

Communication from Public

Name: Citizens for a Better Los Angeles

Date Submitted: 06/30/2026 09:11 PM

Council File No: 26-0803

Comments for Public Posting: CBLA submits the attached letter in response to Councilmember Jurado's motion re ALPRs/outdoor cameras. It's important to look at agreements with private vendors in the context of the LAPD's creation of a Real Time Crime Center to connect cameras used by individual vendors to a unified network. We are concerned that the current approach will result in an ad hoc system with cameras from various vendors linked together a patchwork network infrastructure. In order to balance effective law enforcement with privacy concerns, the City Council should work with the LAPD to develop a comprehensive plan with clear goals, uniform standards and meaningful oversight. Please see the attached letter for our detailed comments.



June 30, 2026

Los Angeles City Council
Los Angeles City Hall
200 N. Spring Street
Los Angeles, CA 90012

Re: Council File 26-0803, Flock Safety / License Plate Reader / Public Safety Considerations
Concerns Re Data Security and Access to Data Collected by Outdoor Cameras

Members of the Los Angeles City Council,

Citizens for a Better Los Angeles (CBLA) is a nonprofit public benefit corporation organized to protect the rights and promote the well-being of all people throughout Los Angeles County. One of our areas of focus is privacy, and we're writing to comment on Councilmember Jurado's motion regarding the use of Flock cameras by the LAPD. We understand Councilmember Jurado's concern about the possible misuse of these cameras, but we believe the current motion fails to consider the range of issues involved with the use of cameras in public spaces and we'd like to suggest a larger and more thorough discussion of these issues.

In the first place, while Flock is aggressively lobbying for the use of its cameras in communities across the US, it is not the only company marketing these services. The LAPD already uses cameras made by Motorola and Axon in some parts of the city. Additionally, the LAPD is creating a Real Time Crime Center to connect cameras used by individual vendors to a unified network. This network could also potentially include Ring cameras installed by private owners of residential buildings. This seems to indicate that, rather than first developing a comprehensive plan to create a network of cameras with clear goals, uniform standards and effective oversight, the city is instead building an ad hoc system with cameras from various vendors linked together a patchwork network infrastructure.

We understand that the LAPD relies on video cameras to identify and locate perpetrators of serious crimes. **We believe that it's possible to balance privacy protections with effective law enforcement, but in order to do that, it's necessary for the city to take a comprehensive view. We suggest that, rather than focusing just on Flock, the city council expand its focus and look at the big picture. To do this, we recommend the following:**

- * Create an inventory of existing/proposed cameras, public and private, and network infrastructure that the LAPD has/will have access to;
- * Request that the LAPD provide an overview of existing and proposed network infrastructure,

- including the vendors involved, with an outline of how the system functions;
- * Review all current and proposed agreements with vendors/potential vendors;
- * Request that the LAPD provide information on persons and entities outside the LAPD who will have access to any/all cameras and/or data; i.e. Flock, Motorola, Ring employees.
- * Ensure that all data held by the LAPD and/or vendors is stored on servers located in the US (preferably in California) and that these servers are governed by US (and California) law;
- * Review the LAPD's policy/policies governing the use of cameras, access to the network and access to data;
- * Ensure that all agreements with vendors require them to be governed by the LAPD policies referred to above;
- * Ensure that all agreements with vendors require them to defend, indemnify and hold harmless the city from any and all actions against the city resulting from failures of the vendors' hardware/software/firmware or security protocols, including actions resulting from data breaches ransomware attacks or unauthorized access to systems maintained by the City of LA;
- * Ask the City Attorney, with assistance from the city's Information Technology Agency, to assess the LAPD's policies and practices with an eye toward potential liability and to make recommendations to the council.

In order to provide context, we provide two recent articles dealing with issues related to municipal camera networks. The first is specific to LA, and covers issues arising from a donation of Flock cameras to the LAPD. The second covers the unauthorized use of municipal camera networks by outside actors to conduct surveillance of individuals and groups.

