

“Stop Flock” Campaign Lesson Learned #3: What “mass surveillance” actually is, and how it is used against community members.

Supporters of surveillance commonly make these arguments:

- We are already being surveilled constantly by our own phones and computers, our “smart speakers,” even our cars. Therefore, why should we worry about police cameras on the street?
- What is the harm in capturing and sharing just one piece of information, such as a license plate?

It is true that surveillance is all around us, using our own personal technology against us to steal our private information. Community-based organizations provide helpful suggestions on how to minimize the flow of our personal data to both big business and the government.

But this web of spying by business is no argument for allowing our local governments to do the same. Adding on more surveillance only makes the problem worse—much worse, because the government has the ability to take away our freedom.

In fact, the Trump administration has sped up the collaboration between the federal government and Big Tech. This is particularly true with Artificial Intelligence (AI). The feds have invested billions of dollars in infrastructure and technology, and are adopting AI for military uses and across the entire federal workforce.

Garbage In, Bias Out

The [Brookings Institution reported in October 2025](#) that the administration was rapidly centralizing vast amounts of data into a shared repository, complying with an executive order to eliminate “information silos.”

According to Wired, DOGE (the so-called Department of Government Efficiency, formerly run by Elon Musk) [“intends to integrate data from agencies](#) such as the Social Security Administration (SSA) and the Internal Revenue Service (IRS) into USCIS’s ‘data lake,’ which contains information on immigration cases.” CIS is the Citizenship and Immigration Service, a sister organization to ICE and CBP within Homeland Security.

Brookings’ report explains that Palantir, a data analytics and technology firm, has won over \$900 million from the administration for projects such [ImmigrationOS](#), a sophisticated system to prioritize people for deportation.

<https://www.americanimmigrationcouncil.org/blog/ice-immigrationos-palantir-ai-track-immigrants/> that “Palantir’s systems pull data from [across government](#)

[databases](#)—regardless of the veracity or accuracy of those databases—including passport records, Social Security files, IRS tax data, and even license-plate reader data. The goal is to create a comprehensive, AI-driven profile of individuals that agencies can use to make faster and more efficient enforcement decisions.”

One Berkeley city council member promised community members, “I will stop supporting Flock if you can show me an example of ICE deporting an immigrant based on information that came from Flock providing Berkeley’s data about them.” But this is not how intelligence-gathering works, whether it is for legitimate investigations, or Trump’s massive assault against immigrants and dissenters.

Intelligence-gathering works by looking at many pieces of information. It requires recognizing patterns in the information, understanding their context, and confirming information from multiple sources.

A spy on a computer chip

The article “[Putting Intelligence in Intelligence Sharing](#),” by the Center for Strategic and International Studies (CSIS), describes intelligence sharing as “the fusion of multiple formats from multiple sources that are analyzed to provide context and direction in an accurate and timely fashion.”

And, especially in the era of AI, no one may ever know the actual piece of information that was “actionable.”

When fighting a virulent epidemic, for example, a broad form of information gathering may be essential. Public health workers even call it “surveillance.”

But the federal government itself is a pathology in the body politic. Persecution of enemies based on their political beliefs and social media is totalitarian, meaning that it criminalizes those who do not support the official MAGA ideology.

Berkeley itself is considering a version of what Palantir is building on the national level. Flock Nova is one of the tools that the police department is asking Berkeley to buy.

Nova was just released in 2025. It is designed to “supplement the ALPR data with people-lookup tools, data brokers, and data breaches to ‘jump from LPR to person,’” according to [404 Media](#).

“According to Matthew Guariglia, senior policy analyst for the civil liberties group [Electronic Frontier Foundation](#), this new controversy could [foreshadow a dim future when it comes to law enforcement](#).

“We’ve often warned that data from automated license plate readers — already a digital dragnet that captures information about millions of people who’ve committed no

crimes — could be combined with other data streams to further invade people's privacy,” he told *Government Technology* via email. “If the reports about Flock Nova are true, this is precisely the kind of dystopian panopticon we’ve warned about.” [The panopticon, literally meaning “all-seeing,” is a conceptual prison design dating to the 18th century in which all prisoners are subject to constant surveillance. George Orwell’s novel *1984* was a supreme example of a modern panopticon using technology and encouraging civilians to spy on each other. — Ed.]

Guariglia goes on, “An officer having someone's entire online persona one click away after a license plate reader scans their plate is an open invitation for police retribution and reprisals based on a person’s First Amendment-protected expression and affiliations.”

What is this world coming to?

For a clear and comprehensive article on the threats posed by developments in the Flock “ecosystem” of surveillance, see the ACLU’s [“Flock’s Aggressive Expansions Go Far Beyond Simple Driver Surveillance”](#), published in August 2025. The ACLU cites a May 2025 [article by 404 Media](#) detailing use of data by brokers such as parking payment apps and credit bureaus. These two articles reveal how the technologies allow police officers to violate the Fourth Amendment and the Privacy Act without the requirement of a warrant, and at the push of a button.

The ACLU adds that “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.’

“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 [to stop] crime, but to protect the bottom line.”

One other piece of software bundled in with ALPRs and the other Flock systems is the Real-Time Information Center (RTIC).

The [Police Accountability Board \(PAB\) explained](#) that the RTIC system “integrates live and historical data from multiple surveillance sources into a unified operational dashboard used by law enforcement for active incident monitoring and investigation. [It] would consolidate Berkeley’s automatic license plate readers (ALPRs), fixed cameras, drone feeds, and community video streams under a single vendor-controlled interface.”

In other words, it operates like Flock Nova, but within the Flock’s surveillance ecosystem. Police may love these tools for their “push of a button” ease of use, but that same ease frightens community members for its potential for abuse.

The *404 Media* article concludes with a quote from the ACLU's Jay Stanley:

“At this moment in history, of all times, you especially don't want to be building authoritarian spying structures for law enforcement. People are being literally put behind bars for writing an op-ed,’ referring to Tufts student Rümeysa Öztürk. Öztürk was released earlier this month after spending six weeks in detention.

“Civil rights groups are increasingly worried that ICE for example could turn to similar surveillance technology as part of its mass deportation efforts.”