcome bipartisan legislation banning Flock cameras across the state.¹ Just last week, the U.S. Senate Judiciary Subcommittee on Crime and Counterterrorism held a hearing on the profound bipartisan concerns surrounding privacy and this AI-powered mass surveillance technology.²

As U.S. Senator Josh Hawley wrote in a letter to Flock Safety's CEO Garrett Langley, Flock "boasts more than 120,000 cameras across 49 states and more than 20 billion vehicle scans every month."³

The ACLU of Wisconsin supports the removal of Flock ALPR and Condor cameras from the Milwaukee County Parks in light of the company's pattern of misleading statements to local governments about its business practices, the profound safety risks illuminated by the explosion of ALPR misuse cases and ALPR inaccuracies, and the distinct concerns surrounding the warrantless tracking of people and vehicles in spaces like parks.

Flock Safety Has Lost Its Credibility

We urge supervisors to stay vigilant and not treat the talking points, flashy marketing materials, and soothing assurances of surveillance tech public relations teams as unquestioned truth. Flock Safety is a multi-billion-dollar company that has expended significant resources lobbying county and municipal officials, including creating a coaching guide for law enforcement agencies entitled, "How to Speak to City Councils About Public Safety Technology."⁴

¹ "Flock cameras draw opposition from across the political spectrum," NPR (Sept. 5, 2026), <https://www.npr.org/2026/09/05/nx-s1-5955778/flock-surveillance-camera-opposition-politics>.

² "Flock, Axon dodge Senate hearing after invite from Chair Josh Hawley," CNBC (Sept. 23, 2026), <https://www.cnbc.com/2026/09/23/flock-axon-senate-hearing-josh-hawley.html>; "Always Watching: Flock's Nationwide AI Surveillance Network," U.S. Senate Committee on the Judiciary, <https://www.judiciary.senate.gov/committee-activity/hearings/always-watching-flocks-nationwide-ai-surveillance-network>.

³ <https://www.hawley.senate.gov/wp-content/uploads/2026/08/2026-08-26-Hawley-Letter-to-Flock-CEO.pdf>

⁴ "'Own the Narrative': Leaked Flock Guide Shows How It Teaches Cops to Promote Its Tech," 404 Media (Aug. 3 2026), <https://www.404media.co/own-the-narrative-leaked-flock-guide-shows-how-it-teaches-cops-to-promote-its-tech/>.

- At an **Oshkosh** Common Council meeting in April, a Flock executive denied that their ALPR system could create heat maps of a vehicle's movements—leading the council to approve a contract that night, only to discover the next morning that Flock had made false statements. The Council then unanimously voted to rescind its Flock contract just 24 hours after their initial approval.⁵
- In **Sheboygan**, city officials moved to terminate their Flock contract after learning that the company had attempted to sell data collected from the city's cameras, including information about traffic volume, vehicle types, and speeds. The police department said it had not consented to the sale and believed the conduct violated its agreement with Flock.⁶
- **Boston** recently announced that it would not continue using Flock after discovering that a data-sharing function had been enabled during a pilot despite a contractual agreement requiring that sharing to be disabled. According to Boston officials, the feature had been enabled by the vendor in error and could have allowed other law enforcement agencies to access data collected by Boston's cameras.⁷
- In **Colorado**, Flock assured Loveland's police chief and the public that federal agencies were not accessing local data because the company held no federal contracts. After evidence proved otherwise, Flock admitted to active pilot contracts with CBP and DHS, chalking up the misinformation to poor communication on the company's part.⁸

This reflects a broader pattern of Flock regularly misleading or even lying about its business practices, safety record, commitment to privacy, and efforts to protect vulnerable populations. Despite countless assurances from law enforcement agencies Flock's PR team to the contrary, we've seen how ALPRs have caused harm across the country.

ICE and CBP have repeatedly used Flock to go after immigrants without warrants.⁹ Kansas police used them to pursue a man who wrote a critical op-ed about the department.¹⁰ A Colorado police officer wrongfully accused a woman of theft based on a Flock hit.¹¹ A mother and her children were held at gunpoint because ALPR cameras wrongly flagged their car as stolen.¹²

⁵ "Oshkosh council rescinds Flock camera contract after 'false statements'," WBAY (April 22, 2026), <https://www.wbay.com/2026/04/23/oshkosh-council-rescinds-flock-camera-contract-after-false-statements/>.

⁶ "Sheboygan canceling Flock contract over undisclosed data tracking," Fox 6 (Sept. 3, 2026), <https://www.fox6now.com/news/sheboygan-canceling-flock-contract-over-undisclosed-data-tracking>.

⁷ "Boston drivers' data left unsecured during Flock pilot due to vendor 'error,' city officials say," Boston.com (Sept. 15, 2026), <https://www.boston.com/news/local-news/2026/09/15/boston-drivers-data-left-unsecured-during-flock-pilot-due-to-vendor-error-city-officials-say/>.

⁸ "Flock Safety Credibility Lost as it Repeatedly Lies to City Councils, Police Departments, and Public Across the Country," ACLU (July 2, 2026), <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>.

⁹ "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows," 404 Media (May 27, 2025), <https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/>.

¹⁰ "Lenexa police investigated author of column criticizing the department. He's 'pissed off,'" NPR (Feb. 2, 2026), <https://www.kcur.org/politics-elections-and-government/2026-02-02/lenexa-police-investigated-column-writer-critical-failure-warn-ice-raid-councilwoman-investigation>.

¹¹ "Flock cameras lead Colorado police to wrong suspect: 'It became my job to prove my innocence,'" CBS News (Nov. 13, 2025), <https://www.cbsnews.com/colorado/news/flock-cameras-lead-colorado-police-wrong-suspect/>.

¹² "When license plate readers get it wrong," CBS News (July 24, 2025), <https://www.cbsnews.com/news/license-plate-readers-alpr-mistakes/>.

A Florida woman spent 13 days in jail facing vehicular homicide charges after Flock mistakenly flagged her car as matching the description of the car involved in the incident.¹³

On July 11th, the Los Angeles Police Department – the third largest police force in the U.S. – allowed its contract with Flock to expire, and the LAPD deactivated all 138 of its Flock cameras. The decision followed an internal audit by the LAPD Office of the Inspector General, which revealed that over a just two-month period, the LAPD had investigated 161 car owners whose vehicles were wrongly identified as stolen by Flock’s system.¹⁴ City leaders stated they walked away due to serious concerns over civil liberties, data ownership, and sharing protocols.

An analysis of nearly 1,500 Flock camera alerts sent to police in Roseville, California flagging vehicles as stolen or used in a felony found that 71% of the time, Flock incorrectly read the license plates.¹⁵

The profound safety and privacy risks of this technology are not hypothetical.

Documented ALPR Misuse by Wisconsin Law Enforcement

In addition to the weaponization of ALPR surveillance by the federal government and other jurisdictions, there is a well-documented pattern of misuse by local law enforcement officers themselves across the country.¹⁶ In Wisconsin—officers are alleged to have used ALPR systems repeatedly for personal, non-investigative purposes.

- **Menasha**, Wisconsin police officer Cristian Morales was charged with misconduct in office for allegedly using a license plate reader system to track a romantic partner.¹⁷ The Washington Post reported Morales “used Flock to check whether his then-girlfriend had gone to a clinic to ‘seek a potential termination of said pregnancy’.”¹⁸
- **Milwaukee** police officer Josue Ayala pled guilty to using Flock to search the license plate of his romantic partner 124 times and the license plate of his partner’s ex 55 times within a three-month time period.¹⁹ According to the criminal complaint, Ayala entered “investigation” as the reason for each search. The misuse was only uncovered after a victim searched their license plate on “HaveIBeenFlocked.com” and alerted police.

¹³ “Innocent woman says police use of Flock camera led to 13 days in jail,” Fox News (Sept. 9, 2026), <https://www.foxnews.com/tech/innocent-woman-says-police-use-flock-camera-led-13-days-jail>.

¹⁴ “LAPD Pulled Over 161 Innocent Drivers Because License Plate Readers Said Their Cars Were Stolen,” Yahoo News (July 13, 2026), <https://www.yahoo.com/news/us/articles/lapd-pulled-over-161-innocent-181207332.html>.

¹⁵ “In one California town, Flock misread license plates in 71% of the alerts it sent to police,” Business Insider (July 31, 2026), <https://www.businessinsider.com/flock-camera-misread-license-plate-reader-california-roseville-police-2026-7>.

¹⁶ “Police Keep Losing Their Jobs for Using Flock Cameras to Stalk People,” Mother Jones (July 18, 2026), <https://www.motherjones.com/politics/2026/07/police-losing-jobs-flock-cameras-alprs/>.

¹⁷ “Menasha police officer accused of license plate recognition system to track his ex,” Fox 11 News (Jan. 9, 2026), <https://fox11online.com/news/crime/menasha-police-officer-accused-of-using-license-plate-recognition-system-to-track-his-ex-girlfriend-cristian-morales-misconduct-in-office-flock-domestic-abuse-restraining-order-cash-bond>.

¹⁸ “How rogue officers turned a nationwide camera network into a tool for stalking,” Washington Post (Aug. 2, 2026), <https://wapo.st/4hf8tgJ>.

¹⁹ “Milwaukee Cop Used Flock Cameras to Track Romantic Partner,” Urban Milwaukee (Feb. 25, 2026), <https://urbanmilwaukee.com/2026/02/25/milwaukee-cop-used-flock-cameras-to-track-romantic-partner/>.

- Former **Kenosha** County Sheriff Deputy Frank McGrath resigned after an internal investigation concluded that he had knowingly and repeatedly misused restricted law enforcement databases. According to the investigation, McGrath allegedly used the Flock network along with a squad car tracking system to remotely monitor another deputy he had been dating, entering “suspicious” as the search reason in the system.²⁰ In August, he was criminally charged with two felony counts of misconduct in public office.
- Criminal charges were filed against **Milwaukee** Police Department Internal Affairs Detective Tehrangi Chapman, who allegedly used Flock’s ALPR system to track two individuals’ locations a total of 20 times over the course of one year.²¹ Shockingly, this MPD Internal Affairs Detective was entrusted with investigating former officer Ayala’s Flock misuse.
- In July, reporting revealed that officers with the **Racine** Police Department and Racine County Sheriff’s Office were under criminal investigation for misusing Flock.²²
- A federal lawsuit claims the **Waukesha** County Sheriff’s Office used Flock cameras to target U.S. Navy veteran Napoleon Jones in retaliation for exercising his First Amendment right to record a traffic stop.²³
- While specifically ALPR technology, **Greenfield** Police Chief Jay Johnson faces felony misconduct charges after allegedly ordering the installation of a department-owned surveillance camera outside his home while in the midst of a divorce proceedings.²⁴

These examples illustrate a consistent reality: misuse is not rare, and it is not prevented by policy alone. When systems allow for the tracking of individuals at scale, abuse becomes an inherent risk.

Removing AI-Powered ALPRs and Flock Cameras from Milwaukee County Parks

Parks are more than a piece of public infrastructure. They are some of the few places where people can gather, organize, protest, worship, socialize, exercise, and participate in community life without needing to purchase access to a private space. The County should not turn these public gathering spaces into surveillance checkpoints.

Flock Safety’s AI-powered ALPRs use advanced computer vision algorithms to automatically identify and catalogue the make, model, color, and license plate of passing vehicles. Flock’s Condor product is also AI-powered and equipped with people and vehicle detection, visible alerts, searchable footage, remote pan/tilt/zoom controls, and integration with other Flock systems.

²⁰ “Wisconsin communities grapple with police misuse of Flock surveillance,” Wisconsin Examiner (March 13, 2026), <https://wisconsinexaminer.com/2026/03/13/wisconsin-communities-grapple-with-police-misuse-of-flock-surveillance/>.

²¹ “Second member of the Milwaukee Police Department charged with misuse of license plate reader system,” WPR (July 9, 2026), <https://www.wpr.org/news/member-milwaukee-police-department-misuse-of-license-plate-reader-system>.