LAPD Deputy Chief Has Expressed Concerns about Flock Cameras

LAPD Deputy Chief John McMahon, who heads the department's Information Technology Bureau, has raised concerns about a donation of Flock ALPR cameras by the Police Foundation. Please see the excerpt below from a story published in the LA Times on April 10, 2025:

The Flock cameras, he [McMahon] said, are not totally compatible with the LAPD's systems, including the department's fledgling realtime crime center, which monitors intelligence gathered from around the city. The department already uses plate readers from major companies Motorola Solutions and Axon, and McMahon said there are strict rules about how long the data they collect is stored, who gets to see it, and when. Its contract with Flock's data policies are slightly different, he said. McMahon, who heads the LAPD's Information Technology Bureau, said police departments should own and "retain full control" of the data they collect and be able to use it "as law enforcement agencies see fit" under the law.

The full article is included as Attachment A.

Ideally, the LAPD/City of LA would own and operate all cameras, network infrastructure and related systems. While vendors may claim that they do not share collected data, there is no way for the city to verify these claims, and there are significant incentives for vendors to find ways to monetize data.

Municipal Camera Networks Have Been Hacked to Spy on Individuals and Groups

There are known cases of outside parties hacking into municipal camera networks to conduct surveillance of individuals and groups. These scenarios could lead to the targeting of individuals and groups based on political association, religious beliefs or other affiliations. AI greatly increases the ability of outside parties to monitor individuals and groups based on physical appearance, travel patterns or types of behavior. A recent article in the Financial Times highlighted the way in which the growth of municipal camera networks have increased the potential for mass domestic surveillance. It offers the following quote from a security official in a nation belonging to

the “Five Eyes” intelligence alliance:

“They’re the ones putting the cameras up — all we have to do is find a way in. And there is always a way in.”

The full article is included as Attachment B.

Again, we urge the council to go beyond Councilmember Jurado's motion and undertake a comprehensive review of the city's network of cameras in public spaces. In this way, working together with the LAPD, the council can enhance public safety, protect citizens' right to privacy, and avoid costly liability claims that could result from a lack of thorough planning.

Thank you for your time.

Sincerely,
Casey Maddren
Citizens for a Better Los Angeles



CALIFORNIA

A rich L.A. neighborhood donated surveillance technology to the LAPD — then drama ensued



Cheviot Hills — a wealthy community sandwiched between the 10 Freeway and Century City — raised more than \$200,000 to purchase scores of controversial, high-tech cameras that scan license plates. (Myung J. Chun / Los Angeles Times)

**By Libor Jany**Staff Writer | [Follow](#)

April 10, 2025 3 AM PT

When residents of a ritzy West L.A. neighborhood experienced an increase in burglaries last year, they decided to invest in technology to fight the problem.

The neighborhood association in Cheviot Hills — a community of million-dollar homes sandwiched between the 10 Freeway and Century City — raised more than \$200,000 to purchase scores of controversial, high-tech cameras that scan license plates.

The automated plate readers, as they are known, enable authorities to track when vehicles of interest pass through certain intersections. The devices can also be mounted on police cars, allowing officers to sweep up troves of license plate data as they drive around. Police say the gadgets help investigate stolen cars, locate fugitives, and solve crimes by checking who came and went from a neighborhood on any given day.

But when the community donated the cameras to the Los Angeles Police Foundation — one of several nonprofits that support the Los Angeles Police Department — they sent them with strings attached: The police were only allowed to use them in Cheviot Hills.

In the months since, the act of charity has ignited discussions about who gets to decide how technology donated to the LAPD is deployed — and whether the data collected by the plate readers could be used for purposes far beyond the intended scope.

Critics have long warned about privacy concerns because the cameras track people without consent or a warrant, collecting data about law-abiding motorists that is stored up to five years.



When Cheviot Hills donated plate-scanning cameras to the Los Angeles Police Foundation — one of several nonprofits that support the LAPD — they sent them with strings attached: The police were only allowed to use them in Cheviot Hills. (Myung J. Chun / Los Angeles Times)

Since its creation more than 25 years ago, the Los Angeles Police Foundation has funneled millions from mostly unnamed donors to the LAPD. Sometimes the money pays for holiday parties or exercise equipment, but it has also been used to acquire cutting-edge police equipment and technology not covered in the department's annual multibillion-dollar budget.

LAPD Deputy Chief John McMahon has accused the Police Foundation of overstepping its bounds with the plate reader donation, according to sources who requested anonymity to avoid retaliation for speaking about internal department matters. McMahon objected to the limitations on where the cameras could be used, the sources

said, and also took issue with the foundation pushing to buy the plate readers from a specific contractor, an Atlanta-based startup called Flock Safety.



