ORDINANCE NO. NS-300.994

AN ORDINANCE OF THE BOARD OF SUPERVISORS OF THE COUNTY OF SANTA CLARA AMENDING DIVISION A40 OF THE COUNTY OF SANTA CLARA ORDINANCE CODE RELATING TO SURVEILLANCE TECHNOLOGY AND COMMUNITY SAFETY

Summary

This Ordinance amends Division A40 provisions relating to the acquisition and operation of surveillance technology.

THE BOARD OF SUPERVISORS OF THE COUNTY OF SANTA CLARA ORDAINS AS FOLLOWS:

Division A40 of the Ordinance Code of the County of Santa Clara relating to Surveillance Technology and Community Safety is hereby amended to read as follows:

DIVISION A40
SURVEILLANCE TECHNOLOGY AND COMMUNITY SAFETY

Sec. A40-1. Findings.

The California Constitution provides that all people have an inalienable right to privacy, which is just as explicitly described in the California Constitution as the right to enjoy and defend life and liberty; the right to acquire, possess, and protect property; and the right to pursue and obtain safety and happiness. State and federal courts, including both the California Supreme Court and the United States Supreme Court, have affirmed individuals' fundamental right to privacy, and the Board finds that protecting and safeguarding this right is a vital part of its duties. Acknowledging the significance of protecting the privacy of County residents, the Board finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes.

To balance the public's right to privacy with the need to promote and ensure community safety, the Board finds that any decision to use surveillance technology must be judiciously balanced with an assessment of the costs to the County and the protection of privacy, civil liberties, and civil rights. The Board finds that proper transparency,

oversight, and accountability are fundamental to minimizing the risks posed by surveillance technologies. The Board finds that a risk-based approach to the evaluation and oversight of surveillance technology is essential to fostering responsible and effective administration of this Division.

The Board finds it essential to have safeguards in place to address potential privacy, civil liberties, and civil rights issues before any new surveillance technology is deployed. The Board finds that if surveillance technology that has a significant potential impact on privacy, civil liberties, and civil rights is acquired and deployed, there must be continued oversight and regular evaluation to ensure that safeguards are being followed and that the Board is assessing the surveillance technology's benefits and potential benefits in addition to its costs and potential costs.

Sec. A40-2. Risk Assessment of Surveillance Technology; Board Approval Requirement for Acquisition and Operation of Higher-Risk Surveillance Technology, and for Related Surveillance Use Policy; and Surveillance Use Policy for Medium-Risk Surveillance Technology

(a) Before engaging in any activities described in subsection (b) or (c), as applicable, a County department shall consult with the County Executive or designee. The County Executive or designee shall determine, after consultation with the County Counsel or designee, whether the surveillance technology is higher-, medium-, or low-risk surveillance technology. If the surveillance technology is higher- or medium-risk surveillance technology, the County department must comply with the requirements in subsection (b) or (c), as applicable.

Examples of factors the County Executive or designee may consider in determining whether a surveillance technology is higher-, medium-, or low-risk surveillance technology include:

(1) Privacy Impact: Whether the technology collects or shares sensitive personal information, including special categories of data (e.g., biometrics, financial, medical, or precise locational data).

(2) Civil Liberties and Civil Rights Concerns: Whether the technology risks infringing upon freedoms, such as the freedom of speech, movement, or assembly, and whether existing law addresses any civil liberties or civil rights concerns.

(3) Prevalence of Technology: Whether use of the technology is widespread or commercially available to the general public.

(4) Security Vulnerabilities: Whether the technology uses outdated, insecure, or poorly maintained systems or the technology was manufactured in or sourced from locations with non-stringent cybersecurity standards or that are known to present security concerns.

(5) Data Sharing Risk: Whether the technology allows for broad or unrestricted sharing of data with third parties or grants access to County systems without adequate monitoring, anonymization practices, or evaluation of the privacy-related risks associated with the data sharing.

