

ORDINANCE NO. _____
AN ORDINANCE OF THE BOARD OF SUPERVISORS OF THE COUNTY OF ALAMEDA ADDING CHAPTER ##### TO THE ALAMEDA COUNTY ADMINISTRATIVE CODE REGARDING COUNTY USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the Board of Supervisors finds that any decision to use surveillance technology must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the County;

WHEREAS, the Board of Supervisors finds that proper transparency, oversight and accountability for the acquisition and use of surveillance technology is fundamental to protecting the rights and civil liberties, including privacy and free expression, of all people;

WHEREAS, the Board of Supervisors finds it essential to have an informed public debate as early as possible about whether to acquire and use surveillance technology;

WHEREAS, the Board of Supervisors finds it necessary that safeguards be in place to protect civil liberties and civil rights before any surveillance technology is deployed.

WHEREAS, the Board of Supervisors finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs;

NOW, THEREFORE, THE BOARD OF SUPERVISORS OF THE COUNTY OF ALAMEDA DOES HEREBY ORDAIN AS FOLLOWS:

SECTION 1. Chapter ##### is hereby added to the Alameda County Administrative Code to read as follows:

1.1 Purpose and Findings.

This Article shall be known as the Surveillance Technology Ordinance.

The purpose and intent of this Article is to impose safeguards to protect civil liberties and civil rights before any surveillance technology is deployed.

The Board of Supervisors finds that any decision to use surveillance technology must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the County.

The Board of Supervisors finds that proper transparency, oversight and accountability for the acquisition and use of surveillance technology is fundamental to protecting the rights and civil liberties, including privacy and free expression, of all people.

The Board of Supervisors finds it essential to have an informed public debate as early as possible about whether to acquire and use surveillance technology.

The Board of Supervisors finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs.

1.2 Definitions.

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

“Annual Surveillance Report” means an annual written report concerning a specific surveillance technology.

(a) The Annual Surveillance Report will include all of the following:

- (1) A general description of how the surveillance technology was used; including the type and quantity of data gathered or analyzed by the technology;
- (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 the 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 Board of Supervisors assess whether the surveillance technology has been effective at achieving its identified purposes;
- (6) Statistics and information about any related Public Records Act requests;
- (7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology 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 the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to;
- (10) Where applicable, a breakdown of where the Surveillance Technology was deployed geographically, by each Police Beat or other similar metric.

(b) The Annual Surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes.

“County Department” means all County agencies, departments, officers, and employees. For purposes of this ordinance “County Department” includes the Alameda County Sheriff’s Office and the Alameda County District Attorney’s Office.

“Exigent Circumstances” A County department’s good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires the use of the surveillance technology or the information it provides.

“Personal Communication Device” means a cellular telephone, 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 County entity or personally owned, that is used in the regular course of conducting County business, and that has not been modified beyond stock manufacturer capabilities to become Surveillance Technology.

“Surveillance” or **“surveil”** means to observe or analyze the movements, behavior, data, or actions of individuals or groups. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

“Surveillance Impact Report” means a written report including at a minimum the following:

- (a) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
- (b) Information on the proposed purpose(s) for the surveillance technology;
- (c) If applicable, the location(s) it may be deployed using general descriptive terms, and crime statistics for any location(s);
- (d) An assessment identifying any potential impact on civil liberties and civil rights and discussion of the technology’s proposed use policy and whether it is adequate in protecting civil rights and civil liberties;
- (e) Identify, specific, affirmative technical and procedural mitigation measures that will be implemented to safeguard the public from each such impact;
- (f) A list of all types and sources of data to be collected, analyzed, or processed by the technology, including “open source” data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
- (g) Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

(h) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

(i) 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;

(j) A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate or undesirable; and

(k) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, 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, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group by a County department. Examples of surveillance technology includes but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; gait analysis software; software designed to monitor social media services, software designed to forecast criminal activity or criminality, biometric identification hardware and software, and video cameras that record audio or video and can transmit or be remotely accessed.

