



ite 'New' Updates, Flock's Creepy Cameras Remain Major Civil Liberties Threat

In response to Flock's announcement of operational changes, the ACLU breaks down why many fall short.

Chad Marlow, ACLU

Tracking ALPR Cameras News Series

August 13, 2026

In response to Flock's announcement of operational changes, the ACLU breaks down why many fall short.

Surveillance company Flock Safety announced several operational changes in response to a torrent of criticism and overwhelming public opposition to its mass government surveillance product.

Flock's threat to privacy stems from its operation of more than 120,000 automatic license plate readers (ALPRs) nationwide, which includes broad location data collection and sharing. While one proposed change to Flock's operations might constitute a positive development, most of the other changes seem to be following Flock's playbook of treating legitimate privacy concerns as mere public relations problems. Several of the proposed changes Flock is touting are merely retreads of previous inadequate safety measures.

ALPR companies like Flock violate our privacy across the country by taking photos of every vehicle passing their cameras, logging detailed information about them into a massive nationwide database, and making it possible to track those vehicles and apply AI to uncover their occupants' private

patterns of life. [The ACLU is fighting alongside communities](#) to cancel local ALPR contracts and push lawmakers to protect our rights from this surveillance nightmare. Below, the ACLU details and responds to Flock's announced changes.

Flock reduces default data retention time period, but the devil may be in the details.

Flock announced it is reducing its standard data retention from one month to one week, conceding for the first time that “roughly 90 percent of all searches on Flock already happen within a week” of the data's collection.

“For cases that need more time, Flock is launching Evidence Mode: when a search is tied to a case number, that data is preserved instead of aging out after 7 days,” Flock said in its statement. “Agencies can still set retention to whatever their state or local policy requires. Evidence Mode will be provided to customers at no cost.”

Our Response: While Flock has not shortened the default retention period to the ACLU's recommended 48 hours, its proposal may be a step in the right direction. Whether this is a real change or just another Flock PR move, however, will depend on how its “Evidence Mode” operates.

If “Evidence Mode” only retains hit result data that police determine may be evidence in an active investigation of a specific case, then the change may be a positive one. But if “Evidence Mode” triggers the retention of any ALPR data that is searched, then the new mode could indefinitely retain all the ALPR data Flock collects and shares nationally. This would make Flock's data retention problem even worse. Even if “Evidence Mode's” data retention hold only applies to hits returned on a given search, it would still retain significant amounts of location data on persons and vehicles who law enforcement do not suspect have engaged in any wrongdoing.

While Flock doesn't establish state or local ALPR data retention periods, its system empowers governments to choose their own retention periods. For states and localities that want and permit longer data retention periods, all they have to do is ask. Although Flock may not technically be the one unlocking the door to months of people's private location data, it is responsible for building the door and handing out the keys.

Flock claims to provide more local control over what their ALPR data can be searched for; it has repeatedly failed to effectuate such limitations in the past.

Flock claims that its changes will provide “more local control,” meaning local police can decide what types of offenses other Flock customers can search their data for. “For example,” Flock said, “City A could allow City B to search its cameras for a stolen vehicle or violent crime while blocking searches related to immigration enforcement.”

Our Response: This is not new. Flock has attempted this before, and the security measure failed because users were easily able to circumvent the system’s requirement that police input the purpose of their search.

For example, on June 12, 2025 Flock started claiming its new “Proactive Search Term Tool” would block any “impermissible” searches, such as abortion-related searches in states like Illinois that prohibit sharing reproductive healthcare data. But police officers quickly realized they could just input “investigation” or even “hehehe” as a search reason and it would be approved. Flock later switched from an open text box to a drop-down menu of reasons, but that just offered police a list of acceptable purposes they could choose from, whether it was accurate or not. Until Flock demonstrates they can develop a reliable, workable system to prevent improper searches, this promise of local control provides nothing more than a false sense of security.

Flock claims the universal roll out of its audit assistance tool will detect police misuse, but the effectiveness of its audit tool has never been independently evaluated.

Flock’s next change makes its “Audit Assistance” tool, which the company claims “flags abnormal search behavior,” a standard feature for all its customers. Flock lauds the effectiveness of its audit tool by simply stating that “identification of [police officer] misuse went up” after it established its audit tool.

Our Response: While providing “Audit Assistance” to all departments makes sense, there is no evidence that the tool works consistently to address what the Washington Post observed is a growing pattern of police officers turning Flock into a personal stalking tool. While dozens of officers have recently been arrested, fired, or otherwise disciplined for misusing Flock for personal reasons, Flock claims these arrests are proof its auditing tool works. However, unless we know the number of officers misusing the system, we cannot conclude if Flock and its auditing tools are catching 95 percent of violators or 5 percent. Flock needs to have its auditing tool analyzed by an independent evaluator to determine its actual effectiveness. Until then, we don’t know if the tool is a real security measure or just window dressing.

