From: Scott Kincaid

To: <u>Public Safety Subcommittee Comment</u>

Cc: \_\_CityCouncilListPublic

Subject: [EXTERNAL] Public Safety Subcommittee - Support of the Real Time Crime Center

**Date:** Thursday, July 18, 2024 2:56:24 PM

Attachments: Real Time Crime Center - Letter of Support 07-18-2024(Kincaid).pdf

#### Good Afternoon,

Please accept the attached letter in support of the Real Time Crime Center in the City of Santa Rosa. Thank you in advance for your efforts in creating a safer Santa Rosa so our residents and businesses can thrive.

Respectfully, Scott

### Scott Kincaid Owner | Project Manager



# **Facility Development Company**

5329 Skylane Blvd.
Santa Rosa, CA. 95403
www.fdc-comp.com
scott@fdc-comp.com
707 523 1722 Ex. 3
707 523-1745 Direct
707 526 4980 Fax
707 495 7058 Cell
CL# 762651

#### "Commercial, Industrial, Residential & Design Build Construction Services"

This and any attached documents are for the use of the intended recipient(s) only and may contain information that is privileged, confidential, or work product that may be exempt from disclosure under applicable law. If you are not the intended recipient, any use, dissemination, distribution, or copying of this communication and any attachments is strictly prohibited, and you are hereby requested to delete this message and any attached documents, to destroy any printed copies, and to telephone or otherwise contact the sender immediately about the error.

City of Santa Rosa Public Safety Subcommittee 100 Santa Rosa Avenue Santa Rosa, CA 95404

Re: Real Time Crime Center

Chair Jeff Okrepkie, Mayor Natalie Rogers, Council Member Eddie Alvarez,

Thank you for continuing to ensure that Public Safety remains a top priority in the City of Santa Rosa. At your upcoming meeting on July 23<sup>rd</sup> you will have a presentation from Chief Cregan on the Real Time Crime Center (RTCC). I am writing to offer my support of the implementation of the RTCC for the following reasons:

- Technology enhancements should be adopted once formally vetted.
- Technology enhancements expand the capacity of resources available to existing staff making their work more efficient and effective.
- Utilizing technology can supplant the need for increased staffing, which is critical in the City's current budgetary constraints.
- Criminal violators are using evolving technics in committing crimes, which should be out matched by law enforcement resources.
- The multifaceted use of the RTCC for large public event safety, sideshow enforcement, combatting organized retail theft, coordinating emergency evacuations, locating missing persons and kidnapping victims is a game changer for our community.
- Proper safeguards will be in place using best practices in policy creation.

In our business we are always looking to provide the tools for our employees to excel at their professional responsibilities. This is one of those important tools available to the City and should be utilized to its full potential. Thank you in advance for your consideration.

Respectfully,

Scott Kincaid Santa Rosa Resident and

**Business Owner** 

From: ross liscum

To: Public Safety Subcommittee Comment
Cc: CityCouncilListPublic; Smith, Maraskeshia
Subject: [EXTERNAL] SRPD Real Time Crime Center7-19

**Date:** Friday, July 19, 2024 9:15:16 AM

July 19, 2024

City of Santa Rosa Public Safety Subcommittee 100 Santa Rosa Avenue Santa Rosa, CA 95404

Dear Public Safety Subcommittee,

Many of us in our community supports the continued efforts by our Santa Rosa Police Department to do all this can to keep us a safer community.

As I know you are aware, the Chief has been very pro-active on trying to keep our city safe for our residents and visitors. As public safety remains a top city priority, I support the Real Time Crime Center implemented that can and will make us safer and not fail in protecting our public safety as many other cities in the Bay Area have.

A healthy community requires a strong local police department and innovated steps to pursue criminals and get them off our streets.

Please support adopting the Real Time Crime Center to capitalize on this technology to assist in the reduction of crime in Santa Rosa. We are hopeful that this will benefit our school safety, sideshows, any organized retail theft and other areas of community concerns. Thank you!