“**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 County departments and used for routine County business and transactions;

(2) County databases and enterprise systems that contain information kept in the ordinary course of County business, including, but not limited to, human resource, permit, license and business records;

(3) County 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 County and department communications and are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices and email systems;
- (8) Manually-operated, non-wearable, 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 County buildings, employees, contractors and volunteers or used in conducting internal investigations involving County employees, contractors and volunteers;
- (11) Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the ordinary course of providing County services;
- (12) Parking Ticket Devices;
- (13) A law enforcement department's interview room, holding cell and police department internal security audio/video recording systems;
- (14) A law enforcement department's 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;
- (15) A law enforcement department's early warning systems.

“Surveillance Use Policy” means a policy adopted by the Board of Supervisors at a regularly scheduled Board of Supervisors meeting for use of the surveillance technology that at a minimum specifies the following:

- (a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.
- (b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
- (c) Data Collection: The information that can be collected by the surveillance technology, including “open source” data.
- (d) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the County.

(f) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), 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.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

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

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

(j) 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 to 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.

1.3 Board of Supervisors Approval.

1. COUNTY DEPARTMENTS OTHER THAN SHERIFF AND DISTRICT ATTORNEY.

(a) Other than the Sheriff's Department or District Attorney's Department, a County department shall obtain Board of Supervisors approval at a public hearing conducted at a regular Board of Supervisors meeting prior to any of the following:

(1) Seeking funds for 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;

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

(3) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the Board of Supervisors pursuant to this Ordinance; or

(4) Entering into a continuing or written agreement with a non-County entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

(b) A County department shall obtain Board of Supervisors approval at a public hearing conducted at a regular Board of Supervisors meeting of a Surveillance Use Policy prior to engaging in any of the activities described in subsection 1(a)(2)-(4).

(c) The County department seeking approval under subsection 1(a) shall submit to the Board of Supervisors a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular Board of Supervisors meeting consent calendar at least thirty (30) days prior to the public hearing required under subsection 1(a). The informational staff report shall be posted on the County website with the Board of Supervisors agenda.

(d) The Board of Supervisors may approve any action described in subsection 1(a) or 1(b) or described in Section 1.4 below, after making a determination that any decision to use a surveillance technology item has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the County; that the proposed use policy will reasonably safeguard civil liberties and civil rights, and that the benefits to the community from use of the technology outweigh the costs.

2. SHERIFF'S DEPARTMENT AND DISTRICT ATTORNEY'S DEPARTMENT.

(a) The Sheriff's Department or District Attorney's Department shall obtain Board of Supervisors approval following a public hearing conducted at a regular Board of Supervisors meeting prior to any of the following:

(1) Seeking funds for 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;

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

(3) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the Board of Supervisors pursuant to this Ordinance; or

(4) Entering into a formal written agreement with a non-County entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

(b) The Sheriff's Department or District Attorney's Department shall obtain Board of Supervisors approval following a public hearing conducted at a regular Board of Supervisors meeting of a Surveillance Use Policy prior to engaging in any of the activities described in subsection 2(a)(2)-(4).

(c) The Sheriff's Department or District Attorney's Department seeking approval under subsection 2(a) shall submit to the Board of Supervisors a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular Board of Supervisors meeting consent calendar at least thirty (30) days prior to the public hearing required under subsection 2(a). The informational staff report shall be posted on the County website with the Board of Supervisors agenda.

(d) The Board of Supervisors may approve any action described in subsection 2(a) or 2(b) or described in Section 1.4 below, after making a determination that any decision to use a surveillance technology item has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the County; that the proposed use policy will reasonably safeguard civil liberties and civil rights, and that the benefits to the community from use of the technology outweigh the costs.

(e) In enacting this Article, the Board of Supervisors is not limiting its rights under Government Code Section 25303, including but not limited to, 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.

(f) In receiving notification and approving or denying the actions in subsections 2(a) or 2(b), the Board of Supervisors shall remain consistent with Government Code Section 25303, and 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 of a county."

(g) To the extent a court of law determines that approving or denying the actions in subsections 2(a) or 2(b) would violate Government Code Section 25303, the Board of Supervisors shall simply receive and discuss notification from the Sheriff's Department or District Attorney's Department regarding subsections 2(a) or 2(b) at a properly-noticed public meeting, on the regular (non-consent) calendar.

1.4 Compliance for Existing Surveillance Technology

(a) A County department possessing or using surveillance technology prior to the effective date of this Article shall submit a proposed Surveillance Use Policy no later than one hundred twenty (120) days following the effective date of this Article for review and approval by the Board of Supervisors pursuant to Section 1.3. If such review and approval has not occurred within four regular meetings from when the item was initially scheduled for Board of Supervisors consideration, a County department shall cease its use of the surveillance technology until such review and approval occurs.