Flock claims requiring the reasons for a search will prevent abuse, even though that same intervention failed miserably before.

Perhaps the oddest part of Flock's announcement is its claims that "now every search will require" police to input a case code, a previously optional requirement it first rolled out in July 2025. While claiming that a "search without a reason is a search that shouldn't happen in the first place," Flock's announcement fails to note how easily users have circumvented "search reason" security measures in the past or how its new policy improves the quality of the feature. This leaves the public wondering how making an ineffective voluntary security measure mandatory will improve its functionality.

Our Response: Until Flock demonstrates through independent evaluation that its search reason requirement is an effective, air-tight security measure, it's reasonable to assume its past failures are prologue.

Transforming an exceptionally dangerous mass surveillance system into one that is fully protective of civil rights and civil liberties is a difficult, if not impossible task. That is even more the case with a company like Flock, whose nearly \$1 billion in venture capitalist funding has locked it into an operational model that seeks to trade our privacy for massive profits. Given that Flock's latest announcement still appears more focused on addressing a perceived PR problem than the significant harms its products create, this is hardly the step forward Flock wants us to think it is. Change may still come as Flock faces this ever growing threat to its corporate viability, and [we will continue to analyze](#) the company's proposals fairly and honestly, but we certainly won't be holding our breath.

Join the Fight to Protect Digital Privacy

Our fight for privacy depends on your support. By donating now, you'll help to fund strategic litigation, advocacy, and organizing needed to defend our right to privacy in the digital age, protect against government surveillance, and much more. Help us make lasting change.

Donate to the ACLU

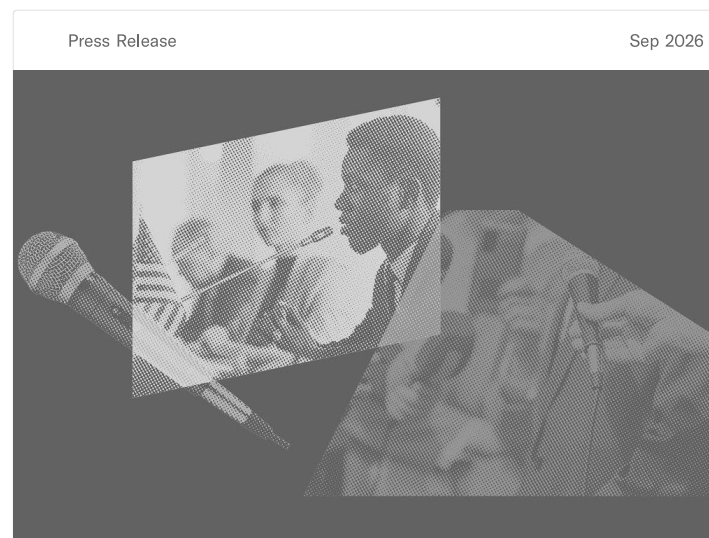
Related Issues

Privacy & Technology

Automatic License Plate Readers

Location Tracking

Related Content



Free Speech Privacy & Technology**ACLU, ACLU of D.C., and National Press Photographers Association Tell Court that Blocking Drone Photography of DHS Operations Violates First Amendment**

WASHINGTON – Today, the American Civil Liberties Union (ACLU), the ACLU of D.C., and the National Press Photographers Association filed an amicus brief in support of a Minnesota photojournalist's lawsuit challenging the Federal Aviation Administration's (FAA) Temporary Flight Restrictions (TFR). Earlier this year, as ICE was carrying out brutal immigration raids across the country, the FAA dramatically expanded restrictions on drone flights, banning such flights over any Department of Homeland Security (DHS) facility or "mobile asset," which included any DHS vehicle. As the amicus explains, the TFR made it functionally impossible for journalists to use drones to gather news in any area where immigration enforcement agents were deployed, violating the First Amendment right to record public officials performing their duties in public. "The FAA's restriction forced journalists reporting on immigration enforcement activity to ground their drones or risk criminal charges. This choice is unacceptable, unconstitutional, and runs roughshod over the First Amendment right to gather news," said Scarlet Kim, senior staff attorney with ACLU's Speech, Privacy, and Technology Project. The brief explains that the FAA's restriction was not about public safety or national security. Journalists were previously already advised and generally adhered to avoiding airspace around sensitive locations, such as active military bases, airports, and aircraft carriers. Moreover, press drones weren't interfering with official activity or putting anyone at risk by capturing immigration enforcement activity unfolding in public. "Under Trump, even the Federal Aviation Administration has become a political censor," said Arthur Spitzer, senior counsel at ACLU-D.C. "The agency should be protecting the safety of the flying public, not protecting ICE from unfavorable news coverage." The brief further explains that journalists were effectively being censored beyond their DHS coverage, since the unpredictability of where any DHS vehicle may be traveling made it functionally impossible for journalists to use drones for any newsgathering in areas where immigration enforcement agents were deployed without putting themselves at risk of severe legal and financial penalties. "Drones have become essential, safe, and economical tools for documenting government activity and other matters of public concern. By creating an unpredictable moving exclusion zone around DHS assets, the FAA forced visual journalists to choose between abandoning lawful newsgathering and risking severe penalties," said Mickey H. Osterreicher, general counsel for the National Press Photographers Association. "Safety restrictions must be narrowly tailored and consistent with the First Amendment, especially when they limit the public's ability to observe government officials performing their duties."

Court Case: Levine v. FAA**Affiliate:** Washington, D.C.

New Hampshire

Sep 2026

**Privacy & Technology**

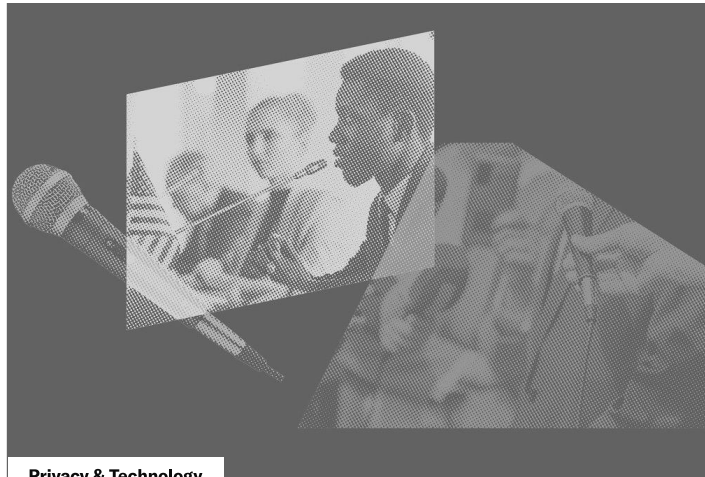
LaValley v. Concord Housing and Redevelopment Authority

On September 2, 2026, the ACLU, ACLU of New Hampshire and New Hampshire Legal Assistance brought a class action lawsuit against the Concord Housing and Redevelopment Authority for installing and operating surveillance devices in tenants' apartments. The devices collected hundreds of millions of data points recording movement, sound levels, and other information from inside tenants' homes.

Status: Ongoing

Press Release

Sep 2026

**Privacy & Technology****ACLU and New Hampshire Legal Assistance Sue Housing Authority Over Electronic Surveillance of Residents**

CONCORD, N.H. — Today, residents of housing developments owned and maintained by the Concord Housing and Redevelopment Authority (CHRA) in New Hampshire sued to block CHRA from harvesting sweeping data about tenants' activity patterns in their homes through surveillance devices purchased from a private company, Minut Inc. In the fall of 2024, CHRA began installing Minut Monitor devices inside people's apartments across the properties it manages, providing government employees with real-time, remote access to granular data about activity within tenants' homes. These devices are capable of collecting data such as the decibel level of detected noise, motion detector readings showing physical movement of residents and guests, smoke and humidity levels, and scans for iOS signals, which can estimate how many people are nearby. "People should feel secure in their homes—not watched, judged, or punished by technology they never asked for. These devices change how tenants interact with their own apartments, turning everyday living into a source of fear," said Christopher Schott, director of New Hampshire Legal Assistance's Fair Housing Project. "No one should worry that an assistance animal, a television, or other routine household sound could trigger penalties simply for living their life." Taken together, the information provided by Minut Monitors can create a mosaic of detail about peoples' lives, revealing when they wake up, when they come and go from their home, and more. Minut Monitors near tenants' beds can even potentially track sound and motion data that could reflect intimate acts. Much of the data is logged on a minute-by-minute basis. For example, each Minut Monitor logs sound-level readings approximately every single minute, up to 1,440 times a day. For one tenant, the Minut Monitor logged more than 140,000 motion events within a seven-month period for just a single