CALIFORNIA

FOR SUBSCRIBERS

LAPD cops shot 21 bystanders in 10 years. How does it keep happening?

March 12, 2025

After McMahon questioned the Flock camera donation in December, foundation board member Jeffrey Neu filed an internal complaint against him alleging bias, the sources said.

Neu did not respond to a request for comment.

McMahon declined to discuss the pending complaint, but told The Times there were good reasons to push back against the donation. The Flock cameras, he said, are not totally compatible with the LAPD's systems, including the department's fledgling real-time crime center, which monitors intelligence gathered from around the city.

The department already uses plate readers from major companies Motorola Solutions and Axon, and McMahon said there are strict rules about how long the data they collect is stored, who gets to see it, and when. Its contract with Flock's data policies are slightly different, he said.

McMahon, who heads the LAPD's Information Technology Bureau, said police departments should own and "retain full control" of the data they collect and be able to use it "as law enforcement agencies see fit" under the law.

"Right now individual companies are trying to monopolize the business and prevent that from happening," said McMahon. "That's not in the best interest of taxpayers."

The Police Foundation did not respond to inquiries.

Holly Beilin, a spokesperson for Flock Safety, said the company recently gave law enforcement users, including the LAPD, the ability to more easily integrate Flock's software with their systems. The department has used Flock cameras before without issue, Beilin said, noting that police can also access privately owned devices with permission from the owner.

For the record:

9:30 a.m. April 10, 2025 *An earlier version of this story said Flock made source code available for free to law enforcement users. It did not.*

“There are more Flock cameras in the Los Angeles metro area than almost any other vendor, and detectives are regularly using them to solve crime,” she said.

She added that under the company's terms of service, Flock customers who give their cameras to police have to abide by Senate Bill 34 and other laws governing the sharing of license plate data.

The Flock dispute has made enough noise to draw more scrutiny from the department's civilian oversight panel, which said it wants to avoid a precedent where crime-fighting technology only goes to areas that can afford it.

At a meeting earlier this year, members of the Police Commission voted to approve the Cheviot Hills donation. The City Council also signed off on accepting the Flock cameras.

But oversight officials have demanded more information about the department's overall strategy for deploying plate readers in other areas of the city.

LAPD officials told the commission they currently have 1,500 police vehicles equipped with plate readers and another 160 devices that are mounted onto poles. The cameras, essentially a beefed-up version of the technology used to collect highway tolls, collect hundreds of thousands of plate numbers every month.

Images of the plates are automatically run through criminal databases and trigger alerts to officers in the field when they record a “hit.” Some vendors claim that new add-ons can detect subtle changes in motorist behavior, such as when a would-be burglar is “casing” a home by circling the block in their car.

The department currently has an information-sharing agreement with five other jurisdictions, who have all agreed that they will not share the data with federal immigration authorities.



Voices

Letters to the Editor: Privacy laws make it too difficult to learn outcomes when and if police are disciplined

March 22, 2025

Commission President Erroll Southers asked how LAPD chooses where the readers are stationed, and whether the decisions are “being influenced by donors.”

Most of the cameras are stationed in the San Fernando Valley, near crime hot spots and critical infrastructure, as well as at highway exits and on-ramps, responded Cmdr. Gisselle Espinoza.

“It is not random, it is not loosey-goosey, it is not something capricious,” she said. “It is very thoughtful.”

A point of contention with the Cheviot Hills cameras is that the neighborhood’s donation to the foundation bypasses the city’s regular procurement policy, which

requires a bid process and vetting of vendors.

In a statement, the Cheviot Hills Homeowners Assn. said it preferred Flock “due to their stellar reputation and strong recommendation from the experts we consulted with.”

Cindy Kane, who sits on the neighborhood association’s board, said residents conferred with police, their local City Council office and other neighborhood associations before making their pick. One factor, Kane said, was that Beverlywood and other nearby communities had already signed deals with Flock.

“The board discussed the privacy issues versus being proactive to address the crime, and that far outweighed the concerns of privacy issues,” she said. “We also determined that working with the Police Foundation was the most effective and efficient way to secure donations from our residents that could be earmarked for this purpose.”