(b) If a court of law determines that approving or denying a Surveillance Use Policy in subsection (a) would violate Government Code Section 25303, the Board of Supervisors shall simply receive and discuss the applicable Sheriff's Department or District Attorney's

Department proposed Surveillance Use Policy at a properly-noticed public meeting, on the regular (non-consent) calendar.

1.5 Use of Unapproved Technology During Exigent Circumstances

A County department may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this Article before that acquisition or use. If the County department acquires or uses a surveillance technology pursuant to this Section, the County department shall do all of the following:

- (a) Use the surveillance technology to solely respond to the exigent circumstances;
- (b) Cease using the surveillance technology within seven days or when the exigent circumstances ends, whichever is sooner;
- (c) Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation unless retention is (i) authorized by a court based on a finding of probable cause to believe the information constitutes evidence of a crime or (ii) otherwise required by law;
- (d) Not disclose to any third party any information acquired during exigent circumstances, unless disclosure is (i) for purposes of responding to the emergency and the third party agrees to be bound by the restrictions in this Section or (ii) otherwise required by law;
- (e) Within 30 days following the end of the exigent circumstances report the acquisition or use to the Board of Supervisors at a regular Board of Supervisors meeting for discussion and/or possible recommendation for approval to acquire or use the surveillance technology; and
- (f) Any technology temporarily acquired in exigent circumstances shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the Board of Supervisors for approval pursuant to Section 1.3 and is approved.

1.6 Oversight Following Council Approval

- (a) By the end of each fiscal year, each County department that uses surveillance technology must present a written Annual Surveillance Report at a regular Board of Supervisors meeting for Board of Supervisors review for each surveillance technology item. If the County department is unable to meet the deadline, the department head shall notify the Board of Supervisors in writing of staff's request to extend this period, and the reasons for that request. The Board of Supervisors may grant reasonable extensions to comply with this Section.

(b) Based upon information in the Annual Surveillance Report, the Board of Supervisors will, at a regular Board of Supervisors meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the County and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

(c) If a court of law determines that the determination to be made in (b) above would violate Government Code Section 25303, the Board of Supervisors shall simply receive and discuss the applicable Sheriff's Department or District Attorney's Annual Surveillance Report at a properly-noticed public meeting, on the regular (non-consent) calendar.

1.7 Prevention of Secret Surveillance Technology Contracts and Agreements

It shall be unlawful for any County Department to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the County shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

1.8 Enforcement

(a) Any violation of this Article 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 Article. An action instituted under this paragraph shall be brought against the County of Alameda, and if necessary to effectuate compliance with this Article or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third party, except a County employee, with possession, custody, or control of data subject to this Article.

(1) Prior to the initiation of any legal proceeding under subsection (a), the County of Alameda 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.

(2) If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous space on the County's website that generally describes the corrective measure(s) taken to address the violation(s).

(b) A court shall award costs to the prevailing plaintiff in any action brought to enforce this Article and any reasonable attorney's fees as may be awarded pursuant to State law.

(c) Nothing in this Article 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.

1.9 Whistleblower Protections

(a) Neither the County nor anyone acting on behalf of the County 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 Ordinance; 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 Ordinance.

(3) It shall be grounds for disciplinary action for a County employee or anyone else acting on behalf of the County to retaliate against another County 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 Ordinance.

(4) 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 County in any court of competent jurisdiction.

1.10 Severability

The provisions of this Article are declared to be separate and severable. The invalidity of any clause, phrase, sentence, paragraph, subdivision, section or portion of this Article, or the invalidity of the application thereof to any person or circumstance shall not affect the validity of the remainder of this Article, or the validity of its application to other persons or circumstances.

SECTION 2. The County Clerk shall certify to the adoption of this Ordinance and shall cause the same or a summary thereof to be published as required by law.

SECTION 3. This Ordinance shall take effect and be in full force and effect thirty (30) days from and after the date of its final passage and adoption.

INTRODUCED on the ___ day of _____, 2018, and PASSED AND ADOPTED by the County of Alameda on this _____ day of _____, 2018, by the following vote:

AYES:

NOES:

ABSTAIN:

ABSENT: