

From: [Ellen Obstler](#)
To: [Brown, Steve](#)
Subject: [EXTERNAL] public comment for agenda item 7.1
Date: Tuesday, July 21, 2026 10:19:39 AM

Community advisory board members

I serve on Petaluma's public safety advisory committee which held community meetings last year and the start of this year about Flock license plate readers. Although the committee opted for now against recommending to the city council to take the readers down, comments from the community led the Petaluma Police Department to stop sharing data with the City of El Cajon, which the State has sued for violating state privacy laws and the Northern California Regional Intelligence Center, which the city and county of San Francisco cancelled its contracts with because of hundreds of improper searches of its database. As time has gone by, we're learning about more and more inappropriate data use and sharing from police stalking their exes, to tracking down women seeking abortions, to - most concerning in our area - providing information to ICE. The SF Chronicle recently published an op-ed warning about the perils of Flock entitled "Tech enables a surveillance state." The author wrote Flock cameras "'entrench[] a surveillance architecture that inverts one of the Fourth Amendment's core assumptions. Rather than requiring law enforcement to develop individualized suspicion before intruding on a person's privacy, automated license plate reader networks collect and retain everyone's movements, allowing officers to search those records for later suspicion, associations or investigative leads. What was once targeted surveillance has become persistent, suspicionless monitoring." https://edition.sfgchronicle.com/infinity/article_popover_share.aspx?guid=6a03ea16-1ecd-4f26-969d-472689326f73&share=true&fbclid=IwY2xjawTL8UNleHRuA2FlbQlxMQBzcnRjBmFwcF9pZBAyMjlwMzkxNzg4MjAwODkyAAEe2pAZh0_Z_JEOPSSAxhsSMpl50VrXAC6Z4eEpgvq9WAqSuMdLaSa0o6sdVts_aem_fgxveh4RHvuRdpV43x6k_Q

Flock cameras do not make the public safer; they do not prevent crimes from happening. They merely make it easier for police to find the people and property they're looking for. The question is at what cost? Is it worth it to violate all of our civil liberties? Is it worth it to even inadvertently expose vulnerable community members' whereabouts? Can we trust Flock, a company partially funded by Peter Theil's "Founders Fund," which also bankrolls Palanir, a sophisticated data surveillance tool used by ICE and Border Patrol to target migrants, to keep information safe?" I hope the City of Santa Rosa will reconsider using these cameras.

Thank you for your consideration.

Ellen Obstler

Dear CAB Members:

On July 22, you will receive a presentation by Santa Rosa Police Department (SRPD) Chief John Cregan on the City's use of Flock Automatic License Plate Readers (ALPR).

ALPRs are just one part of SRPD Chief John Cregan's uncontrolled and warrantless mass surveillance operation, the Real Time Crime Center (RTCC). RTCC was announced to the public in early 2024 "courtesy" of a nearly One Million Dollar Congressional earmark by Representative Mike Thompson at the behest of then Mayor Natalie Rogers (<https://www.pressdemocrat.com/2024/04/10/santa-rosa-police-to-ramp-up-surveillance-across-city-as-first-step-to-create-real-time-crime-center/>). At that time, local civil liberties groups including the American Civil Liberties Union (ACLU), the North Bay Organizing Project (NBOP), and the Sonoma County Commission on Human Rights (CHR) all expressed concerns about this new **uncontrolled and warrantless mass surveillance operation** (<https://www.pressdemocrat.com/2024/04/14/does-santa-rosa-polices-plan-to-boost-public-surveillance-cross-a-line-local-leaders-weigh-in-on-controversial-tech/>). In that article, SRPD Chief John Cregan told the reporter and said he would address the community concerns in an internal rule book for the technology. In 2025, I went back and forth over email with SRPD Chief John Cregan where he continued to allege that a policy for the RTCC would be forthcoming soon (see attached email thread). To date there is no publicly available written policy for the RTCC on SRPD's website. What is needed, and has been called for repeatedly (see attached letters from the ACLU to City Council) is a comprehensive Surveillance Technology Ordinance (STO). Even the Press Democrat called for one (<https://www.pressdemocrat.com/2024/04/17/pd-editorial-deploy-police-tech-but-ensure-oversight/>). Rather than passing an STO to protecting the privacy rights of community members who live, work, or visit the City of Santa Rosa, the Santa Rosa City Council has opted for willful ignorance

As for Flock ALPRs in Santa Rosa, if an adequate STO had been in place, these cameras would not be in place as they currently exist. SRPD's policy for ALPRs would be greatly improved and our contract with Flock would have much greater protections. Please compare SRPD's Policy 443 for ALPRs against the metrics for a sufficient surveillance technology use policy. To be clear a "Surveillance use policy" means a publicly released, legally enforceable written policy governing the City department's use of a specific surveillance technology that, at a minimum, includes all of the following:

1. *Purpose*. The specific purpose(s) that the surveillance technology item is intended to advance. **SRPD's language is not specific.**
2. *Authorized Use*. The uses that are authorized, and the rules and processes required prior to such use and uses of the surveillance technology that will be expressly prohibited. **As long as it is deemed "police business", SRPD appears to allow any use. No uses are expressly prohibited.**

