ACLU

NEWS & COMMENTARY

Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance

Build it (an authoritarian tracking infrastructure) and they (expanded uses) will come

Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy, and Technology Project

August 18, 2025

Free Future home

The cloud Automatic License Plate Reader (ALPR or LPR) company Flock is building a dangerous nationwide mass-surveillance infrastructure, as we have been pointing out for several years now. The problem with mass surveillance is that it always expands beyond the uses for which it is initially justified — and sure enough, Flock's system is undergoing insidious expansion across multiple dimensions. If your community adopts this technology, you need to know it's doing more than just recording what car is driving

where and at what time. It's worth stepping back and looking at an overview of what's going on.

The company's surveillance data is being used by ICE. First, as has received wide attention, this system is being used by ICE to help carry out the Trump Administration's abusive removal program.

Flock sells their cloud-connected cameras to police departments and private customers across the nation, pulls the license plate readings they collect into their own servers, and allows police to do nationwide searches of the resulting database, giving even the smallest-town police chief access to an enormously powerful driver-surveillance tool. The tech news outlet 404Media obtained records of nationwide searches which include a field in which officers list the purpose of their search. These records revealed that many of the searches were carried out by local officers on behalf of ICE for immigration purposes, including its notorious Enforcement and Removal Operations division. Emails from police departments in Oregon also shed light on how local police are providing informal assistance to ICE.

It's safe to say that even many who support the use of ALPR programs by their local police to catch local criminals do not support funneling the data that is collected to the Trump Administration and those carrying out its abusive and often unlawful immigration program.

A search for a recipient of an illegal abortion

The same kinds of police department logs that revealed ICE's access to Flock's dragnet also revealed that a police

officer in Texas used the system to search nationwide for a woman who'd had a self-administered abortion — illegal in the state. An abortion rights group told 404Media that, based on calls to their hotline, already "there is an overwhelming fear" among women that they're "being watched and tracked by the state" — and such reports are hardly going to help. This mass surveillance tool is creating fear among those targeted by immigration, anti-abortion, and other regressive actions, but eventually everyone will become aware that their movements are being tracked. That's no way to live in a democratic society.

Plugging in to data brokers

Meanwhile, as police around the nation expand their uses of this surveillance machinery, Flock is expanding the power of the system itself. For example, the company is planning to plug its systems into commercial data brokers that offer services such as "people lookup." Flock has long claimed that their LPRs don't collect personally identifiable information, as if license plates can't easily be connected to specific people. That claim was always bogus, but with their new product they make that falsity explicit, boasting that the new product will let police "jump from LPR to person."

In the 1970s, after some government agencies were found to be building dossiers on people who aren't suspected of involvement in crime like the East German Stasi, Congress enacted the Privacy Act banning agencies from such recordkeeping. Yet the ethically shady and frequently inaccurate data broker industry does basically the same thing, and when law enforcement becomes a customer of those data brokers, it represents an end-run around the law.

By tying its LPR data together with data brokers, Flock is effectively automating and scaling the end run around our checks and balances that law enforcement data broker purchases represent. (A proposal called the Fourth Amendment is Not For Sale Act that would ban this was passed by the U.S. House in 2024, but got blocked in the Senate.)

From still to video, and with AI

In another major expansion, Flock is turning its plate readers into surveillance cameras. The company has announced that police departments will soon be able to obtain not just still photos from ALPR cameras, but also video, with the ability to request live feeds or 15-second clips of cars passing by the cameras. And Flock is using AI to let law enforcement search through that data using natural language searches. The company uses the example of searching for "landscaping trailer with a ladder," but we have to assume searches could encompass descriptions of anything captured by one of their cameras, including vehicle occupants and bystanders.

We recently wrote about how generative AI is turbo-charging video search and surveillance, and this is an example of the trend. Imagine that a police officer stood on your street writing detailed notes about you every time you drove or walked by them. All the details about what your car looks like (make, model, color, distinguishing characteristics, bumper stickers, etc.), as well as details about visible occupants and pedestrians — how many, at what time, their activities, demographic data, what they are wearing, attributes they may have such as a beard, hat, tattoo, or t-shirt, and what that hat, t-shirt, or tattoo might say. Now

imagine that there is an army of police officers doing this on every block.

This is the surveillance world that Flock is building.

Creating an infrastructure for corporate blacklisting and surveillance

In June, Flock also announced the launch of a "Flock Business Network," a "collaborative hub designed to help private sector organizations work together to solve and prevent crime."

This will sound ominous to anyone familiar with the very long history of private companies and government agencies working together to create watch lists, blacklists, and databases about people in the United States. In the heyday of the labor movement (and perhaps today), organizers were commonly put on blacklists as "troublemakers," and could have trouble getting a job as their name was shared among employers. During the civil rights, antiwar, and other social justice movements of the 20th century, there were a number of private databases created by shady collections of right-wing vigilantes and super-patriots who took it upon themselves to compile dossiers on activists they disagreed with. These private databases, such as the San Diego Research Library and the Western Goals Foundation, were shared with police and government security agencies and took on quasi-official roles in the efforts of police "intelligence" arms to combat those progressive movements, while remaining outside the normal checks and balances of government.

Today, face recognition technology threatens to make these lists easier than ever to create and administer — and so does license plate surveillance. In its announcement, Flock boasted that its service would allow companies to "add vehicles to Flock Hotlists... so any user subscribed to that Hotlist is alerted the next time that vehicle is detected by a Flock LPR," giving the private sector "the power of a shared network to identify threats." Elsewhere Flock says, "By sharing insights and intelligence, companies can identify patterns, suspects, and criminal networks that might not be apparent to a single security team."

Investigating criminals should be the job of law enforcement, not big companies that have strong incentives to use these infrastructures against labor activists, disfavored customers, and others — to use them not for crime, but to protect the bottom line.

Generating suspicion

Finally, as I recently wrote about, Flock has also introduced AI analytics products that shift the company from providing tools for officials to use in *investigating* suspicion to *generating* suspicion. Because the company funnels plate reads from customers across the nation into its own centralized database, it is able to run analytics on that dataset. One such analysis service that it has begun selling is an attempt to identity "large-scale criminal activities" by scanning the movement patterns of all vehicles contained in their dataset to try to identify and alert law enforcement to those that their algorithm decides are "suspect."

Overall, this explosion of new uses is what happens when

you build an authoritarian tracking infrastructure — it expands in more and more ways. State legislatures and local governments around the nation need to enact strong, meaningful protections of our privacy and way of life against this kind of AI surveillance machinery.

Learn More About the Issues on This Page

Automatic License Plate Readers

Accountability in Artificial Intelligence

Privacy and Surveillance **Surveillance Technologies**

Location Tracking **Privacy & Technology**

Racial Justice **National Security**

Related Content

News & Commentary Sep 2025