²² “Two Racine police officers under investigation for alleged Flock camera misuse; DA also reviewing RCSI case,” TMJ4 (July 13, 2026), <https://www.tmj4.com/news/local-news/in-your-community/racine-county/two-racine-police-officers-under-investigation-for-alleged-flock-camera-misuse-da-also-reviewing-rcso-case>.

²³ “Wisconsin Cops Used Flock Over 100 Times To Track a Navy Veteran After He Lawfully Recorded a Traffic Stop,” Reason, (Sept. 2, 2026), <https://reason.com/2026/09/02/wisconsin-cops-used-flock-over-100-times-to-track-a-navy-veteran-after-he-lawfully-recorded-a-traffic-stop/>.

²⁴ “Police chief in Milwaukee County charged with felony misconduct,” WPR (Nov. 11, 2025), <https://www.wpr.org/news/wisconsin-mayor-removal-police-chief-city-investigation-jay-johnson>.

Condor cameras are equipped with “people detection alerts” and “Guardian Mode” which automatically zooms in on people and vehicles and follows them through the frame.²⁵ Ultimately, a person walking through a park is not necessarily less surveilled just because the system is recording their body, clothing, vehicle or movements instead of recording their license plate. People should not have to prove that they are doing something wrong before they deserve to exist in public without unnecessary surveillance.

When placed at the entrances to county parks, these cameras can effectively create a government-accessible record of who came to a particular park on a particular day. That raises serious concerns for First Amendment rights. Earlier this month, reporting revealed that Flock taught law enforcement agencies how they could surveil No Kings protests using Flock’s technology and law enforcement’s own databases in a webinar.²⁶

Political organizations, religious communities, labor groups, LGBTQ+ organizations, activists, and other community groups regularly use public parks for rallies, demonstrations, meetings, festivals, and other events. A person should not have to choose between participating in public life and creating a permanent or searchable record of their vehicle’s presence at a political or religious gathering.

Consider a political rally held at a county park. An ALPR camera at the entrance could record every vehicle that arrived that day. Even if those individuals never committed a crime, law enforcement could potentially use that information to identify who attended the gathering, establish relationships between attendees, or investigate people’s movements before or after the event.

The risk is not limited to the people organizing an event. A vehicle entering a park can reveal sensitive associations: who someone spends time with, what communities they participate in, and which causes or organizations they support. People who use public parks generally have no meaningful ability to opt out. If someone wants to attend a public rally, meet a friend, exercise, or simply spend an afternoon in a county park, they cannot realistically avoid an ALPR camera placed at the only road into the park.

These concerns are particularly significant for people who depend on public spaces because they do not have private yards, private venues, or other places where they can safely gather. Communities that already experience heightened policing may also have greater reason to fear the creation of persistent government records documenting where they gather, socialize, worship, or organize.

And the technology is continuing to develop. A recent Yahoo Tech article²⁷ examined an experiment in which publicly available AI lip-reading software was able to reconstruct portions of conversations from silent camera footage when a person’s face was sufficiently visible. The article does not claim that Flock’s current ALPR cameras themselves routinely read people’s lips. But it illustrates a broader problem: footage collected for one purpose can become increasingly informative as AI tools continue to expand.

²⁵ “Surprise, Surprise: Flock Cameras Are Collecting More Than Just Your Plate and Car Information,” Jalopnik (July 18, 2026), <https://www.jalopnik.com/2217154/flock-cameras-collecting-more-than-plate-car-information/>.

²⁶ Flock Taught Cops How to Surveil No Kings Protesters, 404 Media (Sept. 3, 2026), <https://www.404media.co/flock-taught-cops-how-to-surveil-no-kings-protesters/>.

²⁷ “Flock Cameras Can Read Your Lips Under The Right Conditions,” Yahoo Tech (Sept. 21, 2026), <https://tech.yahoo.com/cybersecurity/articles/flock-cameras-read-lips-under-162330095.html>.

A Growing National Reconsideration of Flock

Policymakers are beginning to recognize that the boundaries between local surveillance and the Trump Administration are hard to maintain; if you collect data on your residents' comings and goings, it will be difficult to keep that from being used in unintended ways. As a result, over 240 jurisdictions across the have ended their relationship with Flock safety through cancelling or nonrenewing their contracts.²⁸ The following Wisconsin jurisdictions have ended their relationship with Flock in recent months:

- Appleton
- Ashland
- Chetek
- Clark County
- Cottage Grove
- Dane County
- De Pere
- Fitchburg
- Fond du Lac
- Fond du Lac County
- Fox Crossing
- Grand Chute
- Kenosha
- Kaukauna
- Lake Mills
- UW-Madison
- Manitowoc
- Marinette
- McFarland
- Menasha
- UW-Milwaukee
- Monona
- Neenah
- North Fond du Lac
- Oconomowoc
- Oneida County
- Oshkosh
- UW-Oshkosh
- Racine
- Racine County
- Ripon
- Sheboygan
- Stevens Point
- Stoughton
- Sturgeon Bay
- Sun Prairie
- Verona
- Waukesha
- Waupaca County
- Waupun
- Winneconne

We respectfully urge the committee to support this resolution. Milwaukee County should be able to enjoy our beautiful parks without assuming their presence is being added to an increasingly sophisticated AI-powered surveillance system run by a tech company that has already lost the trust of local governments and law enforcement agencies across the country.

²⁸ <https://ij.org/institute-for-justice-unveils-new-database-tracking-cancelations-of-license-plate-reader-contracts/>



**STATEMENT OF
CHAD A. MARLOW
SENIOR POLICY COUNSEL
AMERICAN CIVIL LIBERTIES UNION**

**For a Hearing on
“ALWAYS WATCHING: FLOCK’S NATIONWIDE AI SURVEILLANCE NETWORK”**

**Before the
UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND COUNTERTERRORISM**

September 23, 2026

Chairman Hawley, Ranking Member Durbin, and Members of the Senate Judiciary Subcommittee on Crime and Counterterrorism, on behalf of the American Civil Liberties Union (ACLU)¹, I want to thank you for the privilege of testifying before you today.

My name is Chad Marlow and for the past 12 years I have served as a Senior Policy Counsel at the ACLU where my work focuses on surveillance, privacy, and technology issues.² In this role, I lead the ACLU's policy and advocacy work on automatic license plate readers (ALPRs), including the ACLU's "Get The Flock Out" campaign.³

I want to begin my testimony by answering the question on the minds of every member of this committee and the American public. It is a question that reflects a concern shared by virtually every American, regardless of political party or philosophy. That question is simply, "How did a country founded on principles of liberty, personal freedom, and inalienable rights, including the right to privacy, find its people's vehicular locations and movements being tracked by governments at the local, state, and federal level even though virtually none of us are suspected of committing a crime?" Put more succinctly, "How did we get here?"

As you may already know, ALPRs are not new technology. They have been in use in the United States since the late 1990s.⁴ So why then in the last several years have we seen an explosion in the use of ALPRs and their tracking of innocent people? The answer is two-fold. The first is the entry of venture capital funding into the mass surveillance industry, including through ALPR companies like Flock Safety.⁵ Let me be clear: the injection of massive investment into the ALPR industry doesn't reflect a rise in venture capitalist interest in public safety. Rather, it reflects a view that ALPR use, if massively scaled up, could produce the type of windfall profits venture capitalists seek from their investments. But to achieve such returns, the ALPR industry needed to go bigger. Much bigger. And that means more ALPR deployment, more ALPR tracking, more ALPR data retention, more ALPR data sharing, and ultimately more ALPR company profits. In short, mass

¹ For 106 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend, preserve, and extend the individual rights and liberties that the Constitution and laws of the United States guarantee to everyone in this country. With millions of members, activists, and supporters nationwide, the ACLU is an organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C. to preserve American democracy and an open government for all its people.

² Chad Marlow, ACLU, <https://www.aclu.org/bios/chad-marlow>.

³ *Fight Creepy ALPR Cameras: Get the Flock Out!*, ACLU, <https://www.aclu.org/campaigns-initiatives/get-the-flock-out>.

⁴ Law Enforcement and Technology: Use of Automated License Plate Readers (2026), <https://www.congress.gov/crs-product/R48160>

⁵ See, e.g., *Accelerating Innovation: Flock Secures \$275 Million to Advance Crime-Solving Technology*, Flock Safety: Blog (Mar. 13, 2025), <https://www.flocksafety.com/blog/flock-safety-secures-major-funding>.

surveillance companies, like Flock and ALPR companies, trade our privacy for their profits, and the more they trade away, the richer they get.

The second cause of the spike in ALPR use is the advent of artificial intelligence (AI).⁶ While the massive deployment of ALPRs we are seeing in this country allows for the collection of an unimageable amount of private, personal vehicle location data, at some point, you create a data haystack so big, it becomes impossible to find the needle within it. Even an army of human data processors and reviewers could not get through the tens of billions of license plate scans our nation's ALPR companies produce every month. But with the advent of AI, going through such data and using it to identify drivers' intimate patterns of life has become light work. Identifying what doctors' offices, religious institutions, political meetings, or businesses a person frequents, and drawing conclusions about a person's private, personal behaviors from that data – or even using AI to generate flimsy criminal suspicion – went from being an impossible task to an easy, routine one.⁷ Want to formulate a strong guess as to whether a person is an immigrant or gun owner? No problem. Want to generate enough suspicion to justify going after a targeted person or group? Just ask the AI to identify something like the top ten vehicles that drove to a political event for Sen. Josh Hawley or Sen. Dick Durbin and who the AI thinks are the most likely to otherwise engage in some form of suspicious or disfavored activity, and bingo, the AI will gladly oblige. And because these ALPR products are most commonly sold to local police departments one at a time,⁸ funded by our taxpayer dollars, a nationwide mass surveillance ALPR network crept up on us slowly and silently until it finally became too big to not notice. In early 2022, the ACLU became the first organization to sound the alarm about this new, heightened risk, as embodied by Flock's ALPRs-on-steroids business model.⁹ The rest of America caught up a few years later, and now, here we are.

Today, the largest and most problematic ALPR vendor is that company, Flock, who by its own admission collects more than 20 billion license plate scans per month.¹⁰ That's about 57 scans per person in America every month, and that is just Flock – it is certainly billions more when you account for the other ALPR

⁶ Chris Hart & Ariel Chen, *Eyes on the Road: AI, Privacy, and Automated License Plate Readers*, 70 Boston B.J., Winter 2026, <https://bostonbar.org/journal/eyes-on-the-road-ai-privacy-and-automated-license-plate-readers/>.

⁷ Dhruv Mehrotra & Joseph Cox, *Hackers Got Inside a Flock Camera. Its Data Shows How the System Really Works*, Wired (Sept. 16, 2026), <https://www.wired.com/story/hackers-flock-camera-data-shows-how-system-works/>.

⁸ Henley Wing Chiu, *Companies That Use Flock Safety*, Bloomberg (last updated Jan. 25, 2026), <https://bloomberg.com/data/flock-safety/>.

⁹ Jay Stanley, *Fast-Growing Company flock is Building a New AI-Driven Mass-Surveillance System*, ACLU (March 3, 2022), https://www.aclu.org/wp-content/uploads/publications/flock_1.pdf.

¹⁰ *License Plate Cameras Scan 20 Billion Vehicles Monthly – Cities Are Canceling Contracts*, Gadget Rev. (June 30, 2026), <https://www.gadgetreview.com/license-plate-cameras-scan-20-billion-vehicles-monthly-cities-are-canceling-contracts>.

companies, which are nearly as bad as Flock and in some respects are worse.¹¹ These include ALPR companies like Axon and Motorola/Vigilant. If you think this all sounds like an Orwellian nightmare, you'd be right.

Beyond revealing people's intimate patterns of life and making it easy for government agencies to generate suspicion about persons and groups they wish to target or investigate¹² – including a system user's own love interests¹³ – the most concerning adverse impact of ALPR mass surveillance is that it can chill the exercise of people's rights and freedoms. This is why authoritarians love surveillance: in places like East Germany during the Cold War, and modern-day China and North Korea, the main benefit of mass surveillance isn't catching the few people who break the law, but rather is putting all their people in fear of stepping out of line with the government's interests in any way.¹⁴ That is the chilling effect.

And the argument that “if you're doing nothing wrong, you have nothing to fear” is baseless. Let me give you an example. Let's say a person is struggling with alcoholism and that person decides they want to go to an Alcoholics Anonymous meeting. Now, I think we can all agree that going to an AA meeting is not remotely wrong; in fact, it is very beneficial both for that person and for society as a whole. But if that person knows their local government uses ALPRs and that if they go to the local AA meeting, which is hosted by their local church every Tuesday night at 8 p.m., that the ALPR will track their car, identify their Tuesday evening driving location pattern, and be able to figure out – with the help of AI – that they are attending that nearby regular AA meeting and, therefore, are an alcoholic, then the person may not decide to go. They may not go because they do not want the government or anyone else figuring out they suffer from alcoholism. They may not want to risk their life insurance company, or auto insurance company, or health insurance company finding out and raising their rates. And so they do not go to AA, and that regretful but understandable decision hurts us all.

Now as everyone in this room well knows, in 2026, there is a well-worn narrative going around that America is so divided that we cannot agree on anything. Well, I beg to differ. On August 26, 2026, the two biggest anti-Flock,

¹¹ Jay Stanley, *Beware of Other License Plate Surveillance Companies Besides Flock*, ACLU (Aug. 26, 2026), <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/other-alpr-vendors>.

¹² Christopher Ingraham, *The IJ Database of ALPR Abuse*, Inst. for Just. (Aug. 12, 2026), <https://ij.org/the-ij-database-of-alpr-abuse/>.

¹³ Christopher Ingraham, *Police Have Reportedly Used License Plate Readers to Stalk Romantic Interests Dozens of Times in Recent Years*, Inst. for Just. (last updated Sept. 3, 2026), <https://ij.org/police-have-reportedly-used-license-plate-readers-to-stalk-romantic-interests-at-least-14-times-in-recent-years/>.

¹⁴ Lior Volinz, *Authoritarian Surveillance: An Introduction*, 23 *Surveillance & Soc'y* 112 (2025), <https://doi.org/10.24908/ss.v23i1.18975>.

anti-ALPR statements in the nation came from Florida Governor Ron DeSantis and Vermont Senator Bernie Sanders. Now I wouldn't say this is a sign that we have entered a post-partisan political nirvana, but that sure is something. In fact, Americans across the political spectrum have risen up against Flock, ALPRs, and mass surveillance with a passion and unity that is breathtaking.¹⁵

To be sure, their underlying motivations are not necessarily the same.¹⁶ Libertarians oppose ALPRs and mass surveillance because for them, standing against government intrusion into people's private lives is a bedrock principle. For MAGA adherents, mass government surveillance represents the worst of the Deep State. For more traditional conservative Republicans, mass surveillance flies in the face of their commitment to small government. Progressives oppose ALPRs and mass surveillance because they know that surveillance has always been disproportionately deployed against vulnerable and politically disfavored communities. And for centrists and the politically non-engaged, the idea of being tracked everywhere they go, even though they are not suspected of doing anything wrong, is highly offensive. But regardless of where their opposition stems from, all of these people are strongly united against Flock, ALPRs, and mass surveillance.

These united Americans have gone arm-in-arm to their local city councils and state legislatures to demand an end to ALPR-driven mass surveillance with incredible effectiveness: More than 200 localities have discontinued their relationships with Flock in the past 18 months,¹⁷ and in August 2026, Flock terminations reached a staggering rate of more than three per day.¹⁸

The false message Flock, Axon, Motorola and other mass surveillance companies like Ring and Palantir use to promote their products is that they are needed to keep Americans safe.¹⁹ That is a false narrative. As today's hearing is specifically about ALPRs, I will focus on the false public safety claims around that product in particular.

¹⁵ Laura J. Nelson & Kris Maher, *Red and Blue America Have Found Something to Agree on: Flock Cameras Must Go*, Wall St. J. (Sept. 18, 2026), <https://www.wsj.com/us-news/red-and-blue-america-have-found-something-to-agree-on-flock-cameras-must-go-765cd0b2>.

¹⁶ Adam Gramegna, *Americans of All Political Ideologies Unite for Privacy Against Flock Surveillance Cameras*, Military.com (July 24, 2026), <https://www.military.com/americans-political-ideologies-unite-privacy-against-flock-surveillance-cameras>.

¹⁷ Dan King, *Institute for Justice Unveils New Database Tracking Cancellations of License Plate Reader Contracts*, Inst. for Just. (Aug. 26, 2026), <https://ij.org/institute-for-justice-unveils-new-database-tracking-cancellations-of-license-plate-reader-contracts/>.

¹⁸ Cyrus Farivar, *Cities Terminate Flock Contracts at Record Pace in August*, Ars Technica (Aug. 29, 2026), <https://arstechnica.com/tech-policy/2026/08/cities-terminate-flock-contracts-at-record-pace-in-august/>.

¹⁹ E.g., Jacques Peretti, *Palantir: The "Special Ops" Tech Giant That Wields as Much Real-World Power as Google*, Guardian (July 30, 2017), <https://www.theguardian.com/world/2017/jul/30/palantir-peter-thiel-cia-data-crime-police>.

ALPR companies like Flock and Axon frequently claim that their products deter crime and help to catch criminals that would otherwise escape justice. . There is considerable evidence, however, to the contrary. The inability of surveillance to deter crime has been studied and reported on extensively.²⁰ In fact, the only situations in which surveillance has been found to deter crime is with respect to car thefts in public parking lots and, to a lesser degree, on public transportation.²¹ On some level, all of you all already know this. You know all those videos you see of people committing crimes online and on television? Well, if being watched deterred crime, those videos wouldn't be nearly as commonplace, would they?²² In fact, as we have learned from the many recent stories of people defacing and destroying Flock cameras around the country, surveillance technologies seemingly cannot even protect themselves.²³

As for the ability of ALPRs to help police close cases, a recent examination of FBI crime data for the City of Atlanta, Georgia showed that after the city rolled out the dual mass surveillance technologies of Ring doorbells and over 5,000 Flock ALPRs, there was no change in case closure rates.²⁴ Does that mean Flock ALPRs never find a stolen car or wanted person? No. What it means is that they would have been found anyway. So we are essentially trading away our privacy for nothing, other than to make Flock's wealthy investors even richer.

One prominent example of Flock falsely spinning a misleading suspect apprehension narrative to promote its product's efficacy comes from the tragic school shooting at Brown University and murder of an MIT professor in December 2025.²⁵ After Flock publicly claimed that its ALPRs helped identify the car of the shooter, Flock's Chief Legal Officer Dan Haley told NBC's Boston affiliate, "This is a tragic situation, and it's a perfect use case for the value of the technology."²⁶ But the

²⁰ See, e.g., Noam Biale, ACLU, Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found (2008), https://www.aclu.org/sites/default/files/asset_upload_file708_35775.pdf.

²¹ Does Video Surveillance Deter Crime?, Evidence-Based Living: Blog (Oct. 3, 2014), <https://evidencebasedlivinghuman.comell.edu/blog/does-video-surveillance-deter-crime/>.

²² Flock has recently tried to assert that ALPR use reduces vehicle thefts and increase police effectiveness based on a faulty, non-peer reviewed "working paper," the claims of which have been cast into significant doubt by the Institute for Justice in their paper titled "ALPRs and Vehicle Theft:

An Explainer of 'Working Paper: Automated License Plate Readers, Vehicle Theft, and Clearance.'" See Matthew West, Inst. for Just., ALPRs and Vehicle Theft: An Explainer of "Working Paper: Automated License Plate Readers, Vehicle Theft, and Clearance" (2026), <https://ij.org/wp-content/uploads/2026/09/ALPR-and-crime-study-external-explainer-V7.pdf>.

²³ Meg Anderson, *Amid Intense Backlash, People Are Vandalizing Flock Surveillance Cameras*, NPR (Aug. 21, 2026), <https://www.npr.org/2026/08/21/nx-s1-5931849/amid-intense-backlash-people-are-vandalizing-flock-surveillance-cameras>.

²⁴ Joe Wilkins, *Flock Surveillance Cameras Are Actually Horrible for Fighting Crime, FBI Data Shows*, Futurism (Aug. 1, 2026), <https://futurism.com/future-society/flock-surveillance-atlanta-fbi-data-crime-case-solve>.

²⁵ Francesca Regalado, *What We Know About the Shootings at Brown and M.I.T.*, N.Y. Times (Dec. 19, 2025), <https://www.nytimes.com/2025/12/19/us/brown-mit-shootings-what-we-know.html>.

²⁶ Briana Borghi, *How AI Played a Role in the Investigation into Shootings at Brown, MIT*, NBC Bos. (Dec. 19, 2025), <https://www.nbcboston.com/news/local/ai-brown-university-mit-investigation/3865328/>.

truth is that, shortly after the shootings occurred, the perpetrator was found dead in a New Hampshire storage unit of a self-inflicted gunshot wound.²⁷ This is Flock's modus operandi: it claims credit for results that would have been otherwise achieved without Flock's ALPRs and without undermining Americans' privacy.

In the end, what this shows is that while ALPRs may save police investigators a little time and effort, it does not help them close more cases. Americans across the nation have been very clear on this point: if it takes a little more time and effort to find a missing car or locate a suspect, but that means getting to keep our privacy, then so be it.

Flock, other ALPR mass surveillance companies, and their law enforcement proxies regularly promote ALPR use by stoking Americans' fears by presenting hypotheticals about law enforcement not being able to catch the most egregious criminals without their mass surveillance technology, but the American people are not fooled. We know that ALPRs and mass surveillance are not a public safety solution; they are a public safety threat.

Unfortunately, for those of you who might be interested in reviewing the fully independent audits of Flock's and other ALPR companies' efficacy claims, or of their claims that their internal security measures prevent the misuse of their systems and data, you won't find any, because Flock and the other ALPR companies do not permit such audits. While these companies do not care at all about protecting our personal data, they sure do a great job of protecting their own.

And just to quickly touch on a recent hot topic around ALPRs, while I fully acknowledge that the growing number of stories about police officer misuse of Flock are deeply disturbing, they should not become a distraction from the even larger issue; namely, that the greatest threat that comes from a mass surveillance ALPR system is not when it is misused, but when it is used as designed. The AI-empowered mass surveillance of every single American isn't an ALPR product defect – it is its most prominent and intended feature.

So just as I started this testimony with the question “how did we get here?”, I would like to conclude it by asking the question “where should we be going?”

But let's start with explaining where we should not be going.

²⁷ Kimberlee Knuesi et al., *Suspect in Brown University Shooting and MIT Professor's Killing Found Dead, Officials Say*, AP News (Dec. 18, 2025), <https://apnews.com/article/brown-university-shooting-investigation-5b0b254442dd77d9056111bad902dc33>.

The ALPR companies will likely suggest, as most big technology industries do, that they should be permitted to self-regulate, or that loose guardrails that preserve their massive profit and growth models are sufficient to protect Americans' privacy, but we know that won't work. Recent operational changes rolled out by Flock are simply retreads of easily circumventable security measures that had previously failed, and a reduced default data retention period that can will gladly be circumvented upon request.²⁸ In the end, Flock views legitimate privacy concerns as mere PR problems and has sought to mislead the public to get around them. They repeatedly mislead²⁹ to the public and to journalists. They mislead to their own potential customers, be they city councils, state legislatures, or police departments. They even lied about partnering with the ACLU to pass legislation and help design their ALPR system, which I assure you couldn't be further from the truth. Flock's competition, like Axon and Motorola/Vigilant, have adopted the tactic of staying quiet in public, letting Flock fall on its own sword, perhaps hoping after Flock goes out of business, they will sweep up its contracts and profits.³⁰ These companies have done nothing to earn the public's or the U.S. Senate's trust or confidence.

The ALPR companies may also argue that we should just let the courts solve this issue, and they will claim – as they have repeatedly in the past – that where courts have previously weighed in, many held that ALPR use does not violate the Constitution. But this claim is based on outdated case law. In June 2026, the U.S. Supreme Court handed down a decision in *Chatrie v. US*³¹ that raised the very real possibility that mass ALPR surveillance of people's locations without a warrant violates the Fourth Amendment, because even small amounts of location data can reveal very private, personal details about a person's life.