(6) Compliance History: Whether there have been frequent violations of law, policies, or guidelines associated with the use of the technology.

The County Executive or designee, at their sole discretion, may change a surveillance technology's risk level based on these and related factors.

(b) County Departments Other than the Office of the Sheriff and the Office of the District Attorney. Each County department other than the Office of the Sheriff and the Office of the District Attorney must obtain Board approval at a properly noticed public meeting before any of the following with respect to higher-risk surveillance technology, and must obtain approval from the County Executive or designee before any of the following with respect to medium-risk surveillance technology:

(1) Seeking funds for surveillance technology, including, but not limited to, applying for a grant, or accepting state or federal funds or in-kind or other donations;

(2) Acquiring new surveillance technology, including, but not limited to, procuring that technology without the exchange of monies or other consideration;

(3) Using surveillance technology for a purpose, in a manner, or in a location not previously approved under this subdivision; or

(4) Entering into an agreement with a non-County entity to acquire, share, or

otherwise use surveillance technology or the information it provides.

Those County departments must also obtain Board approval of a Surveillance Use Policy at a properly noticed public meeting before engaging in any activities described in subsections (b)(2), (b)(3), and (b)(4) with respect to higher-risk surveillance technology.

Those County departments must develop a Surveillance Use Policy and obtain County Executive or designee approval of the Surveillance Use Policy before engaging in any activities described in subsections (b)(2), (b)(3), and (b)(4) with respect to medium-risk surveillance technology.

(c) Office of the Sheriff and Office of the District Attorney. Other than with respect to surveillance technology limited to use in law enforcement investigations and prosecutions as specifically defined in Section A40-9 of this Division, and subject to subsections (d) through (f) below, the Office of the Sheriff and Office of the District Attorney must notify the Board, and obtain Board approval, at a properly-noticed public meeting before any of the following with respect to higher-risk surveillance technology and must obtain approval from the County Executive or designee before any of the following with respect to medium-risk surveillance technology:

(1) Seeking funds for surveillance technology, including, but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;

(2) Acquiring new surveillance technology, including, but not limited to, procuring that technology without the exchange of monies or other consideration;

(3) Using surveillance technology for a purpose, in a manner, or in a location not previously approved under this subdivision; or

(4) Entering into an agreement with a non-County entity to acquire, share, or otherwise use surveillance technology.

The Office of the Sheriff and the Office of the District Attorney must also notify the Board, and obtain Board approval, of a Surveillance Use Policy at a properly noticed public meeting before engaging in any activities described in subsections

(c)(2), (c)(3), and (c)(4) with respect to higher-risk surveillance technology.

The Office of the Sheriff and the Office of the District Attorney must develop a Surveillance Use Policy and obtain County Executive or designee approval of the Surveillance Use Policy before engaging in any of the activities described in subsections (c)(2), (c)(3), and (c)(4) with respect to medium-risk surveillance technology.

(d) In enacting this Division, the Board is not limiting its rights under Government Code section 25303, including without limitation, its right to supervise the official conduct of all county officers, to require reports, or to exercise budgetary authority over the District Attorney and Sheriff.

(e) Consistent with California Government Code section 25303, however, in receiving notification and approving or denying the actions in subsections (c)(1), (c)(2), (c)(3), and (c)(4), and approving and/or denying any Surveillance Use Policy, the Board shall not "obstruct the investigative function of the sheriff of the county nor shall it obstruct the investigative and prosecutorial function of the district attorney."

(f) With respect to higher-risk surveillance technology, to the extent the Board or a court of law determines that approving or denying the actions in subsections (c)(1), (c)(2), (c)(3), or (c)(4), or approving or denying the Surveillance Use Policy would unlawfully "obstruct" the applicable function of the Sheriff or District Attorney under Government Code section 25303, the Board shall simply receive and discuss notification from the Office of the Sheriff or Office of the District Attorney regarding subsections (c)(1), (c)(2), (c)(3), or (c)(4) and receive and discuss the applicable Surveillance Use Policy at a properly-noticed public meeting. With respect to medium-risk surveillance technology, if after consultation with the County Counsel, the County Executive believes that such matter is covered by this subsection, the County Executive may bring the item to the Board to be received and discussed at a properly noticed public meeting.

