CITY OF SEBASTOPOL CITY COUNCIL
AGENDA ITEM REPORT FOR MEETING OF: January 21, 2025

==========

To: Honorable Mayor and City Councilmembers
From: Ronald Nelson, Chief of Police
Responsible Department: Police
Subject: Approval of Annual Report and Continued Use of Existing Surveillance Technology

==========

RECOMMENDATIONS:
The recommendation is that the City Council receive this report, provide any feedback or concerns to the Chief of Police regarding surveillance technology currently in use in the City of Sebastopol, and authorize the continued use of those systems by city departments.

EXECUTIVE SUMMARY:
The item is to request Council to review the annual Surveillance Technology and Community Safety Report as required by the Sebastopol Municipal Code Chapter 8.80, and to provide any feedback they deem necessary to the Chief of Police regarding the report, and to approve the continued use of all existing surveillance technologies by the City of Sebastopol.

BACKGROUND AND DISCUSSION:
On December 6, 2022, the City of Sebastopol City Council voted unanimously to adopt the Surveillance Technology and Community Safety Ordinance which was incorporated into the City of Sebastopol Municipal Code as Chapter 8.80. The ordinance requires an annual report to be prepared and presented to the council and the public summarizing any surveillance technologies currently in use by the city, as defined by the ordinance, and also lists several other points which are required to be addressed in the annual report.

This annual report is produced as required by the ordinance. The report is attached to this staff report as a separate document detailing the information required to be provided by the Sebastopol Municipal Code Chapter 8.80.

Currently, the only existing surveillance technologies in use by the City of Sebastopol are closed circuit video cameras on city owned buildings, and police department body worn cameras. There have been no changes to any of the systems with city owned buildings except for the Sebastopol Library, which is leased to the Sonoma County Library system. There have been no Public Records Act requests regarding any of the existing systems on city owned buildings. All video surveillance security systems on city owned buildings, with the exception of the library, were purchased and installed prior to the passage of the city ordinance and have not been modified.

During 2023, the Sonoma County Library announced they were going to install CCTV cameras at the Sebastopol branch as part of the Sonoma County Library's "Safe Libraries" program. They were also going to install badge activated security doors for staff areas inside the library. The Sebastopol Library is the last branch in the system to get CCTV. The cameras have already been installed at every other library within the system.

The reason behind the decision to install cameras at the library branches was to provide a safer environment for staff and patrons of the library facilities. Sonoma County Library Director Erika Thibault had stated publicly that there had been incidents at all library branches including in Sebastopol where a Black Lives Matter banner had been destroyed outside the library. There have been incidents of patrons behaving in threatening ways inside branches

that have resulted in those patrons being suspended from accessing the facilities. All funding for the purchase and operation of the CCTV system was through the Sonoma County Library budget.

Director Thibault has stated that the library has policies in place to mitigate the threat to privacy. The video will be recorded 24/7 but will not be monitored unless there is an incident that prompts them to review the footage. Unmonitored video is erased after 14 days and footage will only be disclosed if required by law such as footage requested under the California Public Records Act, or a via a written request pursuant to a lawfully executed subpoena or warrant.

There was also some opposition to the installation of cameras from a member of the Sebastopol Library Advisory Board based on the feeling that the larger library system was not hearing the patrons and staff of the library regarding privacy concerns.

The former Sebastopol City Manager reviewed the Sebastopol Municipal Code, Chapter 8.80, Surveillance Technology and Community Safety Ordinance, which addresses actions by city departments regarding surveillance technology. Initially it was determined the ordinance didn't apply since the library is a separate, independent entity that leases the city owned building. Following the controversy, the issue was revisited and the City Council weighed in on the issue. During the regular public City Council meeting of November 21, 2023, City Council directed staff to make a request to the Sonoma County Library, who had already installed the CCTV equipment but had not activated it, to wait to go "live" with the system until the issue was resolved.