Courts may take years to reach a final decision on this issue, and the U.S. Congress has no obligation to wait for them to do so when all Americans' privacy is a stake. Just as the Constitution creates a rights floor, legislatures, like the U.S. Congress, can raise that floor to establish even greater protections. That is

²⁸ Chad Marlow, *Despite "New" Updates, Flock's Creepy Cameras Remain Major Civil Liberties Threat*, ACLU (Aug. 13, 2026), <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/despite-new-updates-flocks-creepy-cameras-remain-major-civil-liberties-threat>.

²⁹ Chad Marlow & Jay Stanley, *Flock Safety Credibility Lost as It Repeatedly Lies to City Councils, Police Departments, and Public Across the Country*, ACLU (July 2, 2026), <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>.

³⁰ Al Landes, *Cities Ditching Flock Safety Cameras*, Yahoo News (Sept. 18, 2026), <https://www.yahoo.com/news/us/articles/cities-ditching-flock-safety-cameras-172924943.html>.

³¹ 609 U.S. ____ (2026).

precisely what many local and state legislatures have done, and what the Congress should do.

It is well past time Congress tells Flock to Get The Flock Out of our communities. But Congress needs to do more than just take on Flock. This national movement is not just about Flock and never has been. It's about all ALPRs.³² Regretfully, this point has been missed by some cities like Denver, Colorado, where the city cancelled its Flock ALPR contract and immediately signed a contract with Axon. Residents shouldn't be relieved by this change. They should be outraged, and many of them are.

The time has come for Congress to ban any law enforcement entity who receives federal funding from using ALPRs. And this prohibition should be without exceptions. As I suspect this Subcommittee already knows that, when it comes to protecting core American civil rights and civil liberties, if you make one exception, you invite others, and that is a slippery slope we must avoid at all costs. Some states are already showing us the way. Florida has banned the use of ALPRs on all state highways. Texas halted all funding for ALPRs and paused the installation of ALPRs statewide. And Vermont, effective July 1, 2027, will be the first state to ban the use of ALPRs altogether. This is the way. It's time for Congress to use its power of the purse to prohibit the government use of ALPRs in America.

I want to leave you all with one final thought. The ACLU and the American people are deeply grateful for the work of this subcommittee, and for the bipartisan leadership of its Chair and Ranking Member. We are counting on all of you to say no to Flock and to all privacy-undermining ALPRs, regardless of the company that sells or operates them. But your work must not stop there. Americans' objection to ALPRs is, at its core, an objection to mass surveillance. If governments stop tracking our cars with ALPRs and start tracking all of our faces using surveillance cameras and facial recognition technology, things will be even worse, not better. We will have accomplished nothing. That means that this body, when it finishes its immediate work on ALPRs, must turn to combatting the surveillance industrial complex that is threatening the freedom and liberty of every American every day. That means taking action to prohibit government entities from circumventing the Fourth Amendment by buying personal data from data brokers, to prohibit them from using dragnet reverse warrants, which can identify unlimited numbers of people without criminal suspicion based on their location or the words they type into internet search engines, to stand up to EdTech Surveillance companies that rob

³² And, indeed, all government mass surveillance.

our schools of their limited financial resources by falsely claiming they need to spy on our children to keep them safe, and to rein in the corporations that sell facial recognition technology, cell site simulators, AI empowered surveillance cameras, as well as companies like Palantir that seek to generate, collect, and combine our personal data so they can enable their customers to track all of us and make dangerous predictions about who among us presents a threat – an ironic goal given that it is these companies, themselves, that are the actual threat.

So I implore you, members of the U.S. Senate, to be brave and unrelenting in responding to these mass surveillance threats; and please know, with absolute confidence, that the ACLU and the American people stand with you.

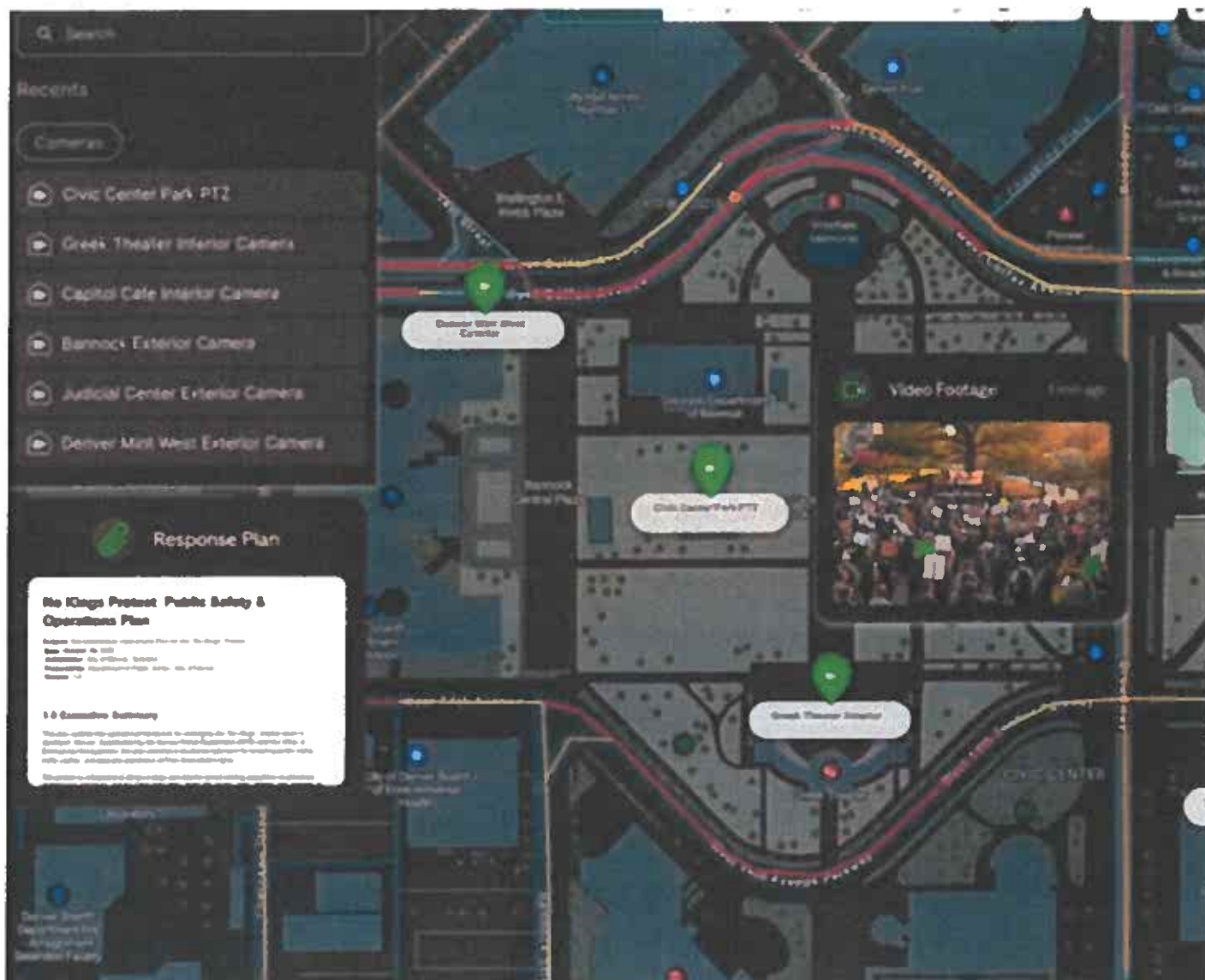
Thank you again for the opportunity to testify today. I look forward to answering your questions.

Flock Taught Cops How to Surveil No Kings Protesters

404media.co/flock-taught-cops-how-to-surveil-no-kings-protesters

Jason Koebler

September 3, 2026



Flock taught cops how they could surveil the No Kings protests and “small parades” using a mix of Flock’s technology and law enforcement’s own databases in a webinar last year. As Flock publicly downplays the power of its automated license plate camera network and highlights its use to solve violent crime, the company’s seemingly endless trove of webinars, training sessions, and blog posts show it offers far more invasive capabilities.

[In the webinar](#), Flock’s director of market management Caity Peak explains how real time crime centers — which are police surveillance centers that utilize Flock cameras and other surveillance cameras — can be used for emergency response, but can also be used to surveil “established events” like 4th of July fireworks displays, parades, bike races, Mardi Gras, and protests. The

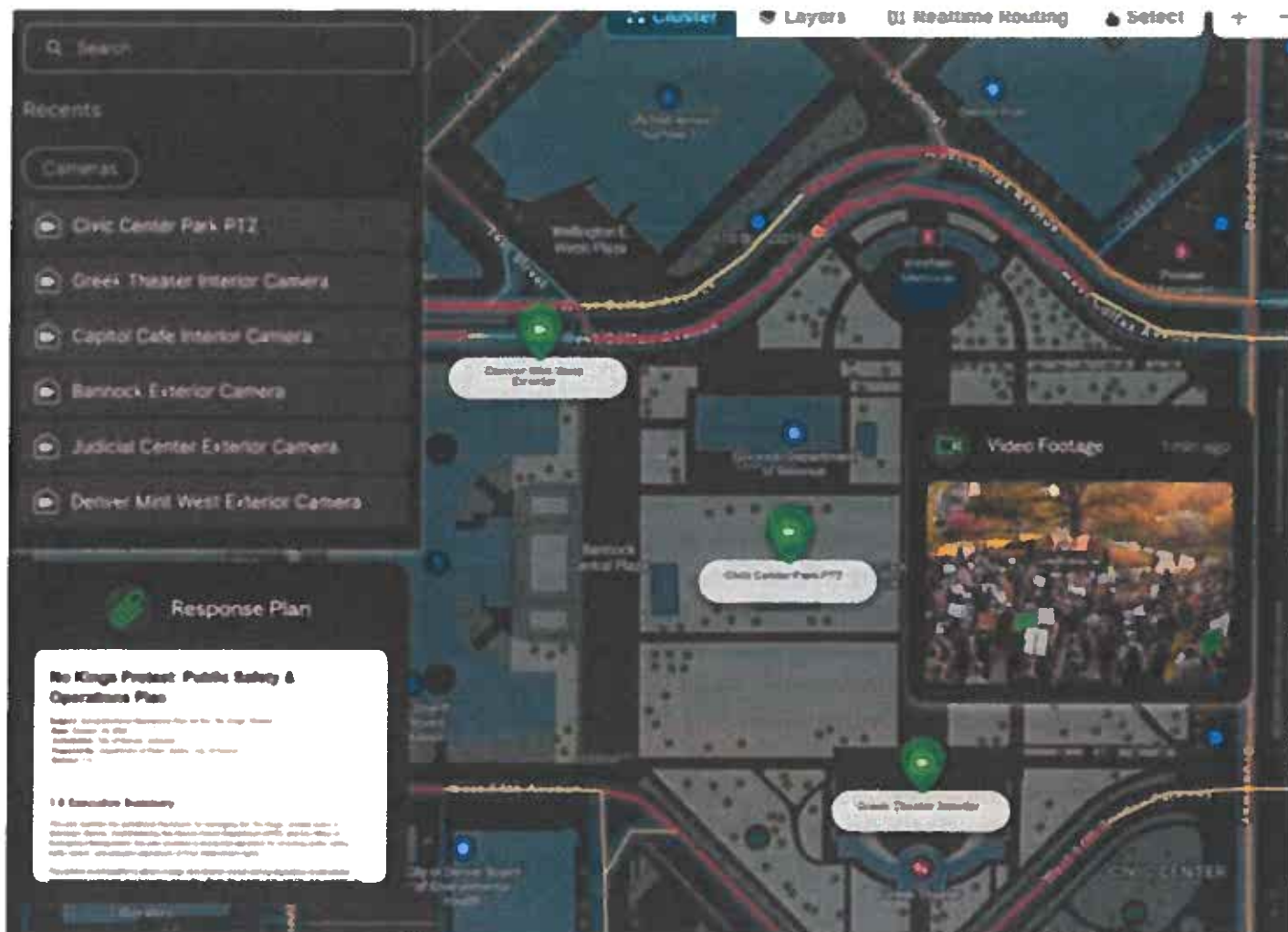
webinar shows just how routine the idea of always-on surveillance has become, and how casually it is used during extremely innocuous events.