3. *Data Collection.* What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology, what types of data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize and delete such data. **There is much debate over what data Flock actually collects.**

4. *Data Access.* The category of individuals who can access or use the collected information, how and under what circumstances data collected with surveillance technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information. **Sec 443.6 (a) seems to only document access by name, date and time; not the reasons or case numbers for that access. We also seem to track and audit who at SRPD accesses our Flock data, but not who from outside agencies accesses our Flock data and their purposes for accessing our data.**

5. *Data Protection.* The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. **Flock is notoriously "leaky" and data has been hacked. It is also regularly misused by problematic Law Enforcement Officers.**

6. *Data Retention.* The limited time period, if any, that information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the surveillance use policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

7. *Public Access.* How collected information can be accessed or used by members of the public, including criminal defendants.

8. *Third-Party Data Sharing.* Which governmental agencies, departments, bureaus, divisions, or units may receive data collected by the surveillance technology operated by the City department, including any required justification or legal standard necessary to share that data, and how it will ensure that any entity sharing or receiving such data complies with the surveillance use policy. **Instances of Flock data from California agencies making its way into the hands of DHS/ICE are ongoing.**

9. *Training.* The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

10. *Auditing and Oversight.* The mechanisms to ensure that the surveillance use policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record-keeping of the use of the technology or access the information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy. **We also seem to audit who at SRPD accesses our Flock data, but not who from outside agencies accesses our Flock data and their purposes for accessing our data.**

11. *Complaints.* What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the municipal entity will ensure each question and complaint is responded to in a timely manner.

It is extremely concerning to me that Sec. 443.4 (b) states that: "Reasonable suspicion or probable cause is not required before using an ALPR." I am not an attorney, but to me, this feels like a violation of our Federal and State Constitutional privacy rights.

I am requesting that your body agendaize a future discussion and action item on surveillance technologies in the City of Santa Rosa, with the purpose of recommending to the City Council that they finally implement an STO to put some guardrails on these out of control civil liberties violations.

Thank you for considering my request.

Respectfully,

Jim Duffy

--

Jim Duffy
NACOLE Certified Practitioner of Oversight (www.nacole.org)
he, him, his
94928jim@gmail.com
707-703-0694



Jim Duffy <94928jim@gmail.com>

Real Time Crime Center Policies

4 messages

Jim Duffy <94928jim@gmail.com>
To: "Cregan, John" <JCregan@srcity.org>

Tue, Jan 28, 2025 at 12:00 PM

Dear Chief Cregan:

At today's SRPSS meeting you said the policies for your Real Time Crime Center would be online soon.

Can you please tell me what date I should put on our calendar to look for this new policy?

Thank you.

Respectfully,

Jim Duffy

--

Jim Duffy
NACOLE Certified Practitioner of Oversight (www.nacole.org)
he, him, his
94928jim@gmail.com
707-703-0694

Cregan, John <JCregan@srcity.org>
To: Jim Duffy <94928jim@gmail.com>

Mon, Feb 3, 2025 at 10:14 AM

Jim,

Thanks for coming to the Public Safety Sub-Committee last week and providing input. We currently have dedicated policies for each of the equipment used in our RTCC including Public Surveillance System, ALPR, Drones, and Body Worn Cameras. My team is in the process of creating a Real Time Crime Center policy which will help provided holistic overview of all of the technology. My hope is to have the draft of the policy in March and have the policy finalized on our website by this spring.

John Cregan | Chief of Police

Santa Rosa Police Department

965 Sonoma Ave. | Santa Rosa, CA 95404

Tel. (707) 543-4070 | Fax (707) 543-3557 | jcregan@srcity.org

Facebook | Twitter | Instagram | Nextdoor | CivicReady



**SANTA ROSA
POLICE**

[Quoted text hidden]

Jim Duffy <94928jim@gmail.com>
To: "Cregan, John" <JCregan@srcity.org>

Thu, Aug 14, 2025 at 6:18 PM

Dear Chief Cregan,

Any update since Juneteenth on those written policies for the Real Time Crime Center? Did you have a chance to look at the AUTHORIZED POLICING TECHNOLOGY (APT) ACT from NYU Law that I sent to you on June 15?

Thanks!

Best Regards,

jim

[Quoted text hidden]

Cregan, John <JCregan@srcity.org>
To: Jim Duffy <94928jim@gmail.com>

Wed, Aug 20, 2025 at 3:33 PM

Jim,

Our team is examining the alternative ordinance that you provided. We are still building out our department policies to ensure that we meet the expectations of our community here in Santa Rosa. I will keep you updated on our progress.