That request was made to Director Thibault who agreed that the CCTV system would not be activated until the matter has been resolved by the city. To date, the camera system still has not been activated, but Director Thibault would like a resolution on the issue and has an interest in being able to utilize the system to enhance safety.

STAFF ANALYSIS:

This report brings us into compliance with the requirements of Sebastopol Municpal Code Chapter 8.80. The requirement of that chapter do not apply to the installation and activation of the CCTV system at the Public Library. Chapter 8.80 applies specifically to surveillance equipment used by a city department and its employees. The Sonoma County Library is an independent legal entity, and not a department of the City. The Sonoma County Library leases the building from the City of Sebastopol. However, nothing in the existing lease agreement prohibits the library from installing surveillance cameras and utilizing them for security purposes. There is a clause in the lease that addresses structural modifications, but the installation of CCTV cameras can be done in a way that does not require structural modifications.

In summary, the decision to install and activate CCTV cameras in the Sebastopol Library lies with the Sonoma County Library system.

Based on that finding, this report is submitted for approval and permission to continue utilizing existing surveillance technology by city departments.

COMMUNITY OUTREACH:

This item has been noticed in accordance with the Ralph M. Brown Act and was available for public viewing and review at least 72 hours prior to the scheduled meeting date.

FISCAL IMPACT:
None.

OPTIONS:

1. That the City Council receive this report, provide any feedback or concerns to the Chief of Police regarding the continued use of existing surveillance technology in the City of Sebastopol, and authorize the continued use of those systems by city departments.

2. That the City Council receive this report, provide any feedback or concerns to the Chief of Police regarding the continued use of existing surveillance technology in the City of Sebastopol, and authorize the continued use of those systems by city departments. In addition, the council may consider and discuss drafting a letter to the Sonoma County Library regarding their CCTV system.

ATTACHMENTS:

1. 2024 Surveillance Technology and Community Safety Report.
2. Text of Sebastopol Municipal Code Chapter 8.80

APPROVALS:

Department Head Approval: RN Approval Date: 01/13/25
CEQA Determination (Planning): N/A Approval Date: N/A
The proposed action is not a project under the California Environmental Quality Act (CEQA)

Administrative Services (Financial) AK Approval Date: 1/13/25
Costs authorized in City Approved Budget: ☐ Yes ☐ No ☑ N/A
Account Code (If applicable)
City Attorney Approval: AM Approval Date: 1/13/25
City Manager Approval: DS Approval Date: 1/14/25

Sebastopol Police Department

Surveillance Technology and Community Safety
2024 Annual Report

Background

In May 2022, the Sebastopol City Council received a request from the ACLU for consideration and support for a future agenda item for a draft city ordinance regarding the oversight of the acquisition and use of surveillance technology which included a ban on certain types of surveillance technology. The City Council was in support of the request and directed staff to review a draft ordinance presented by the ACLU and to work collaboratively with that organization in moving a proposed ordinance forward towards possible adoption.

The Sebastopol Police Department command staff held a series of meetings with ACLU staff discussing verbiage and various aspects of the proposed ordinance. Through a healthy and respectful process, the two entities were able to agree upon a proposed ordinance that balanced the need to provide for public safety, with the concerns of community members, the ACLU, and City Council regarding the use of these rapidly evolving technologies.

These technologies and their potential for overreach, misuse, and unintended consequences were the driving forces behind the desire to codify the future acquisition and use of these technologies.

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.

The key, as with any advancement in technology, is to strike a balance between being able to utilize the technology in an appropriate responsible manner while preventing their misuse for nefarious purposes. These technologies have proven their worth in many instances in helping to bring people who have committed heinous acts to justice. Automated license plate readers, for example, assist law enforcement nationwide on a daily basis in identifying vehicles and suspects who have committed serious crimes and are able to provide near real time information regarding the movements and potential locations of these suspects to aid in apprehension. Fixed mounted surveillance cameras, both privately owned and governmental, often provide leads which lead to the eventual identification of suspects who have committed crimes.