LAPD data shows burglaries in Cheviot Hills doubled from 22 in 2023 to 45 in 2023, but other types of crime in the neighborhood are low compared to the rest of the city.



CALIFORNIA

Mayor and LAPD chief tout double-digit drop in homicides compared with last year

Dec. 10, 2024

The public perception that crime is spiraling out of control — even as statistics show many cities are the [safest](#) they have been in decades — is one factor for why [license plate readers have proliferated](#) across the country.

Civil liberties groups, activists and some academics have called on more states to tighten regulations on the technology, citing concerns about over-policing in communities of color, among other issues.

False positives — where police wrongly identify a suspect based on a vehicle — are a risk, especially since records in the stolen car database are sometimes out of date. There is also worry about the security of the captured data, and [who has access to it](#).

The LAPD's lack of a formal data-sharing agreement with Flock opens the door for federal authorities to potentially request information from the company about an immigrant's whereabouts — undercutting the city's promise not to cooperate in the Trump administration's mass deportation campaign, warned Tiff Guerra, an organizer with the activist group Stop LAPD Spying.



CALIFORNIA

LAPD chief ousts lawyer blamed by union for disclosing thousands of officer photos

April 1, 2025

The group's members and other critics routinely attend commission meetings and decry the department's growing arsenal of predictive policing software, facial recognition and other technologies.

Putting plate readers in Cheviot Hills seems designed to further alienate wealthy communities from Blacks and Latinos, according to Guerra.

“It raises questions, like, who gets surveilled? Who has the ability to pay for that surveillance and who's able to pay for these digital surveillance rings around their communities?” Guerra said.

But whether the plate readers are placed in South L.A. or wealthier areas, police officials say concerns about mass tracking of motorists are overblown.

LAPD Det. Alan Hamilton, who runs the LAPD's detective bureau, said the department already has its hands full trying to solve crimes — there's simply not enough time or

manpower to start acting like Big Brother.

“My detectives are too busy just trying to keep up with the Joneses,” Hamilton said.

More to Read

Push to install license plate readers comes amid questions about how data are shared

June 9, 2026



Inside the Police Commission's fight to retain its civilian oversight role amid LAPD defiance

June 6, 2026



An LAPD gang? Internal report says police unit had 'rampant culture of misconduct'

June 4, 2026



Sign up for Essential California

The most important California stories and recommendations in your inbox every morning.

Sign Me Up



Libor Jany

Libor Jany covers the Los Angeles Police Department. Before joining the Los Angeles Times in 2022, he covered public safety for the Star Tribune in Minneapolis. A St.

Paul, Minn., native, Jany studied communications at Mississippi State University.

Copyright © 2026, Los Angeles Times | [Terms of Service](#) | [Privacy Policy](#) | [CA Notice of Collection](#) | [Do Not Sell or Share My Personal Information](#)

Technology sector

New AI espionage powers trigger Putin camera scare

Russia paused surveillance system after killing of Iran's Supreme Leader exposed how AI can be used on CCTV data to target enemies



Mehul Srivastava in London and **Christopher Miller** in Kyiv

Published YESTERDAY

Russia's security services shut parts of a special surveillance system protecting President Vladimir Putin and his closest aides in the wake of Ayatollah Ali Khamenei's assassination in Tehran, according to two people familiar with the matter.

The system — which is separate from the nearly 300,000 cameras that surveil Moscow's citizens — was only turned back on after engineers combed through it in an attempt to hermetically seal it off from the internet, said one of the people.

The extraordinary precautions were taken after Israeli intelligence harvested vast amounts of video footage from Iran's traffic cameras to help pinpoint the exact location and timing of a February 28 meeting between Khamenei and his closest aides. Several top security officials were killed at the meeting in the opening salvo of the joint US-Israel war on the Islamic republic.

The assassination was a dramatic demonstration of a nascent technological leap: the use of artificial intelligence to parse through millions of hours of video, collected by thousands of cameras, in order to find and surveil targets.