[Quoted text hidden]

July 22, 2024

VIA ELECTRONIC MAIL

TO: Santa Rosa Public Safety Subcommittee

CC: Santa Rosa City Council (Mayor Natalie Rogers, Vice Mayor Mark Stapp, Council Member Eddie Alvarez, Council Member Dianna MacDonald, Council Member Victoria Fleming, Council Member Chris Rogers, Council Member Jeff Okrepkie)

CC: Chief John Cregan, Santa Rosa Police Department

Re: Item 6.2, Real Time Crime Center, Public Safety Subcommittee meeting on July 23, 2024

Dear Mayor Rogers and City Councilmembers:

On behalf of the Sonoma County Chapter of the ACLU of Northern California (“ACLU NorCal Sonoma County Chapter” or “our chapter” or “ACLU”), I submit public comments on agenda item 6.2, “Real Time Crime Center” of the Santa Rosa Public Safety Subcommittee meeting on July 23, 2024.

The Previous Meeting with Police Chief John Cregan

The Sonoma County Chapter of the ACLU of Northern California is writing this letter to express our opposition to the proposed Real Time Crime Center, and to object to a misrepresentation made by the Santa Rosa Police Department (“SRPD”) regarding the ACLU.

Chief Cregan’s Staff Report suggests that SRPD met with our organization in December 2023 to discuss the matter before you today; however, that meeting was actually about the ACLU-NorCal Sonoma County Chapter’s proposal for the city to adopt a Surveillance Technology and Community Safety Ordinance which would limit the exact type of Orwellian surveillance practices that a Real Time Crime Center (which **was not**

mentioned once at that meeting) would facilitate. When we met with him on December 5, Chief Cregan seemed receptive to our proposal, and indicated that we may have an opportunity to present a draft of our proposed Surveillance Technology and Community Safety Ordinance at the July Public Safety Subcommittee meeting. Instead, on the agenda before you is the polar opposite, and we staunchly oppose establishment of a vast citywide surveillance network in the Real Time Crime Center. We object to any impression that the ACLU was consulted about the Real Time Crime Center.

Establishment of the Real Time Crime Center

We recognize your responsibility as elected leaders to maintain safety in our community. However, we have serious concerns with plans to utilize a wide range of surveillance technologies as part of the Real Time Crime Center.

The evidence is clear that while surveillance has increased exponentially, public safety has not. On the contrary, surveillance systems often make people less safe, especially for groups that have historically been in the government's crosshairs. Modern surveillance technology makes it possible for the government to track who we are, where we go, what we do, and who we know. It fuels hightech profiling and perpetuates systems of biased policing. It facilitates deportations, chills speech, and imperils the rights of activists, religious minorities, and people who need reproductive and gender-affirming care.¹

Surveillance systems fuel racial injustice. In a nation where police interactions with the public all too frequently turn dangerous, surveillance systems can exacerbate and magnify these problems, increasing the risk of unnecessary government scrutiny, in-person encounters, and violence. Again and again, police have used surveillance systems to create inaccurate and discriminatory watchlists, engage in discriminatory stops and searches, and upend people's lives. Surveillance technologies amplify the over-policing of Black and Brown communities.

Surveillance endangers immigrant communities, and this fact should be of particular concern for us in Santa Rosa. Across the United States, federal immigration agencies

¹ We encourage you to read the ACLU's new report, "SEEING SURVEILLANCE: THROUGH WHY POLICYMAKERS SHOULD LOOK PAST THE HYPE," available at https://www.aclunc.org/sites/default/files/Seeing_Through_Surveillance__Report_Web.pdf.

have eagerly exploited local databases rich with information collected by private data brokers, municipal agencies, and police departments. This information is fed into a deportation machine that tears apart immigrant communities. In recent years, Immigration and Customs Enforcement (ICE) has further expanded its reach into communities by exploiting local surveillance systems and databases to track, identify, and target immigrant community members for detention and deportation. No local surveillance system is safe from ICE's demands.

Surveillance is frequently ineffective and can lead to life-altering mistakes. Surveillance technology may malfunction in truly tragic ways. Operators cannot be relied upon to catch errors, and, in practice, they have not. In San Francisco, the police relied on a license plate reader scan that erroneously flagged a 47-year-old Black woman's red car as a stolen grey truck. She was improperly stopped, forced to exit her vehicle, handcuffed, and held at gunpoint by four officers.²

We are living in a time where abortion and gender-affirming care is being criminalized in some states, and there is a real threat that surveillance information collected in communities will be exploited to identify, track, and criminalize people who travel for care and the Californians who are helping those people obtain care.³ Deploying surveillance systems in our community may fill databases with information that place people at risk. Even if there are limits to sharing information, once this information is collected, there is no foolproof way to immunize it from legal demands brought by out-of-state governments.

The community, not the police, must be the leader in any decision about the acquisition or use of surveillance technology. Those who may be most impacted need to know when and why surveillance is being considered, what it is intended to do, and what it will cost them — both in dollars, and in their rights. And they need to be empowered to limit or reject surveillance if the costs outweigh the benefits.

² Matt Cagle, San Francisco — Paying the Price for Surveillance Without Safeguards, ACLU of Northern California blog, May 22, 2014, available at <https://www.aclunc.org/blog/san-francisco-paying-pricesurveillance-without-safeguards>. (Denise Green successfully sued San Francisco for violation of her civil rights).