Sec. A40-3. Submission of Higher-Risk Surveillance Technology Surveillance Use Policy

Unless it is not reasonably possible or feasible to do so (e.g., exigent circumstances, a natural disaster, or technological problems prevent it), the County department seeking Board approval under Section A40-2 of this Division with respect to

higher-risk surveillance technology must submit to the Board a proposed Surveillance Use Policy before the public meeting, which shall be made publicly available.

Sec. A40-4. Determination that Benefits Outweigh Costs and Concerns

Before approving any action described in Sections A40-2(b) and A40-2(c) of this Division with respect to higher-risk surveillance technology, the Board shall assess whether the benefits to the impacted County department(s) and the community of the higher-risk surveillance technology outweigh the costs—including both the financial costs and reasonable concerns about the impact on and safeguards for privacy, civil liberties, and civil rights.

Sec. A40-5. Compliance for Existing Surveillance Technologies

(a) Each Surveillance Use Policy approved by the Board prior to April 1, 2025, and that is for higher-risk surveillance technology shall remain in effect unless the Board approves a new Surveillance Use Policy for the surveillance technology, pursuant to Section A40-2, that replaces the prior Surveillance Use Policy or the Board otherwise invalidates the Surveillance Use Policy.

(b) Each Surveillance Use Policy approved by the Board prior to April 1, 2025, and that is for medium-risk surveillance technology shall remain in effect unless the County Executive or designee approves a new Surveillance Use Policy, pursuant to Section A40-2, that replaces the prior Surveillance Use Policy or the County Executive or designee otherwise invalidates the Surveillance Use Policy.

(c) Each Surveillance Use Policy approved by the Board prior to April 1, 2025, and that is for low-risk surveillance technology shall be repealed effective April 1, 2025.

(d) If any section, subsection, paragraph, sentence, clause, or phrase of a Surveillance Use Policy approved prior to the effective date of the Ordinance that added this subsection and that is for higher-risk or medium-risk surveillance technology is for any reason inconsistent with any section, subsection, paragraph, sentence, clause, or phrase of this Division, the inconsistent section, subsection, paragraph, sentence, clause, or phrase of the Surveillance Use Policy shall be invalid and the remaining parts of the Surveillance Use Policy shall remain fully effective.

//

Sec. A40-6. Annual Review by the Board

(a) The County Executive or designee shall submit an Annual Surveillance Report to the Board annually. This report shall list each Surveillance Use Policy for high-risk surveillance technology the Board approved or received pursuant to Section A40-2. For each surveillance technology categorized as medium- or low-risk surveillance technology by the County Executive or designee in the prior fiscal year, the Annual Surveillance Report shall describe the surveillance technology and its intended use(s).

(b) The Board shall hold a public meeting with the Annual Surveillance Report agendized.

Sec. A40-7. Definitions

The following definitions apply to this Division:

(a) "**Annual Surveillance Report**" means a written report concerning specific surveillance technology that includes all of the following information for the prior fiscal year:

(1) A list of all Surveillance Use Policies approved or received by the Board pursuant to Section A40-2;

(2) A description and the intended uses(s) of each surveillance technology the County Executive or designee determined is medium- or low-risk surveillance technology;

(3) A list of all changes to assigned risk level (i.e., higher-, medium-, or low-risk) for surveillance technology and a brief explanation for the change;

(4) A summary of significant non-compliance issues that impact(ed) privacy, civil liberties, or civil rights, and any action taken to address the issues; and

(5) With respect to higher-risk surveillance technology:

(i) Whether and, if so, how often data acquired through the use of the

surveillance technology was shared with outside entities; the name of any recipient entity or entities; how often the data was shared; the type(s) of data disclosed; and the justification for the disclosure;

(ii) A summary of any written community complaints or concerns about the surveillance technology;

(iii) The results of any non-privileged internal audits, County department self-assessments, or assessments conducted by the County Executive or designee; and

(iv) A brief assessment of whether the surveillance technology has been effective at achieving its identified purpose.

