**SURVEILLANCE TOOLKIT: SAMPLE OP-EDS**

# Why Santa Clara County needs a surveillance transparency ordinance

*By George Cammarotal, San Jose Resident & Community Organizer*

Stingrays, Hailstorms, Triggerfishes, FLIRs, Amberjacks, NGI, Harpoons and ALPRS are not exactly household names to most Santa Clara County residents. The names sound like something out of “Moby Dick” meets a science fiction novel. But these pieces of high-tech surveillance equipment and more like them are being used now by local law enforcement, often without public knowledge, input or consent.

That is why Santa Clara County’s Board of Supervisors is considering a global surveillance equipment transparency ordinance. The proposed legislation covers all surveillance technology from cellphone interceptors to license plate readers to facial recognition software to those not invented yet. It dictates a cost-benefit analysis prior to purchase and a proposed usage policy — vetted in a public forum — and after purchase, an annual use audit to provide real data in real time.

High-tech gadgets can be useful tools in the investigation of crimes. But they can also be expensive boondoggles that rarely get used. Or worse, they can be used inappropriately and generate costly lawsuits and unjust outcomes.

This isn’t just a theoretical worry. A 2012 audit of National Security Agency intelligence operations documented 2,776 privacy violations in just one year, including a dozen incidents dubbed “LOVEINT” — meaning the use of the agency’s formidable surveillance apparatus to stalk current or former love interests of NSA staffers.

Policing is not exempt from the racial divides that cross this country. Profiling and targeting can and have been applied disproportionately to certain groups including African-Americans, Latinos, religious groups, young people and those marching in the street for redress of grievances.

As people become aware of the billions in federal funding and the extensive equipment provided directly to law enforcement for surveillance, they want to know when and why it is being considered, what it is intended to do, and what are the real costs before being deployed. They also want rules to ensure proper use, oversight, accountability and safeguards for individual rights.

Gov. Jerry Brown heeded that call in 2015, signing into law three bills that increased surveillance transparency: SB 178 (email privacy), SB 741 (cellphone interceptors) and SB 34 (license plate data usage). But new innovations in technology race ahead faster than equipment-specific legislation can possibly keep up with.

It’s understandable that some sectors of law enforcement have hesitated to embrace the ordinance wholeheartedly. They want to use every tool they can to do their job. But communities increasingly understand the need to ensure that time, energy and resources are not spent on systems that cost more and do less.

The county Finance and Government Operations Committee will review the surveillance transparency ordinance on April 14 at 3 p.m. at 70 West Hedding St. in San Jose. The meeting is open to the public and will have a comment period.

A lack of defined policies opens the door for mistakes, overreaches and even abuses, which thrive in the lack of established use policies. These mistakes create mistrust between law enforcement and residents, especially in communities where crime rates are higher — that are often most surveilled. Such mistrust makes community policing harder, as beat cops must depend on relationships within neighborhoods to get information and investigate and prevent crimes.

Following the public outcry about NSA warrant-less spying and the use of paramilitary equipment by local police, community members deserve reassurance that safeguards and public oversight will be in place if surveillance equipment is going to be used.

It's plain good government.

## Why facial recognition is a threat to civil liberties

*By Christie Hill, Deputy Advocacy Director, ACLU of San Diego and Imperial Counties*

Protecting the freedoms that define America means making smart choices about surveillance and public safety in the 21st century. We're living in an age when machines can collect information about nearly everything we do — from the places we go to the emotions we feel to the people we hang out with — and have the capability to transmit this data to each other and to our government.

When nearly any device can be turned into a hyper-powerful surveillance tool, it's up to us to ensure technology makes us more, not less, safe. That's why we're gravely concerned about the invasive use of facial recognition software in police body cameras.

California state senators will soon vote on a bill to halt this practice. Assembly Bill 1215, the Body Camera Accountability Act, is a sensible public safety measure that will ensure you can walk down the street, attend a protest or ask police for help without having your face automatically scanned and recorded by the government.

In a free country, you don't have to identify yourself to every officer you pass on the street. Face-scanning body cameras would force you to do just that. Facial recognition software is now capable of analyzing live streaming video and identifying, tracking and cataloguing hundreds of people at once. If even a fraction of the estimated 67,200 local law enforcement officers in California were equipped with face-scanning body cameras, it will create a vast, roaming surveillance network that poses an immediate threat to our civil liberties and most fundamental freedoms.

When it comes to facial recognition software, the stakes couldn't be higher. Body cameras and facial recognition simply should not mix.

Top corporate players agree: Facial recognition is incompatible with police body cameras. Axon, the largest maker of police body cameras, recently announced that police should not use its cameras with facial recognition technology after examining the ethical issues such use would raise. Microsoft, a leading purveyor of facial recognition software, has also refused to provide facial recognition for police body cameras in California, recognizing the radical threat to civil rights such systems would pose.

When companies that stand to make huge profits off the marriage of these technologies can't bring themselves to do it, you know it's a bad idea.

As if the threat to our civil liberties isn't enough, facial recognition is inaccurate and racially biased. Study after study has proven that facial recognition software is dangerously likely to misidentify people with darker skin, especially black women. A widely publicized face recognition test recently misidentified 26 California legislators as arrestees in a mugshot database. More than half of them were legislators of color.