Peak explains that [police can use FlockOS](#), a software platform that combines Flock's automatic license plate readers (ALPR), drones, gunshot detectors, 911 data, and other surveillance cameras (including ones Flock does not own) into a "single pane of glass" or single piece of software to look at various types of surveillance in one place during both emergencies and relatively mundane events in a city or town.

0:00

/3:47

"Imagine that you're an incident commander, and you're working this No Kings Protest," Peak explains while a dashboard shows a series of surveillance tools overlaying the city of Denver. "If I'm somebody assigned a traffic post that's working this No Kings Protest, I really don't have time to go in [...] and look at all these places [for different intelligence]. This is an example of viewing all of that in one place. I'm an officer, I can see the response plan that's included, I can pull that up if I need it, but I can also see live video footage as that protest moves throughout the park."



Peak says the surveillance footage can be used to monitor the protests without having cops physically on the ground “making it worse, getting attention.”

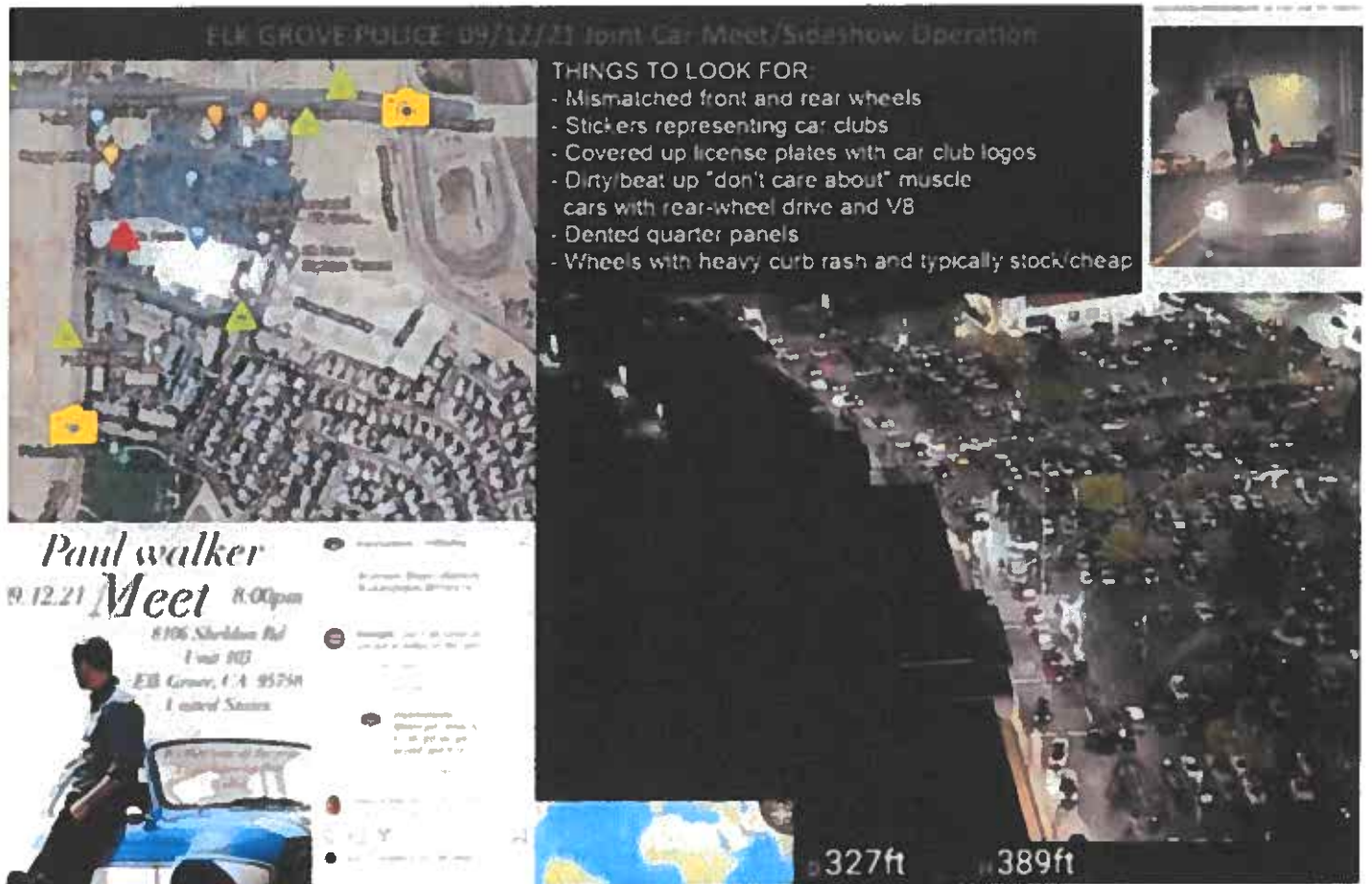
“I’ve got the video footage to monitor when things go sideways, I know when the environment is starting to shift. But I also know a lot of other things as well. I can see traffic flow, so as people are blocking the roadway, maybe that’s OK for a while, but if I see that traffic has been stopped a while, I may need to send officers to that area because I know that road rage is imminent,” she continues. The dashboard Peak shows includes traffic information, a “response plan” for the protest, the floor plans of nearby buildings, as well as a series of video feeds of both outdoor-mounted cameras and cameras inside businesses and government buildings.

404 Media and the [Electronic Frontier Foundation previously showed](#) that police have specifically used [Flock cameras to monitor the No Kings protests](#) and other First Amendment-protected activity. [404 Media found](#) California cops used Flock to monitor an “immigration protest.” The EFF found that the following law enforcement agencies ran Flock searches related to No Kings protests and rallies:

Law Enforcement Agencies that Ran Searches Corresponding with "No Kings" Rallies

- Anaheim Police Department, Calif.
- Arizona Department of Public Safety
- Beaumont Police Department, Texas
- Charleston Police Department, SC
- Flagler County Sheriff's Office, Fla.
- Georgia State Patrol
- Lisle Police Department, Ill.
- Little Rock Police Department, Ark.
- Marion Police Department, Ohio
- Morristown Police Department, Tenn.
- Oro Valley Police Department, Ariz.
- Putnam County Sheriff's Office, Tenn.
- Richmond Police Department, Va.
- Riverside County Sheriff's Office, Calif.
- Salinas Police Department, Calif.
- San Bernardino County Sheriff's Office, Calif.
- Spartanburg Police Department, SC
- Tempe Police Department, Ariz.
- Tulsa Police Department, Okla.
- US Border Patrol

This webinar shows this type of surveillance is not anomalous, and is specifically taught by Flock. The webinar also shows that Flock's latest public stance — that its ALPR cameras are noninvasive technology, that they take only static images at a single place and time, and that they are primarily used to solve the worst crimes — is wildly misleading. Flock has time and time again pitched itself to police as a sort of operating system to solve crime and do real-time surveillance and predictive policing. ALPRs are just one part of this broader surveillance apparatus that Flock has created, markets to police, and teaches them how to use. These real time crime centers are proving increasingly popular with police; Flock now says on its website that more than 4,800 cities around the country [are running FlockOS software](#).



AI-Powered Video: Search and Alerts



One search. Every system. Faster suspect workups.

Peak goes on to give another example, in which police would surveil a car sideshow near Sacramento using a mix of drones, surveillance cameras, ALPRs, and monitoring of social media posts. “We knew it was likely to turn into nefarious activity based on who was promoting the car show,” she says. A list of “THINGS TO LOOK FOR” include “mismatched front and rear wheels, stickers representing car clubs, and covered up license plates with car club logos.” Peak then demos [Flock’s free-form search](#), which is “AI-powered video search and alerts.”

One then explains how Flock Note, the company's deeper investigative tool, can be used to identify

LPR information with “all of your agency data,” which in this example includes “person data, IP data, email data, sex offender data, license plate data, vehicle data, and OSINT [open source intelligence].” A screenshot of the Flock system shows a “street racing suspect” complete with the man’s name, address, email, social media accounts, phone number, and various affiliations.

“It works like a Google Search,” she says, imagining a scenario in which cops pull someone over then use Nova. “I run him through Nova. I can query CAD [computer aided dispatch], RMS [records management system], OSINT, jail records. All these things we have integrated to see that we have contacted him before for sideshows, he has been contacted for spinning cars in an intersection in the last 90 days, he is related to this car club, and now with that information, I have the justification I need to actually tow the car for 90 days instead of just issuing a citation.”

Bourbon Street Attack

Tactical Support & Aftermath

Officer Safety
Provided real-time officer safety alerts



Timeline of Events
Constructed a timeline of the suspect's movements from the time he entered New Orleans through the execution of the attack, to include placing IEDs along Bourbon Street

Evidence Collection
Officer-Involved Shooting with suspect was captured on a RTCC-accessed camera

Information Sharing
Coordinated intelligence fusion with state and federal agencies; Images from RTCC were shared publicly by the FBI

Later in the webinar, police from New Orleans and Flock representatives spoke about how its system was used by police in the aftermath of the Bourbon Street terror attack that killed 14 people on Jan. 1, 2025 and during the Super Bowl and Mardi Gras that year. The webinar highlights how this tech is used after a crime, and how the data often filters across agencies. Ross Bourgeois, who runs New Orleans' real time crime center, says that the city used a "tremendous amount of cameras in a very short time" to recreate the terrorist's movements.

“We were able to use our network of cameras and license plate readers to map out what he did when he entered the city a day or two before the event, up until he executed the event and engaged the police and our shooting situation at the conclusion of it,” Flock’s Patin said, adding

that footage running through FlockOS were eventually shared with the Department of Homeland Security, federal fusion centers, and the FBI. "7 terabytes of information, which was a lot of data, and we were able to share that with our fusion center and our federal partners. Homeland Security, HSI [Homeland Security Investigations, a division of Immigration and Customs Enforcement], and FBI."

United States Senate

WASHINGTON, DC 20510-2509

JUDICIARY
HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS
HEALTH, EDUCATION, LABOR,
AND PENSIONS
SMALL BUSINESS
AND ENTREPRENEURSHIP

August 26, 2026

Garrett Langley
Chief Executive Officer
Flock Safety
3284 Northside Parkway NW
Atlanta, GA 30327

Dear Mr. Langley:

As Chairman of the Senate Judiciary Subcommittee on Crime and Counterterrorism, I am investigating Flock Safety's collection, retention, and dissemination of the data generated by its artificial intelligence surveillance cameras.