(b) "**County department**" means any County department with a recognized County budget unit.

(c) "**Surveillance technology**" means any electronic device, system using an electronic device, or similar technology that is used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometrics, neural, or similar information specifically associated with, or capable of being associated with, any individual or group.

Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers (ALPRs), closed-circuit cameras/televisions (CCTV), cell-site simulators, International Mobile Subscriber Identity (IMSI) trackers, Global Positioning System (GPS) technology, radio-frequency identification (RFID) technology, biometrics-identification technology, and facial-recognition technology.

Surveillance technology does not include, for example:

(1) Prevalent Technology: Smartphones or general consumer electronics, including cell phones with cameras, microphones, or monitoring capabilities commonly included in commercially available cell phones; and digital recording devices, when used with the consent of those recorded; but excluding drones and other technology expressly included in the definition of surveillance technology.

(2) Standard Physical Security Tools: Basic security systems such as locks, keycard or badge readers, password-access technology, metal detectors, and standard motion sensors without biometrics functionality.

(3) Standard Business Software and Hardware: Standard business software (e.g., word processors) and standard business hardware (e.g., standard computers).

(4) Information-Technology-Protection Tools: Information-technology-protection tools including, but not limited to, firewalls and antivirus software.

(5) Medical Equipment: Devices used to diagnose, treat, or prevent disease or injury.

(6) County Data Repositories and Publicly Available Databases: County department data repositories, including, but not limited to, case and record management systems, and publicly available databases.

(7) Non-Digital Observation Tools: Non-digital observation tools used for direct observation without recording capabilities, including, but not limited to, binoculars, telescopes, and night vision goggles.

(8) Communication and Financial Transaction Systems: Standard telephone equipment or systems; standard voicemail equipment or systems; and equipment used to process financial transactions (e.g., credit, debit, and ACH payments).

(d) "**Surveillance Use Policy**" means a policy for use of higher-risk or medium-risk surveillance technology, vetted through the County Executive and the County Counsel, or their designees. With respect to higher-risk surveillance technology, the Surveillance Use Policy shall at a minimum specify the following:

(1) Purpose: The specific purpose(s) for the surveillance technology.

(2) Authorized Use and Deployment Location: Permitted uses, the rules and processes required before those uses, and the location(s) the technology may be deployed.

(3) Data Collection: The information and data elements that the technology collects, including metadata.

(4) Data Access: The individuals who can access or use the collected information, and the rules and processes governing access or use.

(5) Data Protection: The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access controls, and access oversight mechanisms.

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

(7) Public Access: If and how collected information can be accessed by members of the public, including criminal defendants.

(8) Third-Party Data-Sharing: If and how other County or non-County entities can access or use the information, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the information.

(9) Training: The training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials.

(10) Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including, but not limited to, personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy.

(e) "**Exigent circumstances**" means the County Office of the Sheriff's or Office of the District Attorney's good faith belief that an emergency involving danger of death or serious physical injury to any person requires use of the surveillance technology or the information it provides.

Sec. A40-8. Additional Review by Office of Correction and Law Enforcement Monitoring.

With respect to higher-risk surveillance technologies used specifically for law enforcement or jail-related purposes, the Office of Correction and Law Enforcement Monitoring (OCLEM) shall assist the County Executive and the County Counsel, or their designees, in the vetting required by this Division. This Section shall not apply to Countywide Surveillance Use Policies that are also applicable outside the law enforcement or jail context.