Ross Liscum, CRS
Broker Associate
DRE # 00690324
REALTOR Emeritus
CENTURY 21 Epic
DRE # 01523620
1057 College Avenue • Santa Rosa, CA 95404
(707) 303-4242 direct / 953-2731 cell
RossLiscum@Gmail.com

From: Megan

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Surveillance Ordinance
Date: Sunday, July 21, 2024 6:29:33 PM

Dear Public Safety Subcommittee,

Do Not Authorize the Real time crime center prior to creating a city - wide ordinance like Sebastopol has! Citizens don't trust the police to not abuse this invasive and unconstitutional technology and we need a policy to ensure that it is not used unnecessarily!

Megan Gordon

From: <u>Constance</u>

**To:** <u>Public Safety Subcommittee Comment</u>

**Subject:** [EXTERNAL] Spying on us

**Date:** Monday, July 22, 2024 3:24:54 AM

Attachments: constance-240.png

Please do not authorize this surveillance capability - just one step closer to being a police state. Do not promote spying on ordinary people. Please!

Sincerely, Constance Miles



# Constance Miles

Sonoma County End of Life Doula Alliance www.socoelda.com MoonSong@sonic.net (707) 569-4668 From: Richard Canini

To: <u>Public Safety Subcommittee Comment</u>

Subject: [EXTERNAL] Spying

**Date:** Monday, July 22, 2024 8:14:19 AM

## Greetings

Back in the day, we were told about horrible practices such as spying on people by evil governments such as communist East Germany.

Presenty we are told how awful North Korea and China are for spying on people.

Now Santa Rosa City will join totalitarian governments spying on people. Shame on you for violating the Bill of Rights.

Is Santa Rosa the city of the free and the home of the brave?

Richard M Canini USMC Viet Vet From: Chapters

To: <u>Public Safety Subcommittee Comment; Okrepkie, Jeff; Alvarez, Eddie; Rogers, Natalie</u>

Cc: \_\_CityCouncilListPublic; Alvarez, Eddie; Stapp, Mark; MacDonald, Dianna; Fleming, Victoria; Rogers, Chris;

Okrepkie, Jeff; Rogers, Natalie; Cregan, John; info@sonomaaclu.org

Subject: [EXTERNAL] ACLU NorCal - Sonoma County Comment re: Item 6.2, Real Time Crime Center, Public Safety

Subcommittee meeting on July 23, 2024

**Date:** Monday, July 22, 2024 8:54:58 AM

Attachments: <u>image002.png</u>

SoCo ACLU-NC Letter RE Real Time Crime Center 07.22.24.pdf

Chapter 8.80 SMC.pdf

#### Dear Santa Rosa Public Safety Subcommittee:

Attached, please find public comment from the Sonoma County Chapter of the ACLU of Northern California on agenda item 6.2, "Real Time Crime Center" of the Santa Rosa Public Safety Subcommittee meeting on July 23, 2024.

#### Respectfully,

The Sonoma County Chapter of the ACLU of Northern California



Email: info@sonomaaclu.org



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.<sup>1</sup>

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

<sup>&</sup>lt;sup>1</sup> We encourage you to read the ACLU's new report, "SEEING SURVEILLANCE: THROUGH WHY POLICYMAKERS SHOULD LOOK PAST THE HYPE," available at <a href="https://www.aclunc.org/sites/default/files/Seeing\_Through\_Surveillance\_Report\_Web.pdf">https://www.aclunc.org/sites/default/files/Seeing\_Through\_Surveillance\_Report\_Web.pdf</a>.



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.<sup>2</sup>

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. 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.

<sup>&</sup>lt;sup>2</sup> 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).

<sup>&</sup>lt;sup>3</sup> 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.<sup>4</sup>

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

\_

<sup>&</sup>lt;sup>4</sup> See, e.g., Automatic License Plate Readers, Electronic Frontier Found., March 29, 2023, <a href="https://www.eff.org/sls/tech/automated-license-plate-readers">https://www.eff.org/sls/tech/automated-license-plate-readers</a>; You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements, Am. Civ. Liberties Union, July 2013, <a href="https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements">https://www.aclu.org/documents/you-are-being-tracked-how-license-plate-readers-are-being-used-record-americans-movements</a>

<sup>&</sup>lt;sup>5</sup> 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, <a href="https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations">https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations</a>; Matt Cagle, *San Francisco – Paying the Price for Surveillance Without Safeguards*, ACLU Of. Northern Cal., May 22, 2014, <a href="https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards">https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards</a>.