In a few short years, Flock has assembled an unprecedented national surveillance network. Your company boasts more than 120,000 cameras across 49 states and more than 20 billion vehicle scans every month.¹ The overwhelming majority of the Americans captured in those records did nothing wrong. Instead of serving discrete local investigations, as contemplated by our constitutional processes and safeguards, these camera networks harness artificial intelligence to pool what they capture into a national database that customers can search.²

Recent examples of abuse and misuse of personal data reveal the woeful lack of safeguards in these systems. In Missouri, the St. Charles County Police Department terminated its contract this month after an audit revealed that a civilian employee had run Flock searches for personal reasons, completely unrelated to their law enforcement duties.³ Sadly, my home state is not an outlier. In Milwaukee, prosecutors charged a police officer who allegedly searched his girlfriend's license plate 124 times and her former boyfriend's plate 55 times, entering "investigation" as his justification each time. Worse still, the officer was not caught by the company's audit systems—he was caught because a private citizen looked up his own plate on a public website.⁴

Errors and false positives add insult to injury. A Florida woman spent 13 days in jail and faced eight felony counts, including three counts of vehicular homicide, after investigators arrested an owner based on their search of Flock's network for a vehicle description. Prosecutors dismissed the charges seven months later when law enforcement discovered the error and arrested a different person.⁵ One California police department found that a staggering 71% of its alerts were wrong, and the Los Angeles Police Department dropped its Flock contract after an audit showed officers had stopped 161 vehicles incorrectly flagged as stolen in the space of two months.⁶

¹ <https://www.flocksafety.com/blog/the-price-of-free-lpr>

² <https://www.wired.com/story/flock-safety-os-investigate/>

³ <https://www.ksur.org/news/2026-08-23/flock-cameras-misuse-missouri-st-charles-county-police>

⁴ <https://reason.com/2026/08/13/flock-cameras-and-license-plate-readers-are-everywhere-can-we-trust-cops-with-them/>

⁵ <https://www.yahoo.com/news/us/articles/florida-woman-spent-13-days-170100471.html>

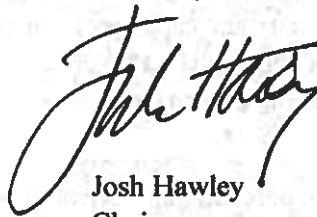
⁶ <https://reason.com/2026/08/13/flock-cameras-and-license-plate-readers-are-everywhere-can-we-trust-cops-with-them/>

Furthermore, once cameras collect driver data, uncertainty abounds in how your company and its customers can sell or use data. Flock's \$8.3 billion valuation comes with enormous pressure to find new commercial applications. Americans demand a full accounting for how their driver data is stored or sold.⁷

To be sure, I want law enforcement to have tools to catch offenders and keep the public safe. But Americans do not surrender their privacy rights when they drive to work, drop their kids off at school, or go to church. The Supreme Court has recognized that a comprehensive, retrospective record of a person's movements is different in kind from ordinary observation in public.⁸ Congress never authorized the network your industry has built. Your company's internal policies are, in practice, the only safeguards for hundreds of millions of Americans. People across the country are now discovering that fact and demanding answers from their elected officials.

In light of this abuse of driver information, the American people want to know who has access to their personal data and how. This investigation will seek those answers. To facilitate that, please produce all documents and information specified in the attached annex no later than **September 8, 2026**. If you have questions about the scope of these requests, please contact my office to discuss.

Sincerely,

A handwritten signature in black ink, appearing to read "Josh Hawley", written in a cursive style.

Josh Hawley
Chairman
Subcommittee on Crime and Counterterrorism
Committee on the Judiciary

⁷ <https://fortune.com/2026/08/24/flock-8-billion-startup-backed-al6z-tiger-surveillance-camera>

⁸ See *Carpenter v. United States*, 585 U.S. 296, 309-10 (2018).

ANNEX

DEFINITIONS

1. **“Document”** means any recorded information in any format, medium, or form, whether written, printed, typed, electronically stored, photographed, filmed, or otherwise preserved, including: emails, text messages, ephemeral messages (e.g., Signal, Telegram, etc.), Slack, Microsoft Teams, Discord, any internal Flock messaging platform, instant messages, source code, application logs, moderation logs, user-report records, dashboards, slide presentations, spreadsheets, financial models, board minutes, board packages, audit reports, legal memoranda, contracts, agreements, regulatory correspondence, engineering specifications, product roadmaps, and design documents, in final and draft form, wherever they may be.
2. **“Flock” or “Company”** means Flock Group, Inc., d/b/a Flock Safety, together with each of its predecessors, successors, parents, subsidiaries, divisions, affiliates, joint ventures, and any entity in which it holds a controlling interest, whether foreign or domestic; each of its present and former officers, directors, employees, contractors, consultants, agents, attorneys, and representatives acting on its behalf; each entity operating under a trade name or product name used by the Company, including but not limited to Flock Safety, Flock OS, Flock Nova, Falcon, Sparrow, Raven, Condor, and Aerodome; and any other person or entity acting for or on behalf of any of these entities. Where a request concerns documents or information in Flock’s possession, custody, or control, that phrase includes documents and information held by any third party from which Flock has the practical ability to obtain them, including cloud service providers and any entity that hosts, processes, or stores data on Flock’s behalf.
3. **“Relevant Period”** means January 1, 2021, through the present, unless a specific request states otherwise.

INTERROGATORIES

Please answer each of the following in writing. If Flock declines to answer any question in whole or in part, state the basis for that refusal. If Flock lacks information sufficient to answer, describe the efforts undertaken to obtain it.

1. State the parameters under which your customers can conduct a statewide or nationwide search of vehicle or driver data, as well as whether those features are enabled by default.
2. State the default retention period for each category of data Flock collects, and identify every change to that default since January 1, 2021, including the date of each change and the reason for it. State the maximum period a customer may select, whether Flock approval is required to exceed the default, and how many customers currently retain data beyond the default.
3. State the total number of confirmed instances of misuse of Flock systems or data known to Flock, by year, since January 1, 2021. For each, state whether the misuse was first identified by Flock’s own monitoring, by the customer, or by a third party.
4. Describe what a user must enter to justify a search. State whether that entry is validated against any external record, whether a supervisor must approve it, and whether a search proceeds if the field is left blank or filled with generic text such as “investigation.”

5. Describe every restriction Flock imposes on the purposes for which its systems may be searched. State whether Flock has assessed whether those restrictions can be circumvented and, if so, the result of that assessment.
6. State Flock's measured accuracy at the level of a complete and correctly attributed vehicle identification. Identify the testing that produced that figure and state the rate at which alerts are later determined to be incorrect.
7. Identify every category of data that Flock's deployed devices capture, including still images, video, audio, wireless signals, and any biometric identifier. For each, state the date on which Flock began capturing it and whether customers may decline.
8. State whether Flock links data captured by its devices to any external data source, and identify each such source, including commercial data brokers and public records aggregators. State whether Flock has ever ingested, licensed, evaluated, or tested data obtained from a security breach.
9. State whether multi-factor authentication is required of all users and, if it has not always been required, when it became mandatory.
10. Describe in detail whether Flock has the capability to biometrically track individuals and explain what physical or technical limitations exist or are imposed on such biometric tracking.

DOCUMENT REQUESTS

1. All policies, procedures, and training materials governing the process by which a law enforcement agency or other entity obtains access to Flock's systems or data, including any vetting, accreditation, written policy, supervisory, or training prerequisites, and all documents concerning the waiver of any such prerequisite.
2. All documents concerning the siting of cameras and sensors, and all documents concerning notice to or approval by local governing bodies or the public before installation, including model ordinances, public-notice templates, signage specifications, and communications with local officials regarding whether public approval is required.
3. All policies and technical documentation concerning when Flock devices record or transmit data, whether recording can be suspended or disabled, who may do so, and whether any such change is logged.
4. All data retention schedules and policies, including default retention periods, the extent to which customers may extend or shorten them, the treatment of backups and of derived data such as vehicle fingerprints or model embeddings, procedures for verifying deletion, and the disposition of data upon termination of a contract.
5. All policies and technical documentation governing who may query Flock's systems and the default geographic scope of a query, together with all documents concerning the sharing of data with other law enforcement agencies, federal agencies, foreign governments, private entities, or data brokers.
6. All policies and technical documentation governing the justification a user must supply to run a search, including whether that field is validated or free text, whether a warrant or supervisory approval is required for any category of search, and a description of every audit capability available

to customers and to Flock, including whether audit records are complete, immutable, and exportable.

7. All documents concerning any known or suspected misuse of Flock systems or data from January 1, 2021 to the present, including internal investigations, audit findings, notifications to customers, notifications to affected individuals, referrals to law enforcement, and any resulting change in policy or product design.
8. All documents concerning the accuracy of Flock's products, including internal and third-party testing of character-level and plate-level read accuracy, false-positive rates for alerts, confidence thresholds and how they are displayed to users, representations made to customers or the public about accuracy, and all documents concerning any stop, detention, or arrest of an individual later determined to have been misidentified.
9. All documents concerning the security of Flock's systems, including multi-factor authentication requirements, credential compromise, unauthorized access or exposure of camera feeds or stored data, penetration testing and remediation, the location and ownership of data storage infrastructure, and access to production systems by personnel or contractors located outside the United States.
10. All contracts, master service agreements, terms of service, data-processing agreements, and end-user license agreements executed with any governmental customer, together with all price lists, fee schedules, and documents concerning pilot programs, discounted or donated equipment, and any assistance Flock has provided to customers in obtaining federal, state, or private grant funding.
11. All documents concerning categories of data other than license plate images that Flock collects, ingests, licenses, or links to its camera data, including audio, video, facial or other biometric identifiers, commercial data-broker records, public records, and any data derived from a breach; and all documents concerning the use of customer or third-party data to train Flock's models.
12. All documents concerning Flock's sources of revenue and capital, including investors holding more than five percent of any class of equity, revenue derived from federal, state, and local government funds, the federal grant programs through which customers have financed purchases, lobbying expenditures, and political contributions.

1. The first part of the report is a general introduction to the subject.

2. The second part of the report is a detailed description of the method used.

3. The third part of the report is a discussion of the results obtained.

4. The fourth part of the report is a conclusion and a list of references.

5. The fifth part of the report is a list of figures and tables.

6. The sixth part of the report is a list of symbols and abbreviations.

7. The seventh part of the report is a list of footnotes.

8. The eighth part of the report is a list of appendices.

9. The ninth part of the report is a list of references.

10. The tenth part of the report is a list of symbols and abbreviations.

11. The eleventh part of the report is a list of footnotes.

12. The twelfth part of the report is a list of appendices.

13. The thirteenth part of the report is a list of references.

14. The fourteenth part of the report is a list of symbols and abbreviations.

15. The fifteenth part of the report is a list of footnotes.

16. The sixteenth part of the report is a list of appendices.

17. The seventeenth part of the report is a list of references.

18. The eighteenth part of the report is a list of symbols and abbreviations.

19. The nineteenth part of the report is a list of footnotes.

20. The twentieth part of the report is a list of appendices.

United States Senate

WASHINGTON, DC 20510

September 16, 2026

Garrett Langley
Chief Executive Officer
Flock Group, Inc.
3284 Northside Parkway
Atlanta, GA 30327

Dear Mr. Langley:

We write seeking information regarding allegations of potential abuse of Flock's surveillance platforms and whether your existing protocols protect Americans' privacy. Despite a professed public commitment to responsible governance, Flock has repeatedly failed to implement the safeguards necessary to protect Americans' civil liberties.

In the last two years, there have been increasingly troubling, documented reports of law enforcement officials abusing Flock's nationwide license plate readers, camera network, and sensors to carry out extensive, unauthorized surveillance. In 2025, investigative reporting uncovered that a deputy in Johnson County, Texas accessed Flock cameras to track a woman by falsely claiming the case was about a "missing person," when in fact the woman's husband reported her to police for attempting to access reproductive health care.¹ Since then, multiple organizations have come forward to express concern that states restricting reproductive health care access are using Flock data to track down patients traveling to other states for care.²

Numerous reports also indicate Immigration and Customs Enforcement (ICE) officials are conducting immigration-related searches of Flock databases to pursue individuals without warrants.³ While Flock claims to "not work with ICE,"⁴ and blames local customers who share information voluntarily with federal authorities for these searches,⁵ Flock has repeatedly failed to prevent ICE officials from accessing its data.⁶ In one instance, Kansas police went so far as to

¹ Jason Koebler & Joseph Coz, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 MEDIA (May 29, 2025), <https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/>; see also Dave Maass & Rindala Alajaji, *Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation*, ELECTRONIC FRONTIER FOUNDATION (Oct. 7, 2025), <https://www EFF.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it>.

² See, e.g., *Our testimony: Remove Flock cameras from Ohio*, ABORTION FORWARD: BLOG (Aug. 10, 2026), <https://abortionforward.org/blog/our-testimony-remove-flock-cameras-from-ohio/>.

³ Koebler & Coz, *supra* note 2.

⁴ *Does Flock Share Data with ICE*, FLOCK (Jan. 6, 2026), <https://www.flocksafety.com/blog/does-flock-share-data-with-ice>.

⁵ See *Id.* (Indicating if a Flock customer chooses to share information with federal authorities "Flock has no ability to change that decision.")