³ Alabama's attorney general says the state can prosecute those who help women travel for abortions, AP News, Aug. 31, 2023, available at <https://apnews.com/article/alabama-abortion-steve-marshall2157a7d0bfad02aad1ca41e61fe4de33>.

Utilization of Surveillance Technologies

Chief Cregan's presentation to the Public Safety Subcommittee names these programs and tools as part of the Real Time Crime Center: automated license plate readers, surveillance cameras, computer aided dispatch system, records management system, drones, fleet and body worn cameras, and gunshot detection software. We oppose deployment of many of these types of technologies and together, it creates a vast surveillance network able to monitor the everyday movements of law-abiding community members. We call attention to specific tools named in Chief Cregan's presentation.

First, automatic license plate readers (ALPRs) are a powerful surveillance system that can be used to invade the privacy of individuals and violate the rights of entire communities. ALPR systems collect and store location information about drivers whose cars pass through ALPR cameras' fields of view, which, along with the date and time of capture, can be built into a database that reveals sensitive details about where individuals work, live, associate, worship, seek medical care, and travel.⁴

ALPR systems are easily misused to harm marginalized communities.⁵ As with other surveillance technologies, police often deploy license plate readers in poor and historically overpoliced areas, regardless of crime rates.⁶ When placed in fixed locations, ALPRs essentially create checkpoints throughout a city that log and monitor

⁴ See, e.g., *Automatic License Plate Readers*, ELECTRONIC FRONTIER FOUND., March 29, 2023, <https://www EFF.ORG/sls/tech/automated-license-plate-readers>; *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, AM. CIV. LIBERTIES UNION, July 2013, <https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements>

⁵ See, e.g., Angel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CRT. FOR JUST., Sept. 10, 2020, <https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>; Matt Cagle, *San Francisco – Paying the Price for Surveillance Without Safeguards*, ACLU OF. NORTHERN CAL., May 22, 2014, <https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards>.

⁶ Dave Maass and Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, ELECTRONIC FRONTIER FOUND., Jan. 21, 2015, <https://www EFF.ORG/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>; Barton Gellman and Sam Adler-Bell, *The Disparate Impact of Surveillance*, THE CENTURY FOUND., Dec. 21, 2017, <https://tcf.org/content/report/disparate-impact-surveillance/>; see also, e.g., Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, THE ATLANTIC, Apr. 22, 2016, <https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/> (summarizing data indicating that Oakland Police Department deployed ALPRs "disproportionately often in low-income areas and in neighborhoods with high concentrations of African-American and Latino residents").

where residents go and when, threatening their freedom of movement and potentially reinforcing historical patterns of neighborhood segregation.⁷ When mounted to police cars, ALPRs turn those vehicles into mobile surveillance machines that indiscriminately capture the driving information of passersby. Such surveillance can amplify racial and economic disparities in our policing and incarceration systems, and also has serious psychological consequences.⁸

Research from California and around the world on video surveillance has repeatedly shown that it has limited efficacy on crime.⁹ A 2019 systemic review of 40 years of video surveillance showed that it has had “no significant effects” in combating violent crime.¹⁰ Surveillance camera programs have a significant impact on privacy. Twenty-four-hour video monitoring of public spaces gives the government a vast quantity of information on private citizens that would otherwise be unavailable, allowing it to monitor people engaging in wholly innocent and constitutionally protected behavior.

We are also concerned that unmanned aerial devices (drones) increase the government’s surveillance power in newly invasive ways. This is in part because drones eliminate traditional practical barriers that have prevented continuous and routine aerial surveillance: for example, unlike a traditional manned helicopter or aircraft, drones are smaller, cheaper to acquire and operate, and easier for humans to fly without advanced skill. Drones can fly lower, more quietly, and navigate private spaces in ways unlike traditional aircraft. The technological advances of drones lower the cost of surveillance, removing a natural existing deterrent to continued and abusive surveillance.

Drones also give police an unprecedented ability to monitor people going about their lives. Small, hovering platforms, drones can explore hidden spaces or peer into windows. They can be equipped with high powered, night-vision cameras. Vendors may

⁷ Laura Schenker, David Sylvan, Jean-Louis Arcand, and Ravi Bhavnani, *Segregation and ‘Out-of-Placeness’: The Direct Effect of Neighborhood Racial Composition on Police Stops*, POLITICAL RESEARCH QUARTERLY, April 2023, <https://doi.org/10.1177/10659129231171516>.

⁸ Chris Chambers, *NSA and GCHQ: The Flawed Psychology of Government Mass Surveillance*, THE GUARDIAN, August 26, 2013, <https://www.theguardian.com/science/head-quarters/2013/aug/26/nsa-gchq-psychology-government-surveillance>

⁹ Nicole Ozer, *Studies and Articles on Video Surveillance*, ACLU of Northern California blog, Jul. 31, 2007, available at <https://www.aclunc.org/blog/studies-and-articlesvideo-surveillance>.