<sup>&</sup>lt;sup>6</sup> 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, <a href="https://tcf.org/content/report/disparate-impact-surveillance/">https://tcf.org/content/report/disparate-impact-surveillance/</a>; see also, e.g., Kaveh Waddell, *How License-Plate Readers Have Helped Police and Lenders Target the Poor*, The Atlantic, Apr. 22, 2016, <a href="https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/">https://www.theatlantic.com/technology/archive/2016/04/how-license-plate-readers-have-helped-police-and-lenders-target-the-poor/479436/</a> (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. 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.

Research from California and around the world on video surveillance has repeatedly shown that it has limited efficacy on crime. A 2019 systemic review of 40 years of video surveillance showed that it has had "no significant effects" in combating violent crime. 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

<sup>&</sup>lt;sup>7</sup> 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, <a href="https://doi.org/10.1177/10659129231171516">https://doi.org/10.1177/10659129231171516</a>.

<sup>&</sup>lt;sup>8</sup> 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-mas s-surveillance

<sup>&</sup>lt;sup>9</sup> 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.

<sup>&</sup>lt;sup>10</sup> 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. The surveillance technology frequently fails to work, confusing gunshots with other noises, and its errors have put innocent people in jail. 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. 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. 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." 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.

<sup>&</sup>lt;sup>11</sup> 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.

<sup>&</sup>lt;sup>12</sup> Garance Burke, Martha Mendoza, Juliet Linderman, & Michael Tarm, How Al-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-7e3345485aa6 68c97606d4b54f9b6220.

<sup>&</sup>lt;sup>13</sup> 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/.

<sup>&</sup>lt;sup>14</sup> 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-ne w-study/.

<sup>&</sup>lt;sup>15</sup> 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 <u>Chapter 8.80 of the Sebastopol Municipal Code</u>, 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.<sup>16</sup>

Speed bumps and other traffic calming techniques have been shown to be effective for traffic safety,<sup>17</sup> 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

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

<sup>&</sup>lt;sup>17</sup> 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),<sup>18</sup> 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.<sup>19</sup>

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.<sup>20</sup> 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

\_\_

<sup>&</sup>lt;sup>18</sup> 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. <sup>19</sup> 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/62cc83c 0118f7a1e018bf162/1657570241282/2022.7.7 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. <sup>20</sup> 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-cincinnatiphiladelphia-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

# Chapter 8.80

#### SURVEILLANCE TECHNOLOGY AND COMMUNITY SAFETY ORDINANCE

000.01.01	
8.80.010	Title.
8.80.015	Purpose and findings.
8.80.020	Definitions.
8.80.030	City Council review mandatory for surveillance technology decisions.
8.80.040	Temporary acquisition during exigent circumstances.
8.80.050	Surveillance impact report and surveillance use policy submission.
8.80.060	Standard for approval and compliance for existing surveillance technology.
8.80.065	Oversight following Council approval.
8.80.070	Prevention of secret surveillance technology contracts and agreements.
8.80.075	Prohibition of certain surveillance technologies.
8.80.080	Whistleblower protections and enforcement.
8.80.090	Severability.

#### 8.80.010 Title.

Sections:

This chapter shall be known as the "Surveillance Technology and Community Safety Ordinance." (Ord. 1145, 2022)

# 8.80.015 Purpose and findings.

Biometric surveillance and predictive policing technologies have the potential to grant government entities the unprecedented power to secretly identify, monitor, and locate people simply going about their daily lives, threatening Californians' privacy, liberty, safety and freedom as guaranteed by the California Constitution.