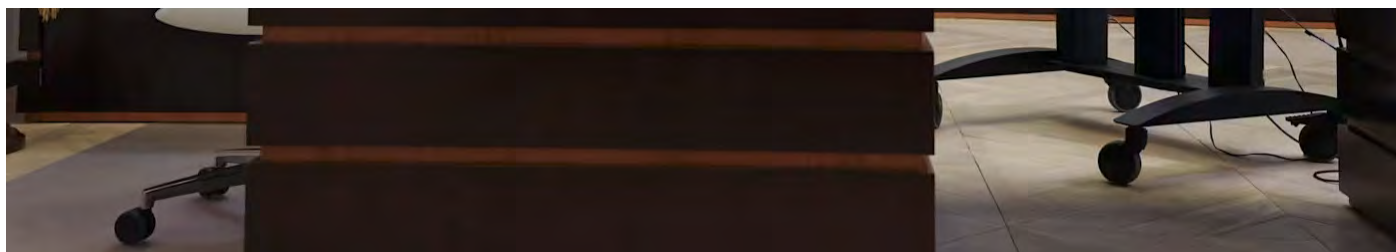
A video grab image taken from footage released by the Israeli military on March 1 shows what it says are large-scale strikes on 'the headquarters of the Iranian terror regime' in Tehran © Israeli Army/AFP/Getty Images

Dmitry Peskov, Putin's spokesman, did not respond to a request for comment. But the director of Russia's FSB, Alexander Bortnikov, cautioned regional security chiefs last week that Russia's vast surveillance apparatus had become a vulnerability — turning the authoritarian regime's tools to monitor its own citizens into a weakness its enemies could exploit.

"The recent elimination of senior Iranian officials by the US-Israel alliance is a clear warning sign," he said on May 26, according to Russian state news agencies. "The victims' locations were identified, in part, through software 'backdoors' in Tehran's video surveillance systems."

Governments have long known that security cameras can be penetrated with ease by experienced hackers or spies such as Israel's elite signals intelligence units. But advances in AI in recent years have enabled them to pinpoint specific behaviours and patterns in the vast visual data sets that result.





The Russians already had major concerns about Putin's personal safety, especially the risk from Ukraine's intelligence services © Alexander Kazakov/AFP/Getty Images

Israel's intelligence officers leveraged these advances to map out the complex geography of Tehran, find patterns of behaviour among the bodyguards of senior officials, and efficiently isolate targets from millions of hours of footage from thousands of cameras. They combined the information with other intelligence streams, including from human sources.

The visual capabilities of AI technology became far more powerful around 2023 and took a further leap about a year ago, said several people familiar with the complex maths behind it. It is orders of magnitude more sophisticated than the so-called machine learning algorithms that enable facial recognition, gun detection or the tracking of vehicles by make or number plate.

In contrast with older tools restricted to a few dozen preset searches, these new tools allow an almost unlimited range of enquiries by enabling language-based searches on video.

That lets intelligence officers hunt through massive streams of videos using simple search terms, such as two men handing a bag to each other; a person who has changed their appearance, or has changed clothes multiple times in a day; or a vehicle that has recently been painted over, or has driven past the same spot several times in a short period.

“This is the holy grail of surveillance,” said a European official whose country uses the technology on its cities. “We are able to look for behaviour, not objects — it has created a world of new possibilities.”

Interviews with nearly a dozen people, including former and current intelligence officers and senior security officials in four countries, revealed alarm at this new capability. It de facto transforms the billions of dollars spent on CCTV systems — especially traffic cams — into a keyhole through which their adversaries can scan vast cities and secure facilities to extract patterns and secrets at an industrial scale.

Once an individual subject is identified, these systems can rapidly build dossiers of their activities spanning months. That helps to recreate not just their own patterns of life but those of the people they interact with.

Such systems can pull in information not just from CCTV, but also from social media, hacked communications, audio picked up by microphones in smart devices and travel histories.

“To put it in simple words, this is the first time in history that we can communicate using language with computers about what they see,” said Matan Goldner, chief executive of a 15-person Tel Aviv-based start-up called Conntour, whose clients include Israeli intelligence and Singapore’s home affairs ministry.

“The capability of simply watching enemies’ sources is not unique or new — but to be able to get the exact moment that you’re looking for in time over thousands of hours, over thousands of feeds, that’s something really, really new in our world,” he said.

The idea that a country’s own surveillance system could be so efficiently and completely turned against it by its enemies has alarmed counter-intelligence officers around the world.

Their initial reaction was to try and close off vulnerabilities in camera systems themselves, a notoriously difficult task given the many generations of cameras that make up the intricate patchwork of most surveillance networks.