¹⁰ Eric L. Piza, Brandon C. Welsh, David P. Farrington, & Amanda L. Thomas, “CCTV surveillance for crime prevention. A 40-year systematic with meta-analysis,” *Criminology & Public Policy* 18, no. 1 (2019). https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1275&context=jj_pubs.

also offer video analytics or biometric surveillance software intended to recognize and track specific people, events, and objects. With a drone, police agencies can more easily watch people without their knowledge and record detailed information about people at home, at protests, and at religious gatherings. An agency may also seek to coordinate multiple drones into swarms that scoop up information and create a system of comprehensive neighborhood surveillance.

Gunshot detection systems, such as ShotSpotter, are flawed in methodology and effectiveness.¹¹ The surveillance technology frequently fails to work, confusing gunshots with other noises, and its errors have put innocent people in jail.¹² Studies of the systems in both San Diego and Chicago both found errors and that they often led to “dead-end” police deployments — in San Diego, 60% of officer dispatches to the scene of the gunshot microphone failed to uncover anything, and in Chicago, the system generated over 40,000 dead-end police deployments.¹³ Not only do the dead-end deployments waste resources that could be used more effectively, but gunshot detection microphones also create a “false technological justification” for overpolicing and contribute to wrongful stop-and-frisks.¹⁴ Rather than supporting public safety, they “increase the frequency of police interactions, which also increases the risk of Black Americans becoming the victims of police brutality or harassment.”¹⁵ Instead of throwing money at gunshot detection microphones, some experts point to properly designed violence reduction strategies as a much more effective public safety intervention.

¹¹ Russell Contreras, Critics say gunshot-detection technology often doesn’t work, Axios, Apr. 9, 2022, available at <https://www.axios.com/2022/04/07/campaign-zero-against-shotspotter-crime>.

¹² Garance Burke, Martha Mendoza, Juliet Linderman, & Michael Tarm, How AI-powered tech landed man in jail with scant evidence, AP News, Mar. 5, 2022, available at <https://apnews.com/article/artificial-intelligencealgorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220>.

¹³ Kara Grant, ShotSpotter Sensors Send SDPD Officers to False Alarms More Often Than Advertised, Voice of San Diego, Sep. 22, 2020, available at <http://voiceofsandiego.org/2020/09/22/shotspottersensors-send-sdpd-officers-to-false-alarms-moreoften-than-advertised/>.

¹⁴ Press Release, MacArthur Just. Ctr., ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study, May 3, 2021, <https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-endpolice-deployments-in-chicago-in-21-monthsaccording-to-new-study/>.

¹⁵ Harvey Gee, “Bang!”: ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry’s Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>.

Surveillance Requires Oversight

Any government use of surveillance must include proper oversight and accountability to protect individuals' rights and liberties and to maintain the critical trust that should exist between law enforcement and the community. For this reason, we drafted a Surveillance Technology and Community Safety Ordinance, which has already been adopted by the City of Sebastopol and which we urge the City of Santa Rosa to adopt as well.

Such an ordinance – which was the actual purpose of the ACLU's previous meeting with Chief Cregan – creates transparent processes which allow law enforcement to obtain and renew approval for the use of certain surveillance devices including in exigent circumstances, while restricting unnecessary and problematic uses and practices.

A copy of Sebastopol's Surveillance Technology & Community Safety Ordinance, now codified at Chapter 8.80 of the Sebastopol Municipal Code, is attached here as an exhibit for reference.

Alternatives to Surveillance That Produce Public Safety Results

As policy-makers, we encourage you to look into and invest in alternatives to surveillance that are proven to increase public safety. Investing in the physical lighting of a neighborhood, rather than installing more cameras, can reap community-wide benefits. Community activists in California have highlighted Oakland's lighting ordinance as an example that streetlights not only prevent crime but also make neighborhoods feel safer.¹⁶

Speed bumps and other traffic calming techniques have been shown to be effective for traffic safety,¹⁷ can be utilized for a fraction of the cost of cameras (less than \$10,000 for a speed bump, while speeding and red-light cameras can cost \$80,000 per

¹⁶ Pacific Institute, Streetlights and Community Safety (2009), <https://pacinst.org/wp-content/uploads/2013/02/streetlights3.pdf>.

¹⁷ Iowa State University, Temporary Speed Hump Impact Evaluation, Final Report (Jul. 2022), https://nacto.org/docs/usdg/temporary_speed_humps_impact_evaluation_hallmark.pdf.

intersection),¹⁸ and do not infringe on privacy by collecting and retaining information about community members.

Above, we detailed our concerns with gunshot detection systems. We understand the need to implement policies to reduce gun violence in our community. Gun buyback programs focus on a core problem — the prevalence of guns — and have been extremely effective in taking guns off the street and in mobilizing communities to examine their stances on gun control.¹⁹

A growing body of research also suggests that greenery like grass and trees, not tracking devices and surveillance, may make cities safer. Research in Philadelphia in 2018 found that vacant lots that were “cleaned and greened” — for a cost of just \$5 per square meter — had statistically significant reductions in overall crime and burglaries over a 38-month period, including a 29% percent drop in gun violence in neighborhoods below the poverty line.²⁰ The researchers extrapolated that if the intervention was scaled across the entire city, it could translate to more than 350 fewer shootings each year.