While surveillance technology may threaten the privacy of all of us, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

The use of biometric surveillance systems and predictive policing technology to watch, categorize, monitor and record the activities and movements of all Californians disproportionately impacts people of color, women, immigrants, LGBTQ people, and political activists of all backgrounds. Bias, accuracy issues, and stereotypes built into biometric surveillance systems and predictive policing technology have been shown to be flawed thus raising the potential for significant harm and injury to the groups previously mentioned.

No decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the <u>First</u>, <u>Fourth</u>, and <u>Fourteenth</u> Amendments to the United States Constitution, as well as Sections <u>1</u>, <u>2</u>, and <u>13</u> of Article <u>I</u> of the California Constitution.

Due to the potential for abuse and misuse, it is imperative and as a matter of best practices that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed.

Whenever a surveillance technology is approved for use in the City of Sebastopol, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

The Sebastopol City Council finds that the public has a right to know about any funding, acquisition, or use of surveillance technologies within the City of Sebastopol. This chapter codifies and guarantees that the acquisition and use of these technologies are subject to rigorous review, public debate, oversight and annual reporting by any City department utilizing these technologies.

This chapter bans the use of certain technologies within the City of Sebastopol absent clearly defined exigent circumstances that would expose our citizens to a major risk to the public safety. Should the technologies be required to be implemented during a public safety emergency, the chapter provides for both limited use and duration with mandated public reporting requirements and significant levels of review regarding their use or any continued use. (Ord. 1145, 2022)

#### 8.80.020 Definitions.

For purposes of this chapter, the following words, terms and phrases shall have these definitions:

"Annual surveillance report" means an annual written report concerning each of the specific surveillance technologies used by the City. The annual surveillance report will include all of the following:

- 1. A general description of how the surveillance technology was used;
- 2. A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
- 3. A summary of community complaints or concerns about each surveillance technology item;
- 4. The results of any internal audits required by the surveillance use policy, any information about violations of the surveillance use policy, and a general description of any actions taken in response;

- 5. Information, including crime statistics, that helps the City Council assess whether the surveillance technologies used by the City have been effective at achieving their identified purposes;
- 6. Statistics and information about any related Public Records Act requests;
- 7. Total annual costs for the surveillance technologies, including personnel and other ongoing costs, and what source of funding will fund the technologies in the coming year;
- 8. Any requested modifications to the surveillance use policy and a detailed basis for the request;
- 9. Where applicable, a general breakdown of what physical objects each surveillance technology hardware was installed upon, using general descriptive terms; and for each surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to;
- 10. The summary of all requests for City Council approval for the use of any surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed surveillance use policy before approval;
- 11. The annual surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes and/or information protected, restricted and/or sealed pursuant to State and/or Federal laws, including information not required to be released by the Public Records Act.

"Biometric surveillance technology" means any computer software that uses face recognition technology or other remote biometric recognition in real time or on a recording or photograph.

"City" means the City of Sebastopol, and "City Department" means any City department and its officers and employees.

"Face recognition technology" or "FRT" means an automated or semiautomated process that:

- 1. Assists in identifying or verifying an individual based on an individual's face; or
- 2. Identifies or logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

"Other remote biometric recognition" means:

- 1. An automated or semiautomated process that assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on physiological, biological, or behavioral characteristics ascertained from a distance;
- 2. Uses voice recognition technology; or
- 3. Identifies or logs such characteristics to infer emotion, associations, activities, or the location of an individual; and does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.

"Personal communication device" means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless-capable tablet or similar wireless two-way communications and/or portable internet-accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

"Predictive policing technology" means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to be connected to a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g., heat maps).

"Surveillance impact report" means a written report including at a minimum the following:

- 1. Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
- 2. Information on the proposed purpose(s) for the surveillance technology;
- 3. If applicable, the location(s) it may be deployed and crime statistics for any location(s);
- 4. The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
- 5. An assessment identifying with specificity any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and what specific, affirmative measures will be implemented to safeguard the public from those potential adverse impacts;
- 6. Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis; and
- 7. A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, and any known adverse information about the technology such as unanticipated costs, failures, civil rights, or civil liberties abuses.