In India, the government set a hard deadline of April 1 — a month after the [FT reported the Israeli hack of Tehran’s camera system](#) — for Chinese cameras to be banned from the country.

Indeed, the Iranians themselves were able to hack security cameras in Israel, according to people familiar with the matter. But without the ability to digest the continuous stream of images, the utility of those hacks was limited.

The Russians already had [major concerns](#) about Putin’s personal safety, especially the risk from Ukraine’s intelligence services, who have penetrated traffic cameras in Russia. They

have also used cell phone location data to aid in assassinations of senior Russian military officials in the heart of Moscow.



Russian investigators suspect that Ukrainian secret services were behind the car bomb attack that killed Lieutenant General Fani Sarvarov in December 2025 © Anastasia Barashkova/Reuters

Despite Russia's precautions, one independent Ukrainian hacker told the FT that cameras in Moscow, and even around the Kremlin, "are still working and regularly hacked". He declined to say if Ukraine had the capability to analyse them at scale.

The US and the UK, which have access to such tools, have provided the Ukrainian military with precise targeting information in the past, including intelligence based on high-resolution images from surveillance drones.

China is starting to use this technology to sharpen its surveillance. The FT has [reported](#) on procurement data that shows China is investing in new generations of AI-enabled cameras and software that can interpret scenes, identify patterns of behaviour and retrieve footage using written prompts.

But those advances also create more opportunities for China's rivals to peek efficiently

inside its borders. A security official in a nation in the “Five Eyes” intelligence alliance said: “They’re the ones putting the cameras up — all we have to do is find a way in. And there is always a way in.”

The earliest working iteration of these analytical tools that the FT could find dates back to around 2023, about the time commercially available AI started being able to generate videos from text commands.

The reverse of that technology — using text to search through video — supercharged the ability to hunt through streams of data collected by the cameras that are omnipresent in modern life.

During December 2025 protests in Iran, the regime installed new video cameras to monitor the crowds, said a person familiar with the situation.

Israel was able to hack those new video streams in real time, said a regional official familiar with the matter, providing valuable insights into the membership of the [Basij, a paramilitary force that the regime uses for security](#).

In March, when the Basij set up checkpoints during the war, Israel could identify them, even though many members stopped wearing their distinctive — if unofficial — camouflage jackets.





Iranian protesters gather around burning cars in Tehran, in January. The regime installed cameras to monitor the crowds © Aghasht / Middle East Images/AFP/Getty Images

This was possible through streams of data collected from dash and traffic cams, car registration numbers and patterns of movement at checkpoints collected from drones, said a person familiar with the operation.

Airis, a Washington-based company that includes veterans of Israeli signals intelligence units, sells a system that can identify, and then track, people who display behaviour matching that of smugglers or cartel members — such as large nylon bags being carried at night or armed men with specific badges or tattoos.

Within just the past year, deploying AI on the various streams of data, including that scraped from social media, has “shortened the time to do this sort of work from days to minutes,” said Rotem Abeles, a co-founder of Airis. “That’s the order of magnitude of improvement.”

Such techniques are not infallible, however. Countries applying AI to surveillance face enemies — especially among non-state actors such as militant groups Hizbollah and Hamas — with low-tech measures such as handwritten messages and old analogue phone lines.

During the war in Gaza, Israel’s most sophisticated so-called “interception, surveillance and reconnaissance” systems failed to locate the Hamas chief, [Yahya Sinwar](#), architect of the October 7, 2023 attacks.





The IDF, outlining how Yahya Sinwar was located and killed, said he was spotted by chance by its forces in the Rafah area in southern Gaza © IDF/AP

Israel and its allies devoted vast resources to finding him, including “gait analysis” to try to pick out the tall, lanky man’s long stride in crowds. Instead, he was killed in October 2024 in what the military described as a chance encounter.

In his final moments, captured by a drone that failed to recognise him, Sinwar was wearing goggles and a tightly wound scarf that covered his distinctive ears — a low-tech foil to Israel’s high-tech hunt.

[Copyright](#) The Financial Times Limited 2026. All rights reserved.

Follow the topics in this article

Technology sector

FT Edit

Vladimir Putin

Mehul Srivastava

Christopher Miller