Conclusion

In conclusion, we oppose the creation of the proposed Real Time Crime Center at this juncture. Instead, we encourage the City of Santa Rosa to adopt an ordinance that would impose reasonable checks and balances on law enforcement’s use of surveillance in order to protect civil rights and liberties. We also strongly object to any

¹⁸ Implementation costs for automated red light camera systems range from \$67,000 to \$80,000 per intersection, Intelligent Transportation Systems Joint Program Office, Sep. 30, 2003, available at <https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/2b209ad2c5ad2ab985256db10045892b>; Mark Lazzaretto, City Manager, City of San Gabriel, Staff Report: City-Wide Speed Hump Policy Consideration (Aug. 20, 2019), <https://www.sangabrielcity.com/DocumentCenter/View/11543/Item-6A--City-WideSpeed-Hump-Policy>.

¹⁹ J.B. Wogan, Cities Rethink Gun Buyback Programs, *Governing*, Feb. 27, 2023, available at <https://www.governing.com/archive/gov-cities-rethink-gunbuyback-programs.html>; Helen Webley-Brown, Anna Sipek, Katie Buoymaster, Juilee Shivalkar, Will Owen, & Eleni Manis, Surveillance Technology Oversight Project, ShotSpotter and the Misfires of Gunshot Technology (Jul. 14, 2022), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/62cc83c0118f7a1e018bf162/1657570241282/2022.7.7_ShotSpotter+Report_FINAL.pdf; Harvey Gee, “Bang!”: ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry’s Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>.

²⁰ Jackie Flynn Mogensen, The Surprising Science of Fighting Crime With... Trees, *Mother Jones*, 2019, available at <https://www.motherjones.com/environment/2019/04/trees-crime-cincinnati-philadelphia-ida-b-wells-chicago/>.

implication that the ACLU was consulted with, or approved of, a Real Time Crime Center.

Respectfully,

The Sonoma County Chapter of the ACLU of Northern California



Northern
California
Sonoma County Chapter

January 28, 2025

VIA ELECTRONIC MAIL

TO: Santa Rosa Public Safety Subcommittee

CC: Santa Rosa City Council (Mayor Mark Stapp, Vice Mayor Eddie Alvarez, Councilmember Dianna MacDonald, Councilmember Victoria Fleming, Councilmember Caroline Bañuelos, Councilmember Jeff Okrepkie, Councilmember Natalie Rogers)

CC: Chief John Cregan, Santa Rosa Police Department

Re: Item 6.1, Drone as First Responder Program, Public Safety Subcommittee meeting on January 28, 2025

Dear Santa Rosa Public Safety Subcommittee, Mayor Stapp, and City Councilmembers:

On behalf of the Sonoma County Chapter of the ACLU of Northern California (“ACLU NorCal Sonoma County Chapter” or “our chapter” or “ACLU”), I submit public comments on agenda item 6.1, “Drone as First Responder Program” of the Santa Rosa Public Safety Subcommittee meeting on January 28, 2025.

We write to you to urge you to consider the serious privacy and civil rights ramifications of drones and “drone as first responder” (DFR)¹ specifically.

Privacy Concerns with Utilization of Surveillance Technologies

The evidence is clear that while surveillance has increased exponentially, public safety has not. On the contrary, surveillance systems often make people less safe, especially

¹ Jay Stanley, *Eye-in-the-Sky Policing Needs Strict Limits*, ACLU White Paper, (July 27, 2023), <https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits>.

for groups that have historically been in the government's crosshairs. Modern surveillance technology makes it possible for the government to track who we are, where we go, what we do, and who we know. It fuels hightech profiling and perpetuates systems of biased policing. It facilitates deportations, chills speech, and imperils the rights of activists, religious minorities, and people who need reproductive and gender-affirming care.²

Surveillance systems fuel racial injustice. In a nation where police interactions with the public all too frequently turn dangerous, surveillance systems can exacerbate and magnify these problems, increasing the risk of unnecessary government scrutiny, in-person encounters, and violence. Again and again, police have used surveillance systems to create inaccurate and discriminatory watchlists, engage in discriminatory stops and searches, and upend people's lives. Surveillance technologies amplify the over-policing of Black and Brown communities.

Surveillance endangers immigrant communities, and this fact should be of particular concern for us in Santa Rosa. Across the United States, federal immigration agencies have eagerly exploited local databases rich with information collected by private data brokers, municipal agencies, and police departments. This information is fed into a deportation machine that tears apart immigrant communities. In recent years, Immigration and Customs Enforcement (ICE) has further expanded its reach into communities by exploiting local surveillance systems and databases to track, identify, and target immigrant community members for detention and deportation. No local surveillance system is safe from ICE's demands.

Substantive Civil Rights and Liberties Concerns with Drones

The Council's conversation with the public and departments should focus on identifying agreed-up issues or problems that the community wants to solve. Then, there should be an in-depth examination of evidence-based non-surveillance interventions that actually achieve those goals. We urge Council to question whether the harms of this invasive surveillance technology outweigh the purported benefits, especially because drones have not been demonstrated to meaningfully prevent crime or improve public safety. To the contrary, research has cast doubt on the efficacy of drones, finding that they provide minimal cost advantage to comparable manned aircraft and provide no more security than manned aircraft despite being significantly more expensive.³ In light of these

² We encourage you to read the ACLU's new report, "SEEING SURVEILLANCE: THROUGH WHY POLICYMAKERS SHOULD LOOK PAST THE HYPE," available at https://www.aclunc.org/sites/default/files/Seeing_Through_Surveillance__Report_Web.pdf.

