

2026 City Council Candidate Questions

Surveillance Technology

What principles should govern Palo Alto's use of surveillance technology? Discuss where you would draw the line between legitimate public-safety tools and unacceptable government surveillance, and what oversight, transparency, warrant, retention and data-sharing rules do you believe should apply?

BRYNA CHANG

The principles I would apply are:

- **Proportionality:** Surveillance tools should be proportionate to the safety benefit they provide
- **Transparency:** The public should know what tools the city uses, what data is collected, how long it is retained, and who can access it
- **Oversight:** Any surveillance technology should require council approval and be subject to regular public reporting and audit
- **Data minimization:** Collect only what is necessary. I would support strict ALPR data retention limits — likely 30 days (as is already PAPD policy) or less for data not associated with an active investigation
- **No unauthorized sharing:** Palo Alto data should not be shared with federal immigration authorities or other agencies without a warrant, consistent with California law; in addition, PAPD's policy already requires that data cannot be shared with other California cities unless they sign an agreement to abide by Palo Alto's policies.
- **Warrant requirements:** Law enforcement access to retained surveillance data should require a warrant or documented exigent circumstances.

In the Flock debate, I take seriously the legitimate concerns on both sides: protecting residents' privacy while giving our police effective tools to investigate crime and apprehend dangerous offenders.

Flock has faced serious concerns over the sharing of license-plate data with federal agencies in violation of state law and local policies, as well as misleading statements from company leadership. In addition, Palo Alto license-plate data is searched up to 200,000 times a month by Northern California law-enforcement agencies, far more than appears necessary to investigate serious crime. I believe stronger privacy protections are needed.

At the same time, automatic license-plate readers have proven valuable in solving crimes and identifying repeat and dangerous offenders. Police Chief James Reifschneider told the Council in June that the department had identified more than 130 cases in which Flock played an important evidentiary role in identifying and arresting suspects. I support exploring alternatives, including the Genetec system, which was recently adopted by Stanford. Genetec lacks some of Flock's regional data-sharing benefits, but allows data to be stored locally under greater agency control.

Public safety is extremely important to Palo Alto residents, and I support giving our police the tools they need to fight crime effectively and cost-effectively while establishing strong safeguards against misuse of residents' data.

I will continue listening to both sides as we work toward the right balance between protecting privacy and reducing crime.

In the near term we should:

- 1) Limit how outside-agency searches can be limited, as narrowly as practicable, to felonies, sex crimes, and narrowly defined crimes of regional concern, such as organized retail theft. The police auditor is investigating this.
- 2) Review prohibiting PAPD from searching historical travel data for traffic citations, infractions, other low-level offenses, and exploratory use.

3) Reduce the data retention time from 30 days to 7 in line with Flock's new default retention period for new customers. The police auditor is investigating this.

4) Evaluate Genetec (used by Stanford) and other vendors who can provide a more secure data architecture and more accurate license plate readers with less false positives. The police auditor is doing this. We should not switch before a thorough evaluation is fully completed and the audit is completed and only then if the evaluation shows an alternative to be effective at both increased privacy protections and helping PAPD with crime fighting both with real-time alerts and investigations.

YUDY DENG

My experience serving on the Police Foundation board and talking directly with our officers has given me valuable insight into how technology like automated license plate readers can help solve crimes. When used properly, these tools can give officers information much faster and help them identify vehicles connected to serious crimes.

At the same time, as an immigrant and a mother of two, protecting privacy and civil liberties is very important to me. I don't want technology that helps keep us safe to become a system that unnecessarily tracks where innocent people go.

My principle is simple: technology should be used to investigate crime, not to monitor everyday life.

That means surveillance tools should have a clearly defined public-safety purpose, strict limits on access, short data-retention periods, and strong restrictions on data sharing. Every search should be logged and auditable. Access should be tied to a legitimate law-enforcement purpose, with a warrant or other appropriate legal process where required by law. The City should regularly report to the public how the technology is being used, how often it contributes to investigations, who has access to the data, and whether there have been any violations of the policy.

I would draw a clear line against broad facial recognition, indiscriminate mass location tracking, or creating a permanent database of people's movements simply because they are going about their daily lives.

I also have concerns about relying on a vendor like Flock to control sensitive data. Stanford recently moved away from Flock to a system where its license-plate data is transferred to a server Stanford exclusively controls. That tells me we should examine our options as well. The question isn't just whether ALPR technology works; it's whether we can achieve the same public-safety benefit with stronger privacy protections.

And no technology should get a permanent blank check. We should periodically evaluate whether it is actually reducing crime and helping investigations. If the benefits don't justify the privacy risks, we should change the technology, change the vendor, or stop using it.

We're Silicon Valley. We should be able to use technology to make people safer while setting one of the highest standards in the country for privacy, transparency, and accountability.

HENRY ETZKOWITZ

Did not answer.

GARY GECHLIK

I am for protecting human life above all. Flock cameras fit into that equation. These cameras save lives and are the only way to bring the crime down in Palo Alto to the level of Saratoga and Los Gatos. If you want to live with less crime, you have to accept that remote monitoring is part of the future of crime control.

RAYMOND LEE GOINS

I oppose any form of mass surveillance. It gives our community a false sense of security, and our civil liberties should not be violated. We should not treat our city like it's a business, with security cameras everywhere.

BRIAN HAMACHEK

I oppose an automated license plate reader network that routinely records the movements of people who are not suspected of wrongdoing.

I support targeted investigations, adequate police resources, and technology tied to a specific public-safety need. I oppose indiscriminate data collection that allows people's movements to be reconstructed later.

ED LAUING

Flock failed its customers and the citizens of many cities with their policies and software flaws. They need to go.

This tool for solving crimes is highly valued by our police department who have many positive results for ALPR. And, in general, I am highly supportive of our police dept. But we will have to re-start a review of other possible vendors to see IF there is one with fail-safe software we can trust. As of now, I don't know of a valid alternative.

VICKI VEENKER

All uses of this type of technology require a legitimate law enforcement purpose. I draw the line at facial recognition which I do not think we should use, but if we can get comfortable with ALPRs, the safety benefits may outweigh the privacy concerns.

If the City is to maintain use of ALPRs,

1) use should be frequently (at least monthly), regularly, and thoroughly audited. We should review use both via random sampling and any instances flagged for suspicious behavior, such as repeated queries of the same plate by the same user;

2) the audit should verify that the vendor and anyone with access only uses it for a legitimate law enforcement purpose linked to a specific police report, case file, charge and user;

3) verify on-schedule data deletion;

4) only share with Bay Area jurisdictions with similar or more stringent audit and other access protocols; we need reciprocal agreements to the same terms with any other agency before sharing with them; and

5) maintain a small number of cameras located only on major high-traffic thoroughfares and not in neighborhoods.

We are awaiting the Independent Police Auditor's report on whether vendors can meet the above requirements, our high expectations of deterrence of abuse, and rapid identification of any abuse.

Also, based on what I've seen, I believe we should discontinue use of Flock.