"Surveillance technology" means any software, electronic device, system utilizing an electronic device, or similar, used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group. "Surveillance technology" includes but is not limited to:

- 1. International mobile subscriber identity (IMSI) catchers and other cell site simulators;
- 2. Automatic license plate readers;
- 3. Electric toll readers;
- 4. Closed-circuit television cameras;
- 5. Gunshot detection hardware and services;

- 6. Video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras;
- 7. Mobile DNA capture technology;
- 8. Biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases;
- 9. Software designed to monitor social media services;
- 10. X-ray vans;
- 11. Software designed to forecast criminal activity or criminality;
- 12. Radio-frequency ID (RFID) scanners;
- 13. Tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network.

"Surveillance technology" does not include the following devices, hardware or software:

- 1. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones, and printers, that are in widespread use by City departments and used for routine City business and transactions;
- 2. City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resources, permits, licenses, and business records;
- 3. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;
- 4. Information technology security systems, including firewalls and other cybersecurity systems;
- 5. Physical access control systems, employee identification management systems, and other physical control systems;
- 6. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;
- 7. Manually operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices, and email systems;
- 8. Manually operated, nonwearable, handheld cameras, audio recorders and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

- 9. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;
- 10. Computers, software, hardware, or devices used in monitoring the work and work-related activities involving City employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
- 11. Parking ticket devices;
- 12. Police department interview room and holding cell;
- 13. Police department computer-aided dispatch (CAD), records/case management, Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1, and related dispatch and operation or emergency services systems;
- 14. Police department early warning systems.

"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.
- 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.
- 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.
- 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.
- 5. *Data Protection.* The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
- 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.

- 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.
- 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. (Amended as part of January 2023 update; Ord. 1145, 2022)

# 8.80.030 City Council review mandatory for surveillance technology decisions.

A City department must obtain City Council approval by ordinance of a surveillance use policy following a public hearing conducted at a regular City Council meeting, prior to engaging in any of the following:

- A. Seeking funds for a surveillance technology, including, but not limited to, applying for a grant or soliciting or accepting State or Federal funds or in-kind or other donations for the purpose of acquiring surveillance technology;
- B. Acquiring or borrowing a new surveillance technology, including, but not limited to, acquiring such technology without the exchange of monies or consideration;
- C. Using a new or existing surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council in accordance with this chapter; or
- D. Entering into an agreement, including a written or oral agreement, with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data-sharing agreements. (Ord. 1145, 2022)

# 8.80.040 Temporary acquisition during exigent circumstances.

A. A department may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this chapter. Nothing in this section or chapter shall preclude law enforcement from utilizing these technologies or utilizing mutual aid from a law enforcement partner who may opt to utilize

these technologies during exigent circumstances, which for the purposes of this chapter is defined as an emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of surveillance technology or the information it provides. Any surveillance technology temporarily acquired in exigent circumstances shall be returned within seven days following the conclusion of the exigent circumstances, unless the department acquires the surveillance technology in accordance with the requirements of this chapter.

- B. If a department acquires or uses surveillance technology for exigent circumstances, the department shall do all of the following:
  - 1. Use the surveillance technology solely to respond to the exigent circumstances;
  - 2. Cease using the surveillance technology within seven days, or when the exigent circumstances end, whichever is sooner;
  - 3. Keep and maintain only data related to the exigent circumstances, and dispose of any data that is not relevant to an ongoing investigation, unless its retention is (a) authorized by a court based on a finding of probable cause to believe the information constitutes evidence of a crime; or (b) otherwise required by law;
  - 4. Not disclose to any third party any information acquired during exigent circumstances unless such disclosure is (a) authorized by a court based on a finding of probable cause to believe the information constitutes evidence of a crime; or (b) otherwise required by law; and
  - 5. Submit a written report summarizing that acquisition and/or use of surveillance technology under this section to the City Council within 60 days following the inception of the exigent circumstances. (Ord. 1145, 2022)