³ Abigail Hall, Drones: *Public Interest, Public Choice, and the Expansion of Unmanned Aerial Vehicles* (September 17, 2014). Available at SSRN: <https://ssrn.com/abstract=2497539>.

concerns, communities are objecting to the use of drones by police agencies when given the opportunity.⁴ This is reflective of broader public sentiment against the use of drones for domestic surveillance.⁵ While we appreciate the information included in the presentation by SRPD, it should be accompanied by clear data to back up the supposed benefits of the DFR program.

Public sentiment is further justified by the serious civil rights and liberties concerns raised by drones. They are more invasive than traditional aerial surveillance because they present fewer barriers to frequent use and are less conspicuous. Unlike a traditional manned helicopter or aircraft, they are smaller, cheaper to acquire and operate, easier to operate without advanced skill, and capable of being equipped with invasive tracking systems. Drones can fly lower, more quietly, and navigate private spaces in ways unlike traditional aircraft. For example, a group of folks hosting a religious gathering in their backyard would be aware if a helicopter hovered over their property but might never know if a drone were flying overhead and recording video and audio of their gathering for unknown uses. The technological differences between manned aircraft remove natural limits that currently exist to deter continuous and routine aerial surveillance.

The amount of highly personal information drones can collect is nothing short of staggering. Small, hovering platforms, drones can explore hidden spaces or peer into windows. They can be equipped with high powered, night-vision cameras. So called “see-through imaging” can monitor people on the inside of a building. Through distributed video, a number of drones working in concert like a swarm of sentient insects can scoop up sensitive information with unsettling precision. Drones can be coupled with powerful sensors such as facial recognition, license plate trackers, and other software to automate the identification and tracking of community members. In many

⁴ When the Los Angeles Police Department proposed acquiring and using drones in 2019, it received over 1,675 letters in response to requests for public comment on its proposed drone program, the vast majority of which urged LAPD to halt the program in its entirety. Makeda Easter and Kate Mather, *Civilian oversight panel hears guidelines for LAPD use of drones*, LA TIMES (October 3, 2017), available at <http://www.latimes.com/local/lanow/la-me-ln-lapd-drones-20171002-story.html>. The public also expressed its opposition to the drone program in two separate petitions, one with over 1,900 signatories and another with more than 800 signatories. See *Drone-Free LAPD. No Drones, LA!*, MoveOn.org Petitions, Drone-Free LAPD. No Drones, LA! | MoveOn; see also Shomik Mukherjee, *Concord police to get drones, but promise not to spy*, EAST BAY TIMES (Oct. 14, 2021) <https://www.eastbaytimes.com/2021/10/14/concord-police-to-adopt-drones-program-promises-no-surveillance-amid-pushback/>

⁵ See Terance Miethe, Miliikeala S.J. Heen, & Emily Trosyhnski, *Public Attitudes About Aerial Drone Activities: Results of a National Survey (Research in Brief report)*, CENTER FOR CRIME AND JUSTICE POLICY (July 2014) [Research-PublicAttitudesaboutAerialDroneActivities.pdf](https://www.unlv.edu/research-public-attitudes-about-aerial-drone-activities) (unlv.edu); see also Stephen Rice, *Eyes In The Sky: The Public Has Privacy Concerns About Drones*, FORBES (Feb. 4, 2019) [Eyes In The Sky: The Public Has Privacy Concerns About Drones](https://www.forbes.com/2019/02/04/eyes-in-the-sky-the-public-has-privacy-concerns-about-drones/) (forbes.com) (citing data from a study revealing that drone use generates fears of police and that the general public opposes ongoing drone surveillance)

jurisdictions, drones capture footage from the moment they take flight until the moment they land, raising the possibility that drone-mounted cameras will capture high-definition imagery of private property and Santa Rosa community members going about their daily lives. SRPD should clarify the footage that drones would capture and whether it includes the entirety of all drone flights.

The Santa Rosa City Council should take very seriously the real possibility that the DFR program drones could expand into an even more invasive surveillance system and impose legal limits that prevent a citywide drone program from taking flight. Even when approved for a limited set of specified uses, it is often easy for police to expand the scope and intrusiveness of surveillance drones in ways the public and elected leaders never approved. These threats are not hypothetical. Drones touted as public safety tools are now available to monitor people in their private homes, workplaces, and places of worship, as well as in public spaces and during First Amendment protected events like protests.⁶ Indeed, police in Northern California have previously deployed drones to monitor students and immigrants' rights protests, and even used them to spy on encampments and unhoused people during the pandemic.⁷

Low-income communities of color in certain areas like Los Angeles have been dealing with oppressive aerial surveillance for many years, from police helicopters. Those communities have found such surveillance physically and psychologically harmful.⁸ Drones, too, are likely to be deployed first and foremost in low-income communities — though they could easily become far more pervasive and ever-present than police helicopters, which are expensive and thus subject to natural limits on their deployment⁹, especially in communities that don't have very well-funded police departments.