⁶ Koebler & Cox, *supra* note 2.

use Flock data to target a man who wrote an op-ed criticizing the department's role in a local ICE operation.⁷ An analysis of police and court reports by the *Washington Post* revealed that at least 50 law enforcement officers have been charged or accused of misusing Flock's surveillance system for unauthorized purposes.⁸

Despite these alarming developments, Flock continues to expand its network and collaborations with other data-sharing entities. A leaked corporate presentation reveals that Flock plans to partner with Nexar, a dashcam producer, to collect data from roughly 350,000 devices installed in rideshare vehicles.⁹ Nexar is currently in negotiations with AI company, Nauto, to create an "intelligence engine" of a scale "that no simulation and no single company's dataset can match."¹⁰ Flock and Nexar's proposal to collect and disseminate data from hundreds of thousands of consumer and rideshare dashcams risks creating an expansive, pervasive surveillance network that lacks adequate consumer consent, transparency, or accountability.

We understand that, in response to the recent public outcry against its products, Flock published a series of updates to its privacy standards.¹¹ Unfortunately, these changes still leave many important questions unanswered. For example, although Flock shortened the default data retention timeline from 30 days to 7 days, it introduced a feature called, "Evidence Mode," which allows detectives to "preserve specific [Automated License Plate] ALR data as evidence for an active investigation in cold storage."¹² Flock failed to explain how it plans to prevent misuse of this feature or what constitutes an active investigation. Flock also purported to add another capability, titled "offense filtering for sharing," which would allow Flock users to limit searches of their data by outside agencies to certain types of offenses. However, a similar filtering requirement implemented in June 2025 failed to stop officers from querying restricted data using nonsensical, frivolous words to bypass the filtering system, including inputting the phrase "hehehe" to ostensibly circumvent prohibited search terms, instead of listing the actual terms they intended to search for.¹³ Clearly, this attempted corrective action was insufficient. Flock also updated its features to require law enforcement customers to adopt a program that

7 Jay Stanley, *Kansas Town Uses License Plate Readers to Go After Man Who Wrote Op-Ed*, ACLU (Feb. 3, 2026), <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/alpr-against-op-ed-writer>.

8 Drew Harwell, Douglas MacMillan & Aaron Schaffer, *How Rogue Officers Turned A Nationwide Camera Network Into A Tool For Stalking*, WASH. POST (Aug. 2, 2026), <https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>.

9 Joseph Cox, *Flock Pitched a Plan To Turn Uber and Lyft Drivers Into Roaming Surveillance Vehicles*, 404MEDIA (Aug. 7, 2026), <https://www.404media.co/flock-pitched-a-plan-to-turn-uber-and-lyft-drivers-into-roaming-surveillance-vehicles/>.

10 Nexar and Nauto to Merge, *Creating the Independent Infrastructure Platform for Physical AI*, PR NEWswire (Jul. 1, 2026), <https://www.prnewswire.com/news-releases/nexar-and-nauto-to-merge-creating-the-independent-infrastructure-platform-for-physical-ai-302815865.html>.

11 Garrett Langley, *Flock Updates Privacy, Accountability, Security and Transparency Safeguards*, FLOCK (Aug. 13, 2026), <https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency>.

12 *Id.*

automatically flags abnormal activity for administrator review. What qualifies as abnormal activity remains undefined. Furthermore, it is unclear whether Flock will also require those customers to adopt its “proactive lockout” feature, which would automatically suspend accounts exhibiting abnormal behavior.

Flock claims to have the tools to protect the American people from further abuses of its platform. It must use them. As part of our legislative oversight to protect and preserve Americans’ privacy and civil liberties, we request responses to the following questions no later than September 25, 2026:

1. Flock is currently subject to a patchwork of ordinances from cities, counties, and states across the country, how is Flock operating in that type of patchwork environment?
 - a. Does Flock track if and when its technology is not compliant with any local ordinances or state laws?
 - b. Does Flock request data on whether its technology violates any local ordinances or state laws?
2. When will Flock mandate its “proactive lockout” feature for law enforcement partners?
3. What additional safeguards has Flock included in its “offense filtering for sharing” feature to protect against misuse?
 - a. What additional safeguards has Flock implemented to prevent law enforcement officials from querying sensitive information using pretextual justifications?
 - b. Why did Flock choose to restrict transparency by switching to a generic dropdown menu rather than implementing stricter auditing of free-text entries? Furthermore, how does a pre-populated list prevent an officer from simply clicking a false, pretextual category to bypass oversight?
 - c. Does Flock plan to periodically review whether its law enforcement customers are compliant with its safeguards?
4. What specific safeguards has Flock deployed, placed in development, or evaluated to prevent system misuse of any kind? Please detail how each safeguard operates in practice, the rollout timeline for in-progress features, and the explicit reasons why any considered safeguards were rejected.

13 Chad Marlow & Jay Stanley, *Flock Safety Credibility Lost as it Repeatedly Lies to City Councils, Police Departments, and Public Across the Country*, ACLU (July 2, 2026), <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> (“In September 2025 alone, a local Oregon police department was allowed to search Flock’s ALPR system after entering “investigation” into the search reason field 111 times and “hehehe” into the field on 20 occasions. . .”).

- a. Does Flock support or plan to support hardware authenticators, such as security keys or smart cards, to prevent sharing credentials and ensure every system action is tied to a single verified individual?
 - b. Does Flock support or plan to support restricting system access so that searches are blocked unless the user is actively on duty, within an authorized location, and within an authorized time window?
 - c. Does Flock support or plan to support mandatory two-person sign-off to approve searches?
5. What corrective action does Flock plan to take to ensure that women seeking reproductive health care in states that protect access to reproductive health care do not have their data tracked by Flock Automatic License Plate Readers (ALPRs)?
6. How is Flock ensuring that it is compliant with California's privacy laws?
 - a. What are the error rates for Flock's data captures?
 - b. What accountability and transparency policies does Flock have for error rates?
 - c. Has Flock conducted a legal analysis of California's privacy law in relation to its product and its use by local law enforcement?
7. Although Flock's proposed partnership with Nexar may not be in effect at this time, a leaked presentation for the Georgia Attorney General's Office reveals that Flock actively pitched a plan to leverage approximately 350,000 rideshare and delivery vehicle dashcams as mobile license plate scanners.¹⁴ Does Flock still plan to partner with Nexar to collect data from rideshare dashcams?
 - a. If so, will rideshare drivers be made aware that their dashcams are collecting data and be allowed to provide consent for such data collection?
 - b. Will rideshare drivers participating in the program be required to disclose to their passengers that their data may have been collected by Flock?
 - c. What steps does Flock plan to take to protect the privacy of rideshare drivers and their passengers who will be recorded by this or any other similar program?

In addition to the information requests above, as part of our legislative oversight, please preserve all records and communications between you, your employees, consultants, contractors, agents, state and local law enforcement, Immigration and Customs Enforcement, and the Department of Homeland Security, regarding Flock cameras. This applies to internal communications and communications with U.S. departments and agencies. This includes but is not limited to: records and communications via email, whether official or personal; mobile devices; encrypted or

¹⁴ Zachary Chambers, *Flock Secretly Pitched 350,000 Rideshare Dashcams to Police; Passengers Have No Rights*, Tech Times (Aug. 7, 2026), <https://www.techtimes.com/articles/323541/20260807/flock-secretly-pitched-350000-rideshare-dashcams-police-passengers-have-no-rights.htm>.

disappearing messaging applications; social media; calendar entries; meeting notes; and voicemail and text messages. To the extent that you use any auto-delete functions, you should immediately suspend auto-delete functions and notify persons with control over potentially relevant records of their preservation obligations. This preservation request covers both past and current efforts, as well as any planned or in-development measures responsive to the issues raised in this letter.

We look forward to your prompt response and appreciate your attention to this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "A.B. Schiff", written over a horizontal line.

Adam B. Schiff
United States Senator

A handwritten signature in blue ink, appearing to read "Ron Wyden", written over a horizontal line.

Ron Wyden
United States Senator



How to Speak to City Councils About Public Safety Technology

Building Trust, Demonstrating Accountability, and Preparing for Tough Questions

[DOWNLOAD NOW](#)

 **Flock**

Table of Contents

Introduction	1
Chapter 1: Trust Is Now Part of the Job	2
Chapter 2: Moving the Conversation from Surveillance to Governance	4
Chapter 3: Accountability Is Stronger When It Is Visible	6
Chapter 4: The Strongest Budget Argument Is Local	8
Chapter 5: Local Control Matters	9
Chapter 6: Transparency Builds Resilience	10
Conclusion: Own the Narrative Before Someone Else Does	11
Resources & Next Steps	12

INTRODUCTION

The conversation around public safety technology has *changed*.

A few years ago, agencies introducing a new technology program were primarily asked whether it **worked**.

Could it help solve crimes? Would it improve investigations? Could it help officers respond more effectively?

Those questions still matter. Today, however, they are joined by another set of concerns.

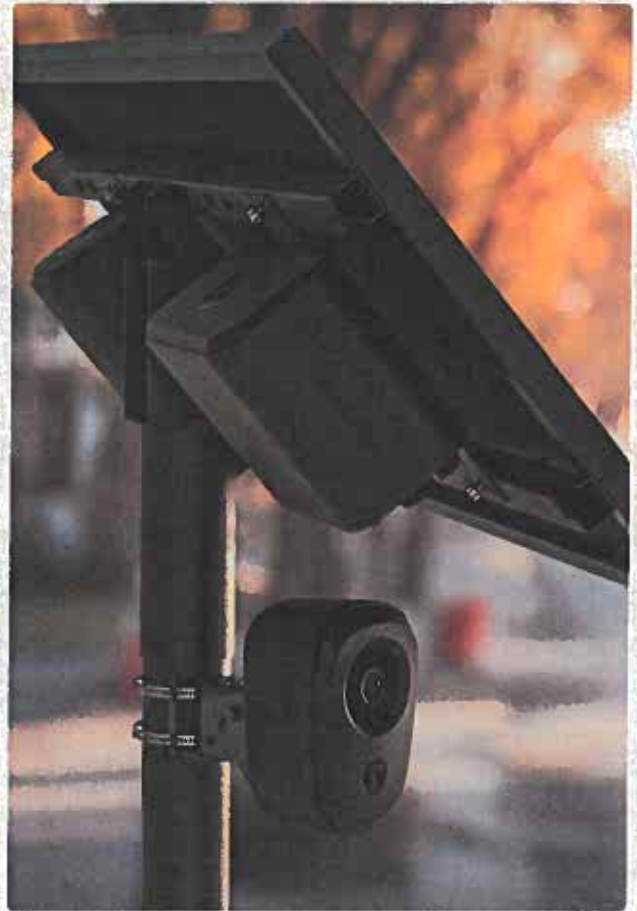
- 1 Who has access to the data?
- 1 How is the technology governed?
- 1 Drivers make mistakes
- 1 How can the public verify that those safeguards are working?

For law enforcement leaders, this shift represents a new reality. Public safety technology is no longer evaluated on performance alone. Councils and communities increasingly **expect transparency, oversight, and accountability alongside public safety outcomes**. The agencies earning long-term support are not avoiding those conversations. They're leading them.

As Chris Colwell, SVP, Customer Experience at Flock, explained during the How to Speak to City Councils webinar:

"The agencies that fare best aren't the ones with the best talking points after the fact. They're the ones who walked into council meeting chambers first, before there was anything to react to and said 'here's *what* we're using, here's *why* we're using it, and here's *how* you can hold us accountable.'"