Technology is not inherently bad, however, due to the potential for their harmful use or misuse, it is prudent for the public to be informed about the types of technology which are in place, being used by, or being considered for purchase by their governmental agencies. It is reasonable for our citizens to expect transparency and to be able to set parameters for the acquisition, and under what restrictions governmental entities will be permitted to utilize these technologies, as well as having

firsthand knowledge regarding where these technologies are deployed. The use of public funds for these technologies makes it even more imperative that the public has a voice and a right to weigh in with the decision makers when their taxpayer monies are being expended on these technologies.

The proposed City Ordinance was presented to the City Council as a discussion item on November 1, 2022. Public comment was received with no negative comments and the City Council directed staff via a 5-0 unanimous vote to move forward with the adoption process.

On December 6, 2022, the item was scheduled for adoption at the regularly scheduled City Council Meeting. Ordinance number 1145, was adopted by a unanimous vote and amended the City of Sebastopol Municipal Code, Chapter 8, by adding Chapter 8.80, the "Surveillance Technology and Community Safety Ordinance".

The ordinance as adopted contains several provisions and requirements. The ordinance bans certain types of surveillance 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 those exigent circumstances occur, the ordinance provides for both limited use and duration with mandated public reporting requirements and significant levels of review regarding their use or any continued use.

Prohibited types of surveillance technologies are as follows:

1. Biometric surveillance; or
2. Predictive policing technology; or
3. Facial recognition technology; or
4. Any information obtained from biometric surveillance or predictive policing technologies.

The ordinance requires the Police Department to author an annual report concerning each of the specific surveillance technologies used by the City. The report shall 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 standards(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 help 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.

Applicable Technologies Currently in Use

Since the passage of the Surveillance Technology and Community Safety Ordinance which is Chapter 8.80 of the City of Sebastopol Municipal Code, the City of Sebastopol has not added any additional technologies to what existed and was operational at the time the ordinance went into effect. Below is a list of current assets and applicable technologies in use in City of Sebastopol owned buildings and by city departments.

City Hall – 7 closed circuit video surveillance cameras. The cameras are deployed on the exterior of the City Hall campus at various points around the building. All cameras record video and the video is available for retrieval for 30 days. There have been no instances since the implementation of the ordinance where video was required to be downloaded and utilized for criminal prosecutions or other means.

Public Works Yard – 6 closed circuit video surveillance cameras. Four of the cameras are deployed on the exterior of the building at various points to provide a 360° view on the exterior of the building and a view of the yard. Two cameras are deployed on the interior of the building where tools, equipment and vehicles are stored (garage area), but not on the internal portion of the building where offices and where staff conduct day-to-day business.

Community Center – There are 3 closed circuit video surveillance cameras deployed on the exterior of the Community Center building. All cameras record video and the video is available for retrieval for 30 days. There have been no instances since the implementation of the ordinance where video was required to be downloaded and utilized for criminal prosecutions or other means.

Youth Annex – 2 closed circuit video surveillance cameras are deployed on the exterior of the Youth Annex to provide views of any possible entry points to the building. All cameras record video and the video is available for retrieval for 30 days. There have been no instances since the implementation of the ordinance where video was required to be downloaded and utilized for criminal prosecutions or other means.

Fire Department – There are 4 closed circuit video surveillance cameras deployed on the exterior of the Fire Department. All cameras record video and the video is available for retrieval for 30 days. There was one instance since the implementation of the ordinance where video was required to be downloaded and utilized for investigative purposes by the police department for suspect identification and possible criminal prosecution regarding a hit and run collision when a vehicle collided with the Fire Department building. There were no instances during 2024 where video was requested by the Police Department for use in any investigations.