# 8.80.050 Surveillance impact report and surveillance use policy submission.

- A. The City department seeking approval under SMC <u>8.80.030</u> shall submit to the City Council a surveillance impact report and a proposed surveillance use policy via an informational staff report on a regular City Council meeting consent calendar at least 45 days prior to the public hearing required under SMC <u>8.80.030</u>. The informational staff report shall be posted on the City website with the relevant City Council agenda at least 30 days prior to the public hearing.
- B. The City Council may request revisions to the surveillance impact report or surveillance use policy submitted by the City department. (Ord. 1145, 2022)

# 8.80.060 Standard for approval and compliance for existing surveillance technology.

- A. The City Council shall only approve a request to fund, acquire, or use a surveillance technology under SMC 8.80.030 if it determines the benefits of the proposed surveillance technology outweigh its costs, that the surveillance use policy will safeguard civil liberties and civil rights, that no alternative with lesser economic cost or impact on civil rights or liberties would be as effective, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or group.
- B. A City department or departments possessing or using surveillance technology prior to the effective date of the ordinance codified in this chapter shall submit or jointly submit a proposed surveillance use policy no later than 120 days following the effective date of the ordinance codified in this chapter for review and approval by the City Council pursuant to SMC 8.80.030.
- C. If a City department is unable to meet this 120-day timeline, the department may notify the Council in writing of the department's request to extend this period and the reasons for that request. The City Council may grant City departments extensions of up to 90 days beyond the 120-day timeline to prepare and submit a proposed surveillance use policy.
- D. If the City Council has not approved the continuing use of surveillance technology, including the surveillance impact report and surveillance use policy, within 180 days of their submission to the City Council, the City department shall cease its use of the surveillance technology and the sharing of surveillance data therefrom until such time as City Council approval is obtained in accordance with this chapter. (Ord. 1145, 2022)

# 8.80.065 Oversight following Council approval.

- A. A City department that obtains approval under SMC <u>8.80.030</u> must submit to the City Council, and make available on its website, an annual surveillance report for each surveillance technology used by the City department within 12 months of Council approval, and annually thereafter on or before November 1st. The annual report shall be a single report detailing each type of technology that was utilized by the City. If the City department is unable to meet the deadline, the department head shall notify the City Council in writing of staff's request to extend this period, and the reasons for that request. The City Council may grant reasonable extensions for good cause.
- B. Based upon information in the annual surveillance report, the City Council will, at a public hearing during a regular City Council meeting, reassess whether that surveillance technology as used continues to meet the standard of approval set forth in SMC 8.80.060. If it does not, the City Council shall consider:
  - 1. Directing that the use of the surveillance technology cease;

- 2. Requiring modifications to the surveillance use policy that are designed to address the Council's concerns; and/or
- 3. Directing a report back from the department regarding steps taken to address the Council's concerns. (Ord. 1145, 2022)

# 8.80.070 Prevention of secret surveillance technology contracts and agreements.

- A. It shall be unlawful for the City or any City department to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this chapter, and any conflicting provisions in such future contracts or agreements, including, but not limited to, nondisclosure agreements, shall be deemed void and legally unenforceable. The City and any City department shall have one year from the effective date of the ordinance codified in this chapter to bring any existing contracts or agreements into compliance with this chapter; after that date, any conflicting provisions in contracts or agreements signed prior to the enactment of the ordinance codified in this chapter shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that predate this chapter.
- B. To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related nondisclosure agreements, if any, regardless of any contract terms to the contrary. (Ord. 1145, 2022)

# 8.80.075 Prohibition of certain surveillance technologies.

- A. It shall be unlawful for any City department to obtain, retain, access, or use:
  - 1. Biometric surveillance technology; or
  - 2. Predictive policing technology; or
  - 3. Facial recognition technology; or
  - Any information obtained from biometric surveillance or predictive policing technologies.
- B. A City department's inadvertent or unintentional receipt, retention, access to, or use of any information obtained from subsections (A)(1) through (A)(4) of this section shall not be a violation of this subsection; provided, that:
  - 1. The City department does not request or solicit its receipt, access to, or use of such information; and