Sec. A40-9. Temporary Acquisition and Use of Surveillance Technology Related to Law Enforcement Investigations and Prosecutions

Notwithstanding anything in this Division to the contrary, the Office of the Sheriff and Office of the District Attorney may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this Division before that acquisition or use unless a State law or federal law preempts or conflicts with this exigent-circumstances exception in any manner (e.g., Civil Code section 1798.90.5 et seq.; Government Code section 53166). However, if the Office of the Sheriff or Office of the District Attorney acquires or uses surveillance technology in exigent circumstances under this Section, that Office must report that acquisition or use to the County Executive or designee within 15 days of the acquisition or use. If the County Executive or designee determines that the technology is higher-risk surveillance technology, the Office of the Sheriff or Office of the District Attorney must (1) report the acquisition or use to the Board of Supervisors in writing within 120 days following the end of those exigent circumstances or within 120 days following the County Executive's or designee's determination that the technology is higher-risk surveillance technology, whichever is later; and (2) submit a proposed Surveillance Use Policy to the Board within 120 days following the end of those exigent circumstances or within 120 days following the County Executive's or designee's determination that the technology is higher-risk surveillance technology, whichever is later. The County Executive or designee must include the surveillance technology in the next Annual Surveillance Report to the Board following the end of those exigent circumstances. If the Office of the Sheriff or Office of the District Attorney is unable to meet the 120-day timeline to submit a proposed Surveillance Use Policy to the Board, that Office may notify the Board in writing of the Office's request to extend this period and the reasons for that request. The Board may grant extensions of up to 90 days beyond the original 120-day timeline to submit a proposed Surveillance Use Policy.

Sec. A40-10. Enforcement

This Division does not confer any rights upon any person or entity other than the Board of Supervisors or its designee to seek the cancellation or suspension of a County contract. This Division does not confer any rights to damages or any monetary relief. This Division does not confer a private right of action upon any person or entity to seek injunctive relief against the County or any individual unless that person or entity has first provided written notice to the County Executive and the Board of Supervisors, by serving the Clerk of the Board, regarding the specific alleged violation of this Division; and has provided the County Executive and the Board with at least 90 days to investigate and achieve compliance regarding any alleged violation. If the specific alleged violation is not remedied within 90 days of that written notice, a person or entity may seek injunctive relief in a court of competent jurisdiction. If it is shown that the violation is the result of arbitrary or capricious action or conduct by the County or an officer thereof in their official capacity, the prevailing complainant in an action for injunctive relief may collect from the County reasonable attorney's fees—computed at one hundred dollars ($100) per hour, but not to exceed seven thousand five hundred dollars ($7,500) in total—if they are personally obligated to pay the fees. However, a prevailing complainant may not recover attorney's fees under this Section and under Government Code section 800 for the same arbitrary or capricious action or conduct.

Sec. A40-11. Retaliation is a Ground for Discipline

It shall be a ground for disciplinary action for a County employee to retaliate against any individual who makes a good-faith complaint to the County Executive, County Counsel, or pursuant to Chapter 7 of Division A25, that there has been a failure to comply with any part of this Division.

//

//

//

//

//

Sec. A40-12. Administrative Policies

The County Executive is authorized to issue administrative policies and guidelines to interpret or enforce this Division, and to define or address any ambiguities herein.

PASSED AND ADOPTED by the Board of Supervisors of the County of Santa Clara, State of California, on FEB 2 5 2025 by the following vote:

AYES: Abe-Koga, Arenas, Duong, Ellenberg, Lee

NOES: NONE

ABSENT: NONE

ABSTAIN: NONE

OTTO LEE, President
Board of Supervisors

Signed and certified that a copy of this
document has been delivered by electronic
or other means to the President, Board of Supervisors.
ATTEST:

CURTIS BOONE
Acting Clerk of the Board of Supervisors

APPROVED AS TO FORM AND LEGALITY:

SOHAYL VAFAI
Deputy County Counsel