We should keep in mind that, with advances in artificial intelligence, video is becoming a far more searchable, accessible, and analyzable — and therefore dangerous — set of data than it used to be. There will be a constant incentive on the part of both government and private contractors to run video datasets through machine learning

⁶ Jeff Stone, *UK police may use drones to monitor protests, siege operations*, INTERNATIONAL BUSINESS TIMES (January 5, 2016), <http://www.ibtimes.com/uk-police-may-use-drones-monitor-protests-siege-operations-2250287>.

⁷ See Dave Maass & Mike Katz-Lacabe, *Alameda and Contra Costa County Sheriffs Flew Drones Over Protests*, ELECTRONIC FRONTIER FOUNDATION (Dec. 5, 2018) Alameda and Contra Costa County Sheriffs Flew Drones Over Protests | Electronic Frontier Foundation (eff.org); April Glaser, *Homeless people are at risk from the coronavirus. Police have a contentious solution: drones*, NBC NEWS (April 24, 2020) Homeless people are at risk from the coronavirus. Police have a contentious solution: Drones. (nbcnews.com).

⁸ Arielle Samuelson, *The environmental terrorism of police choppers*, HEATED (May 4, 2023), <https://heated.world/p/the-environmental-terrorism-of-police>.

⁹ Jay Stanley, *We Already Have Police Helicopters, So What's the Big Deal Over Drones?*, (March 8, 2013), <https://www.aclu.org/news/smart-justice/we-already-have-police-helicopters-so-whats-big-deal-over>.

algorithms for AI training purposes and to search for particular violations of the law or other facts of interest to law enforcement that might be buried within. Human attention is no longer a limiting factor when it comes to analyzing video data.

The principle of community consent was codified into California law by AB 481 (2021-2022) at Cal. Govt. Code §§ 7070-75. In passing that law, the Legislature declared the “public has a right to know about any funding, acquisition, or use of military equipment by state or local government officials, as well as a right to participate in any government agency’s decision to fund, acquire, or use such equipment.”¹⁰ Among other requirements, that statute mandates that a law enforcement agency must seek and obtain city council approval of a program and set of policies prior to using “military equipment”¹¹ “for a purpose, in a manner, or by a person not previously approved by the governing body.”¹² A City Council is not obligated to approve a program and cannot do so unless it determines it is “necessary,” that “no reasonable alternative” exists “that can achieve the same objective,” and that any policies safeguard the “public’s welfare, safety, civil rights, and civil liberties.”¹³

Surveillance Requires Oversight

Any government use of surveillance must include proper oversight and accountability to protect individuals’ rights and liberties and to maintain the critical trust that should exist between law enforcement and the community. For this reason, we drafted a Surveillance Technology and Community Safety Ordinance, which has already been adopted by the City of Sebastopol and which we urge the City of Santa Rosa to adopt as well.

Such an ordinance creates transparent processes which allow law enforcement to obtain and renew approval for the use of certain surveillance devices including in exigent circumstances, while restricting unnecessary and problematic uses and practices.

A copy of Sebastopol’s Surveillance Technology & Community Safety Ordinance, now codified at Chapter 8.80 of the Sebastopol Municipal Code, is attached here as an exhibit for reference.

¹⁰ Cal. Govt. Code §§ 7070-75 is also referred to by Assembly Bill 481 (2021-2022) and is available here: https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB481.

¹¹ Under the law, drones are explicitly listed as a type of “military equipment,” as they are “unmanned, remotely piloted, powered aerial or ground vehicles.” Cal. Govt. Code §7070(c)(1).

¹² Cal. Govt. Code § 7071(a)(1)(E).

¹³ Cal. Civil Code. s. 7071(d)(1).

Given the novelty of a DFR program, unanticipated issues are likely to emerge. Policies are needed in three areas: usage limits, transparency, and data handling. Good policies, including on usage limits, transparency, and privacy, should not be left up to police departments, but should be given legal force by a city council or other legislative body as part of a vote to approve a DFR program. To increase transparency to the public, the time, purpose, destination, and precise route of every DFR flight must be published. The practice of per-flight transparency should be regularized and mandated as a part of any police drone program.

Conclusion

We are concerned that the Santa Rosa community and City Council have not been able to adequately and meaningfully consider the proposed DFR program, its impact on civil rights and liberties, and the availability of non-surveillance alternatives. We urge the City Council to investigate the purported need for the DFR program, and to question whether the cost to the community outweighs the stated benefits. We encourage the City of Santa Rosa to adopt an ordinance that would impose reasonable checks and balances on law enforcement's use of surveillance in order to increase transparency and protect civil rights and liberties, and to update SRPD's Policy on Unmanned Aerial System (UAS) Operations accordingly.

Respectfully,

The Sonoma County Chapter of the ACLU of Northern California