In the real world, misidentifications lead to wrongful stops, arrests and deadly use of force. We can't risk these kinds of mistakes. Instead of placing our faith in flawed technology, we must explore and adopt more humane approaches to public safety.

Even if facial recognition was perfectly accurate, if we allow body cameras to be used to track the public, other law enforcement agencies could begin mining the data. California is home to millions of immigrants and refugees from all over the world. And we already know the U.S. Immigration and Customs Enforcement has sought to use facial recognition to identify immigrants.

Those opposed to Assembly Bill 1215 call facial recognition a tool, but this description couldn't be less true when it comes to body cameras. It is reckless to use the public as test subjects with facial recognition-enabled police body cameras — and even to arrest people — when experts have concluded the technology is inaccurate and biased, when the largest body camera maker has announced it has no place on body cameras, and when we know ICE may demand access to body camera databases to target and deport Californians.

Adding facial recognition to body cameras will not only threaten our civil rights, it will undermine the public safety benefits of body cameras, which were only to be used to ensure police accountability. Indeed, 62 percent of likely 2020 California voters — across political parties and regions — strongly agree that body cameras should be used solely for oversight and accountability and not to track and identify people.

We shouldn't allow police to use technology that will make us less safe. Will body cameras that promised to increase public trust in police now be turned against our communities and used to violate our privacy and fundamental freedoms? It's up to us.

In a free country, you don't have to identify yourself to every officer you pass on the street. Face-scanning body cameras would force you to do just that.

# New surveillance oversight law keeps communities safe and redefines tech leadership

*Technology should work for the public good, not against it.*

*By Matt Cagle and Brian Hofer*

Technology should work for the public good, not against it. Yet, San Francisco's city departments are currently permitted to use invasive, high-tech surveillance systems without consulting with residents or setting up basic rules to keep us safe. The harms that technologies like drones, automatic license plate readers, and face recognition can inflict are real and will fall hardest on our already-marginalized community members.

Next week, San Francisco's Board of Supervisors will vote on a law, authored by Supervisor Aaron Peskin, that ensures surveillance technology is considered and used responsibly by requiring public debate, clear use policies and a final Board vote. The ordinance also specifically prevents the city from deploying face surveillance technology.

The legislation is supported by the ACLU and a broad coalition representing immigrants, people of color, the homeless, the LGBTQ community, and others who are most subject to abusive surveillance. San Franciscans should ask their supervisors to pass this law.

Opponents of the legislation say that democratic oversight is impractical and would stop residents from sharing information with the city. But this process works – six other Northern California localities have adopted similar laws. And the ordinance explicitly allows city departments to accept and use tips from the community.

San Franciscans have experienced the danger of hastily deployed surveillance firsthand.

For instance, SFPD pulled over Denise Green, a Black woman, when a patrol car's automated license plate reader mistakenly indicated that her car was stolen. License plate readers are known to have a 10 percent error rate, but there were no policies requiring officers to verify automated readings. The police forced Ms. Green out of her car, to her knees, and held her at gunpoint.

Ms. Green's story demonstrates that unaccountable surveillance makes us less safe and less free. We know that surveillance technology is used most often against people of color and immigrants, who are, in turn, most in danger of racially biased violence.

This ordinance also recognizes the unprecedented dangers of face surveillance— a new technology that, as a New York Times experiment showed, exploits public camera feeds to secretly track people by scanning their faces against photo databases.

Experts have warned face recognition is inaccurate for people of color and women. But even if it were completely accurate, the city should still reject it.

Face surveillance is incompatible with a healthy democracy. In China, it's already being used to profile and control a largely Muslim ethnic minority. In one Chinese city, a once-bustling public square became desolate after this technology was installed.

If unleashed, face surveillance would suppress civic engagement, compound discriminatory policing, and fundamentally change how we exist in public spaces.

A young adult should have confidence that the city isn't logging their first visit to a gay bar. A Muslim resident should not worry their visit to a mosque will place them on a watchlist. And an immigrant should be able to show their face in public without fear of deportation.

Modern technology gives the government unprecedented surveillance powers. To put things in perspective: in 1973, the SFPD possessed intelligence files on over 100,000 people, including civil rights demonstrators, union members, and anti-war activists. These records took decades to amass.

Today, city police can stockpile information on 100,000 residents in a few hours.

The legislation before the Board brings these systems out of the shadows with a simple process of public accountability that also ensures that San Francisco lives up to its sanctuary promise. Indeed, a recent ACLU report found that the Trump administration is trying to use data from local surveillance systems to locate and deport immigrants.

An overwhelming majority of Bay Area voters support laws requiring oversight and transparency of government surveillance and oppose the government's use of face recognition.

San Francisco sits at the center of innovation; by passing this law, the Board of Supervisors can redefine what tech leadership means.

SPEAK UP Ask your supervisor to support the “Stop Secret Surveillance” ordinance by emailing Board.of.Supervisors@sfgov.org

Matt Cagle is a Technology and Civil Liberties Attorney at the ACLU of Northern California.
Brian Hofer is the Executive Director of Secure Justice.