- 2. The City department creates a log of such receipt, access to, or use and, within seven days of the event, submits that log to the City Council for inclusion in the City Council's subsequent regular meeting agenda.
- C. Any violation of this chapter constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this chapter. An action instituted under this subsection shall be brought against the City of Sebastopol.
- D. No data collected or derived from any use of technology in violation of this chapter, and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the State of California. Data collected or derived in violation of this chapter shall be considered unlawfully obtained, and shall be deleted upon discovery.
- E. A court shall award costs to the prevailing plaintiff in any action brought to enforce this chapter and any reasonable attorney's fees as may be awarded pursuant to State law. (Ord. 1145, 2022)

## 8.80.080 Whistleblower protections and enforcement.

- A. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:
  - 1. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this chapter; or
  - 2. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this chapter.
- B. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this chapter.
- C. Any employee or applicant who is injured by a violation of this section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

#### D. Enforcement.

1. Any violation of this chapter constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this chapter. An action instituted under this subsection shall be brought against the City of Sebastopol, and if necessary to effectuate compliance with this chapter or a surveillance use policy (including to expunge

information unlawfully collected, retained, or shared thereunder), any third party, except a City employee, with possession, custody, or control of data subject to this chapter.

- 2. Prior to the initiation of any legal proceeding under subsection (D)(1) of this section, the City of Sebastopol shall be given written notice of the violation(s) and an opportunity to correct such alleged violation(s) within 30 days of receipt of the notice.
- 3. If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous space on the City's website that generally describes the corrective measure(s) taken to address the violation(s).
- E. A court shall award costs to the prevailing plaintiff in any action brought to enforce this chapter and any reasonable attorney's fees as may be awarded pursuant to State law.
- F. Nothing in this chapter is intended to, or shall be interpreted to, conflict with the Constitution of the United States, the Constitution of the State of California, or with any State or Federal law. (Ord. 1145, 2022)

### 8.80.090 Severability.

- A. The provisions of this chapter are declared to be separate and severable. The invalidity of any clause, phrase, sentence, paragraph, subdivision, section or portion of this chapter, or the invalidity of the application thereof to any person or circumstance, shall not affect the validity of the remainder of this chapter, or the validity of its application to other persons or circumstances.
- B. The City Council hereby declares that it would have passed this chapter and each and every section, subsection, sentence, clause, phrase, and word not declared invalid or unconstitutional without regard to whether any other portion of this chapter or application thereof would be subsequently declared invalid or unconstitutional.
- C. The City Clerk shall certify to the adoption of the ordinance codified in this chapter and shall cause the same or a summary thereof to be published as required by law.
- D. The ordinance codified in this chapter shall take effect and be in full force and effect 30 days from and after the date of its final passage and adoption. (Ord. 1145, 2022)

#### The Sebastopol Municipal Code is current through Ordinance 1149, passed October 3, 2023.

Disclaimer: The City Clerk's Office has the official version of the Sebastopol Municipal Code. Users should contact the City Clerk's Office for ordinances passed subsequent to the ordinance cited above.

City Website: www.ci.sebastopol.ca.us

Hosted by General Code.

From: Pat Cull

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Real Time Crime Center
Date: Monday, July 22, 2024 9:07:28 AM

I am horrified at the proposal to set up surveillance of the population on our city streets. This is an unforgivable incursion on rights to property.

Pat Cull

Santa Rosa 95409

From: Robin Jurs

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Real Time Crime Center
Date: Monday, July 22, 2024 9:17:57 AM

In my opinion, I find it untenable that the City of Santa Rosa will be literally spying on its citizens and in truth it is nothing less than that. At least the potential exists that innocent (NON-crime offending people) will be scrutinized in their comings and goings throughout Santa Rosa. I find this deplorable, especially in light of what we are hearing from the likes of Trump Maga folks who will go to any lengths to find out more about us and try to find ways to curtail our activity unless (and until) we line up behind them. For Santa Rosa to be doing this at this time is frightening. I am totally opposed to this Crime Center as it infringes upon the rights of anyone and everyone who come into and through Santa Rosa.

Please do not approve of this proposal.

Robin Jurs

Santa Rosa, CA 95409

From: jrwikse@aol.com

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Increased surveillance
Date: Monday, July 22, 2024 9:22:39 AM

Please rethink wasting funds to increase the surveillance society locally.