unit – an average of more than 700 motion events per day. All told, CHRA has amassed hundreds of millions of data points from within tenants' apartments. The data is stored indefinitely and available to CHRA employees on demand. The class action lawsuit was filed by New Hampshire Legal Assistance, the American Civil Liberties Union of New Hampshire, and the American Civil Liberties Union. As the complaint explains, this invasion of privacy in individuals' homes by a government agency is unacceptable and violates two provisions of the New Hampshire Constitution, Article 19 and Article 2-b. Article 19 prohibits unreasonable searches by the government. Article 2-b, which was added to the New Hampshire Constitution by referendum in 2018, provides that "an individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent." "We're suing because everyone deserves privacy in their own home. The government shouldn't get to know if you are getting up in the middle of the night to use the bathroom or when your morning alarm goes off just because you live in public housing," said Maria Savarese, staff attorney at the ACLU of New Hampshire. "Our state constitution is clear: we have the right to live free from government surveillance and intrusion in our homes." Furthermore, CHRA's implementation of Minut Monitors over the past two years has been marked by severe lack of transparency and a dismissal of tenants' objections. Throughout the installation process, significant information was left out of notices to tenants, painting the technology as much less invasive and far-reaching than the Minut Monitors' actual capabilities. For example, CHRA did not disclose the occupancy and motion sensor capabilities of the devices, only disclosing the use of sensors for smoke, noise, temperature, and humidity detection. When residents asked outright whether the monitors placed in their homes included motion sensors, CHRA failed to directly answer the question. CHRA also omitted from their tenant communications that Minut's terms of service includes a warning about potential inaccuracies in the AI and machine learning models used to analyze and detect the presence of cigarette smoke. This is especially alarming considering that CHRA's stated purpose of installing Minut Monitors is to substantiate lease violations that can lead to eviction. When one resident asked to see the data produced from tracking her day-to-day activity, CHRA denied her request. In multiple instances, CHRA disregarded residents' concerns about the surveillance they were subjected to. Tenants are not able to opt out of this invasive surveillance, and if they attempt to remove the devices from their units, they are subject to significant fines and have been threatened with eviction. CHRA failed to create any policy for secure data retention and destruction, despite a request to do so by its own Board of Directors, leaving Minut free to handle residents' data however it wants. Minut's data retention policy also gives the company complete authority to retain user information for any duration and purpose. CHRA did not share this policy with tenants at any point. The lawsuit also explains that far from improving tenants' housing

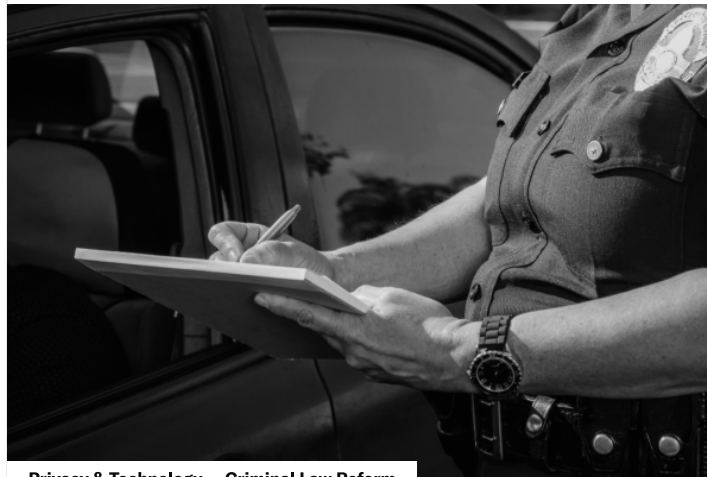
experience, CHRA's insistence on surveillance exposes them to serious safety risks. For example, access to the data could severely endanger victims of domestic violence or stalking whose abusive former romantic partners or stalkers could learn details about their patterns of life. "A government-installed sound meter and motion sensor hovering near your bed should be the stuff of dystopian science fiction, but it is reality in Concord. Public housing residents shouldn't have to choose between becoming homeless and being subjected to constant electronic monitoring inside the privacy of their own homes," said Nathan Freed Wessler, deputy director of ACLU's Speech, Privacy, and Technology Project. "This case happens to rely on the robust protections of the New Hampshire Constitution, but landlords across the country are now on notice: subjecting your residents to this chillingly invasive surveillance will land you in court."

Court Case: LaValley v. Concord Housing and Redevelopment Authority

Affiliate: New Hampshire

News & Commentary

Sep 2026



Privacy & Technology **Criminal Law Reform**

Another Problem With AI-Assisted Police Reports: Companies Can Have Incentives to Distort Their Content

Police Companies Could Train Their AI to Hide Use of Their Products or Make Them Look Good

By: Jay Stanley



© 2026 American Civil Liberties Union