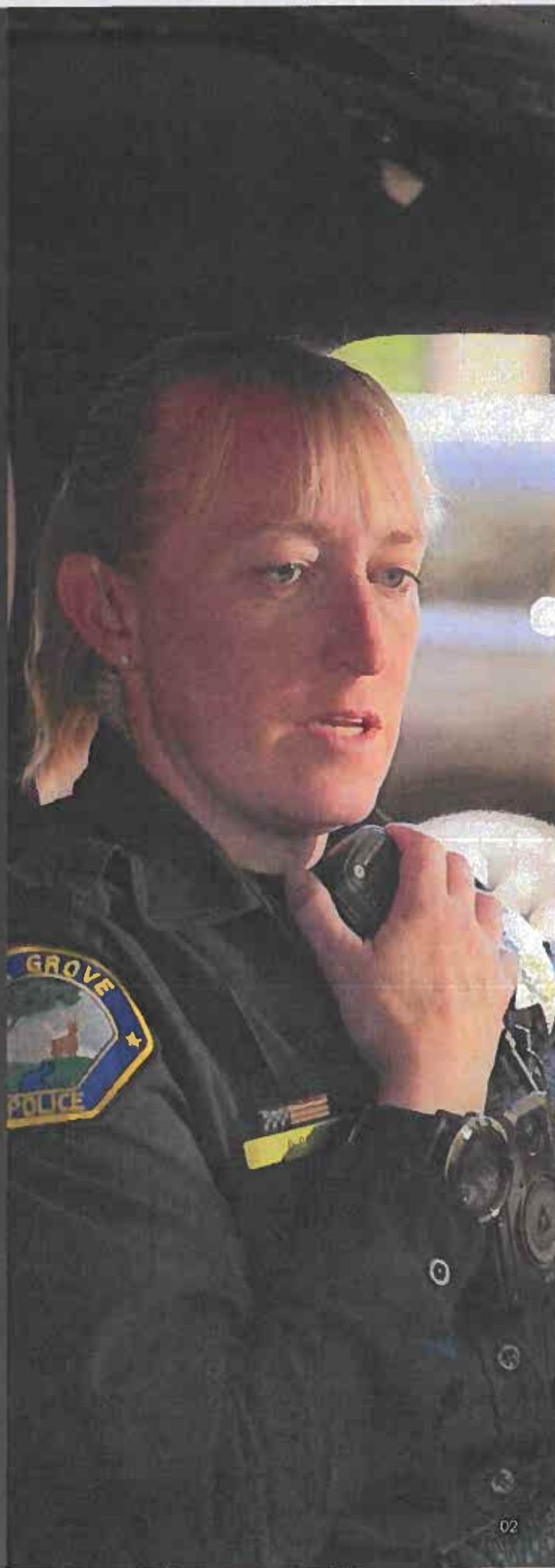
That final point has become the **foundation of successful public safety technology programs**. Not trust alone, demonstrable accountability. The agencies building durable support understand a simple truth: if you do not tell the story of your program, someone else will.



CHAPTER 01

Trust is now part of the job.

Every law enforcement leader understands operational readiness. Policies are reviewed. Personnel are trained. Systems are tested. Outcomes are measured. Increasingly, trust has become part of operational readiness as well.



A program can generate *strong investigative outcomes* and still encounter opposition if stakeholders do not understand how it works or how it is governed.



Across the country, councils are evaluating technology through two lenses at the same time.

Those questions are deeply connected. Flock's Real Time Strategist, Jamie Hudson, has spent decades working in law enforcement and real-time public safety. One pattern stands out when agencies struggle in council discussions. The challenge often begins **long before the meeting** itself.

Opponents have a very carefully scripted narrative. They come prepared. You should also have a carefully scripted presentation that addresses those concerns ahead of time.

The agencies that navigate these conversations successfully rarely wait until a council meeting to educate stakeholders.

They brief city managers early. They meet with council members before votes occur. They share policies proactively and answer questions before public comment periods become the first introduction to the program.

Moving the Conversation from Surveillance to Governance

One of the most common questions agencies hear today is whether license plate recognition (LPR) technology constitutes mass surveillance. Many leaders instinctively respond by attempting to refute the claim. Flock's Jamie Hudson recommends a **different approach**.



Instead of debating terminology, successful agencies focus on governance.

- ❗ Who controls the system?
- ❗ Who can access it?
- ❗ How is information used?
- ❗ How is use reviewed?
- ❗ What safeguards help ensure policies are followed?

Those are questions agencies can answer clearly.

The strongest council presentations spend less time describing technology capabilities and more time explaining the policies that surround them. They show **how searches** are tied to legitimate investigations.

They explain retention policies. They describe auditing requirements. They demonstrate oversight rather than simply promising it.

Most importantly, they bring the conversation back to local priorities.

You care about your community. That's why you're bringing this in. Bring it back to your local need, your local community, the effect it's going to have on quality of life and crime reduction.

"Don't avoid the concept of mass surveillance because you're not going to convince opponents that it's not."

Jamie Hudson, Real Time Strategist, Product Consulting & Training at Flock

Oakland, California offers a powerful example of what that looks like in practice.

140+

Public comments submitted during review

Split

Privacy commission opposed; safety committee deadlocked

7-1

Final council vote in favor of the program



When Oakland's City Council considered its LPR program, the discussion became one of the most scrutinized public safety technology debates in the state. **More than 140 public comments were submitted.** The Privacy Advisory Commission opposed the proposal, and the Public Safety Committee deadlocked before the issue reached the full council.

The discussion was no longer about whether the technology worked. It was about whether the city could govern it responsibly.

Rather than focusing solely on crime reduction, city leaders centered the **conversation on oversight.** They demonstrated live audit logs, explained approval requirements, outlined independent compliance reviews, and showed how accountability would function in practice. The result was a **7-1 council vote in favor of the program.**

The lesson is instructive. The conversation shifted when officials stopped asking the public to trust the technology and started showing how the technology could be audited, reviewed, and held accountable. **Trust moved from assumption to evidence.**

CHAPTER 03

Accountability Is Stronger When It Is Visible

One of the most effective ways to build confidence is to show safeguards rather than simply describe them. That is where Flock's governance tools become important.

Ashley Haber, who leads Flock's Trust & Compliance products, describes her team's mission as helping agencies demonstrate accountability, transparency, and compliance in ways that are visible and easy to understand.



Modern oversight requires more than policy documents. It requires systems that support those policies in practice. Flock builds accountability tools right into their product, with features including;



Agency-Controlled Sharing gives departments control over who can access their data and when. Sharing relationships can be enabled, restricted, or revoked by the agency itself.



Audit Assistance helps administrators surface and review atypical search patterns, document findings, and maintain a clear record of oversight activities.



Offense Type Analytics provides visibility into how searches are being conducted across the organization, allowing command staff to compare search activity against local crime trends and operational priorities.



Transparency Portals allow agencies to publish policies, usage information, and program details directly to the public through an agency-managed website.

Together, these tools help transform accountability from an abstract concept into something that can be demonstrated. This shift from policy to proof is becoming increasingly important.

In Oakland, a former skeptic ultimately cited the accountability framework surrounding the program as a key reason for supporting it. **Oversight mechanisms became as important as the technology itself.** Audit trails, independent reviews, and documented governance practices helped move the discussion from speculation to verification.

Communities rarely ask for perfect technology. They ask for accountable technology. The ability to demonstrate who searched what, when they searched it, and why they searched it allows agencies to answer those questions with facts rather than assurances.

We recommend sharing these videos for more information around how **Flock builds safeguards** into our products:

- ✓ [How Flock is Helping Agencies Improve Transparency and Accountability with Audit Assistance](#)
- ✓ [What Flock License Plate Readers Actually Do \(and What They Don't\)](#)
- ✓ [Inside a Flock LPR Search: How Investigators Actually Use the Tool](#)
- ✓ [Who Can See Flock Data? How Sharing Controls and Audits Really Work](#)

The Strongest Budget Argument Is Local

Questions about funding appear in nearly every council conversation. When elected officials ask whether a program is worth the investment, they are rarely asking for a technical explanation. ***They are asking whether it creates meaningful value for their community.*** Max Weinstein, Director of Public Trust and Technology, encourages agencies to avoid abstract ROI discussions.

"When a council member asks if this is the best use of public safety funding, what they're really asking is: convince me that it matters here."

The most persuasive answers begin with **local outcomes**. Community members want to hear about:

- ✓ Recovered stolen vehicles.
- ✓ Missing persons located.
- ✓ Investigative leads generated.
- ✓ Officer hours saved.
- ✓ Cases cleared more quickly.

Many agencies have found success by reframing the financial discussion itself. The comparison is rarely technology versus nothing.

The comparison is technology versus the cost of unresolved crime.

Max encouraged agencies to compare technology investments against the costs of unresolved crime and noted that **a single recovered vehicle can often exceed the annual cost of a camera**. He frequently points agencies toward tools like CrimeGrade, which estimate the annual cost of crime per household. That perspective changes the conversation from what technology costs to **what inaction costs**.

Everett, Washington provides a useful example. Following a temporary pause related to public concerns and evolving state legislation, Everett reactivated its program under updated legal requirements. The discussion was not framed around technology features. **It was framed around outcomes.**

250+

Arrests supported

Since launching its LPR program, Everett Police Department credited the system with supporting more than 250 arrests, *helping recover stolen vehicles, and assisting with missing persons investigations*. Rather than debating theoretical value, city leaders were able to point to results occurring within their own jurisdiction. That is often where the strongest ROI conversations begin.

CHAPTER 05

Local Control Matters

Questions about data sharing often generate the strongest reactions during public meetings. Will information be shared with federal agencies? Can outside entities access local data? Who ultimately controls what happens to information collected within the community?

Flock's Max Weinstein believes the answer should be simple and direct.

The customer, the agency, controls their own data. That principle is central to successful governance conversations. Sharing relationships are agency-controlled. *Participation is opt-in.* Agencies can revoke sharing relationships whenever they choose. In many states, legislation further limits how information may be shared across jurisdictions.

"Flock does not own data, period. We don't own your data. The agency does. The customer, the agency, controls their own data."

Max Weinstein, Director of Public Trust and Technology,
Customer Experience at Flock

Transparency Builds Resilience

No technology program is immune from scrutiny. The agencies that maintain public trust are not necessarily the ones that avoid challenges. They are the ones that ***respond to those challenges with transparency and discipline.***

One CA law enforcement agency recently faced this reality firsthand. As public concerns around data sharing gained attention across its region, agency leadership **conducted a review of historical audit activity and identified a configuration issue** that had unintentionally created access during an early setup process.

Rather than waiting for the issue to surface publicly, the agency initiated a full review, investigated the circumstances, worked closely with Flock to understand exactly what had occurred, and shared its findings directly with elected officials.

As the Chief involved in the process explained:

"We wanted to be the expert in the room about what happened, why it happened..."

The result was not the collapse of the program. Council support continued. Oversight increased. Public accountability strengthened.

That outcome highlights an important reality. Trust is not built by avoiding difficult conversations. ***Trust is built by addressing them directly.***

Richmond, California provides another example.

After concerns emerged around data sharing and sanctuary city policies, the city's program was paused and subjected to intense public scrutiny.

Rather than relying on generalized claims about effectiveness, department leadership presented two and a half years of local results, **including 274 arrests and 259 vehicle recoveries** connected to the program. The council ultimately voted 4-3 to reinstate the system. The deciding factor was not a new technology feature. It was a clear connection between **governance, accountability, and measurable public safety outcomes.**

Richmond California

2.5

Years of local results presented

274

Arrests connected to the program

259

Vehicle recoveries on record

4-3

Council vote to reinstate the system

Own the Narrative Before Someone Else Does

Every community conversation about public safety technology eventually comes down to the same question. *Can this program improve safety while remaining accountable to the public it serves?*



Trust is not built through promises. It is built through transparency, oversight, and outcomes that communities can see for themselves.

- ✓ Lead early.
- ✓ Show the guardrails.
- ✓ Demonstrate accountability.
- ✓ Measure what matters.

The agencies succeeding today are answering that question before they are asked. They are publishing policies, they are demonstrating oversight, they are sharing outcomes, they are explaining governance, and they are inviting scrutiny.

As Flock's Chris Colwell reminded attendees:

"This story is going to get told either way. The only question is whether you're going to be the one telling it."

Chris Colwell, Director, Product Consulting & Training at Flock

The strongest technology programs are not defined by cameras, software, or investigative tools. They are defined by how responsibly those tools are governed.

Resources and *next steps*

Continue the conversation.
Ways to keep building accountable
support for your program:

- ✓ Explore the [Flock Trust Hub](#) to learn more about privacy, transparency, data governance, and accountability.
- ✓ Book a council preparation call to review your upcoming presentation, stakeholder concerns, and local policy considerations.
Email Chris Colwell at chris.colwell@flocksafety.com.
- ✓ Connect with your Customer Success Manager or our Support Team at support@flocksafety.com for onsite support, council engagement assistance, and additional resources designed to help your agency navigate public conversations with confidence.