Jack Wikse

Santa Rosa, CA

From: <u>Laura González</u>

To: Public Safety Subcommittee Comment

**Subject:** [EXTERNAL] RTCC

**Date:** Monday, July 22, 2024 10:04:01 AM

As a resident of SR, I am extremely concerned about the proposed RTCC. The government does not need to surveil the public to this extreme.

Do not pass this unwarranted and highly intrusive proposal. I know some have said that Keegan is a good guy and won't misuse an RTCC. That's not the point. The point is that the proposal itself is not needed and is an a front to the public.

As the ACLU wrote it's members, "A Real Time Crime Center crosses the line into unwarranted invasion of personal privacy and perpetuating stereotypes on marginalized communities. Those communities under constant surveillance are more likely to end up on government and law enforcement watchlists and become disproportionately subject to arrest and charges for minor violations."

No RTCC!

Laura Gonzalez District 7 Sent from my iPhone From: Barbara Lee

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Real Time Crime Center
Date: Monday, July 22, 2024 10:19:14 AM

I am writing to express my concern about the possibility of the City providing funding for a Real Time Crime Center.

Automated license plate readers, surveillance cameras giving the police the ability to monitor and collect our information without our consent is egregious. It's unwarranted and unnecessary invasion of our personal privacy and further adversely affects the lives of our poorest and most vulnerable citizens. You already have the ability to do much of what you're saying a "Real Time Crime Center" would accomplish.

I implore you to invest in solutions that lift up, not suppressi the marginalized.

Barbara Lee

From: <u>corlene van sluizer</u>

To: <u>Public Safety Subcommittee Comment</u>

**Subject:** [EXTERNAL] Prevention

**Date:** Monday, July 22, 2024 10:41:49 AM

#### Let's face it straight on:

Crimes are committed largely through desperation...

When we can treat the mentally ill; the veterans that come back from war with TRAUMA, when the racial divide is closed economically and with opportunity for all...when the homeless and houseless are given respect and listened to and supported in their needs for a life of integrity...THEN we will have less crime.

Lets put the programs and money to help the under privileged, which includes education and rehabilitation in the prisons...etc. etc. SERVICE, SERVICE....rather than surveillance and police presence around the corner.

I think therapist and counselors should be employed as has been suggested and implemented.

Let's look at THE SOURCE for criminal behavior rather then more intimidation and confrontation...

WHAT ARE YOU THOUGHTS??? A citizen for solutions rather than bandaids. Corlene

From: BONNIE CLARK

To: Public Safety Subcommittee Comment
Subject: [EXTERNAL] Real time crime monitoring
Date: Monday, July 22, 2024 10:52:45 AM

Although I'm well for lower g and preventing crime, I believe that this proposal goes too far. It allows for abuse of monitoring when put on the wrong hands.

I ask that you not approve this plan.

Respectfully, Bonnie Clark

Santa Rosa, CA

Sent from my iPhone

From: <u>City Council Public Comments</u>

To: Public Safety Subcommittee Comment
Subject: FW: [EXTERNAL] NO to a Real Time Crime Ctr

**Date:** Monday, July 22, 2024 1:12:37 PM

From: Jennifer LaPorta

**Sent:** Monday, July 22, 2024 10:29 AM

To: City Council Public Comments <cc-comment@srcity.org>

**Subject:** [EXTERNAL] NO to a Real Time Crime Ctr

Dear Santa Rosa City Council,

As a homeowner resident of Santa Rosa, I strongly oppose this idea. A Real Time Crime Center crosses the line into unwarranted invasion of personal privacy and perpetuating stereotypes on marginalized communities. Those communities under constant surveillance are more likely to end up on government and law enforcement watchlists and become disproportionately subject to arrest and charges for minor violations.

Instead of investing in a Real Time Crime Center, we should focus on community-based solutions to enhance public safety. Community initiatives and increasing access to youth programs, restorative justice programs, and social services to provide positive opportunities for young people, address the roots of crime.

Sincerely, Jennifer LaPorta 95407