Ives Park – There are 4 closed circuit video surveillance cameras deployed on the exterior of the Ives Park pool facility. That facility is managed by the pool board. All cameras record video and the video is available for retrieval for 30 days. There have been no instances since the implementation of the ordinance where video was required to be downloaded and utilized for criminal prosecutions or other means.

Historical Society Building – There are 4 closed circuit video surveillance cameras deployed on the exterior of the Historical Society building which is owned by the city. All cameras record video and the video is available for retrieval for 30 days. There have been no instances since the implementation of the ordinance where video was required to be downloaded and utilized for criminal prosecutions or other means.

Police Department – There are 12 closed circuit video surveillance cameras located at the police department. Four of the cameras are deployed to view the exterior of the building. The remaining 8 cameras were deployed to provide constant surveillance of the jail cells and booking areas. However, we have rendered our jail inoperable and have decertified it for use with BSCC. The system cannot record and video is not retrievable. The system is obsolete technology and we have explored options to update to a modern system that meets security needs for the police department and the people who come into the police station. Information obtained from the system was not utilized for any investigative or prosecutorial purposes since the implementation of the ordinance or during 2024.

The Sebastopol Police Department requires all officers to wear body worn cameras which shall be activated during any type of enforcement, investigative activities or during transports. The cameras do not utilize any prohibited technologies and are strictly video recording devices. Cameras are not required to be activated during casual, friendly interactions with the public. Sebastopol Police Department policy number 417 outlines the usage of body worn cameras for our personnel. We currently have 16 Axon body worn cameras in inventory. The videos recorded by the cameras are uploaded to cloud storage seamlessly when the cameras are docked post shift in their charging docks. The videos are

retrievable via software and can be shared with the District Attorney, Public Defender and Probation Offices via secured electronic means, when requested for review in determining prosecution and evidentiary value. The videos can also be downloaded to be provided to comply with Public Records Act requests and requests by attorneys, both civil and defense, when those requests comply with existing laws.

Generally, any case that is submitted to the D.A. for review for prosecution will have an accompanying request from the D.A., Probation Department, or the Public Defender's Office for any and all body worn camera video associated with the case. During calendar year 2023, there were approximately 154 requests for body worn camera footage, and we provided approximately 270 separate videos based upon those requests. Due to the departure of our Records Supervisor, 2024 numbers are unavailable at this time but are likely very similar to 2023.

We have a contract with Axon, Inc. which covers the cloud storage for all video, maintenance, and replacement of any cameras that become inoperable. That contract runs through December 2027. The cost for the year 2025 is $14,194,41. Essentially it costs approximately $1,000 per year per officer to outfit them with body-worn cameras and pay for the storage for all of their videos. The annual cost for that contract was negotiated to remain static and achieve cost savings through the life of the contract. The annual amount will remain the same through 2027.

Additional Required Reporting Information

There have been no community complaints regarding the surveillance technology in use. This includes the use of body worn cameras by the police department.

Audits of police body worn camera videos do randomly occur to ensure that officers are complying with policy and law. Additional reviews are conducted regarding all use of force incidents, complaint allegations, or suspected policy violations.

Regarding the building surveillance systems throughout the city, there have been no audits conducted. There have been no violations of the surveillance technology ordinance. There have been no Public Records Act requests regarding the building surveillance technology in currently in use. Police body worn camera video is requested frequently as explained in the previous section.

All of the building surveillance camera systems currently in use are in good condition overall with the exception of the police building system, and absent any unanticipated repair or maintenance costs, there will be no expenditures in the coming year.

There currently are no requests for modification to the ordinance and no pending requests from any city departments for the purchase and/or use of any additional surveillance. technology.

Chapter 8.80
SURVEILLANCE TECHNOLOGY AND COMMUNITY SAFETY ORDINANCE

Sections:

8.80.010 Title.

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 First, Fourth, and Fourteenth Amendments to the United States Constitution, as well as Sections 1, 2, and 13 of Article I 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 8.80.030 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 8.80.030. 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 8.80.030 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

4. 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)