SURVEILLANCE TOOLKIT: MODEL LEGISLATION FOR A SURVEILLANCE TECHNOLOGY & COMMUNITY SAFETY ORDINANCE

KEY PRINCIPLES OF THE MODEL ORDINANCE

- **Informed Public Debate at Earliest Stage of Process**: Public notice, distribution of information about the proposal, and public debate prior to seeking funding or otherwise moving forward with surveillance technology proposals.
- **Determination that Benefits Outweigh Costs and Concerns**: Local leaders, after facilitating an informed public debate, expressly consider costs (fiscal and civil liberties) and determine that surveillance technology is appropriate or not before moving forward.
- **Thorough Surveillance Use Policy**: Legally enforceable Surveillance Use Policy with robust civil liberties, civil rights, and security safeguards approved by policymakers.
- **Ongoing Oversight & Accountability:** Proper oversight of surveillance technology use and accountability through annual reporting, reviewed by policymakers, and enforcement mechanisms.

MODEL ORDINANCE TEXT

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF ######## ADDING ARTICLE ####

OF THE ######## MUNICIPAL CODE REGARDING OVERSIGHT OF THE CITY'S ACQUISITION AND/OR USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the City Council finds it essential to have an informed public debate as early as possible about decisions related to surveillance technology.

WHEREAS, the City Council finds that 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.

WHEREAS, the City Council finds that, 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.

WHEREAS, the City Council finds that decisions regarding if and how surveillance technologies should be funded, acquired, or used, and whether data from such technologies should be shared, should not be made until meaningful public input has been solicited and given significant weight.

WHEREAS, the City Council finds 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; and

WHEREAS, the City Council finds that, if a surveillance technology is approved, 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.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF ######## DOES HEREBY ORDAIN AS FOLLOWS:

SECTION 1. Article #### is hereby added to ######## Municipal Code to read as follows:

1.1 Title.

This Article shall be known as the Surveillance Technology & Community Safety Ordinance.

1.2 City Council Review Mandatory for Surveillance Technology Decisions

(a) 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:

(1) 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;
(2) Acquiring or borrowing a new surveillance technology, including, but not limited to, acquiring such technology without the exchange of monies or consideration;
(3) Using new or existing a surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council in accordance with this Act; or
(4) Entering into an agreement, including a written and oral agreement, with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data-sharing agreements.

1.3 Surveillance Impact Report and Surveillance Use Policy Submission

(a) The City department seeking approval under Section 1.2(a) 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 forty-five (45) days prior to the public hearing, required under Section 1.2(a). The informational staff report shall be posted on the City website with the relevant City Council agenda at least thirty (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.

1.4 Standard for Approval

(a) The City Council shall only approve a request to fund, acquire, or use a surveillance technology under Section 1.2(a) of this Act 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.

1.5 Compliance for Existing Surveillance Technology

(a) A City department or departments possessing or using surveillance technology prior to the effective date of this Article shall submit or jointly 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 City Council pursuant to Sections 1.2.
(b) If a City department is unable to meet this 120-day timeline, the Department may notify the Board 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.
(c) If the City Council has not approved the continuing use of surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy, within one hundred eighty (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 Act.

1.6 Oversight Following Council Approval

(a) A City department that obtains approval under Section 1.2 of this Act 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 twelve (12) months of Board approval, and annually thereafter on or before November 1. 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 Section 1.4. 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 Board's concerns; and/or (3) directing a report-back from the department regarding steps taken to address the Board's concerns.

1.7 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 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. Conflicting provisions in contracts or agreements signed prior to the enactment of this Act 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 pre-date this Act.

(b) To the extent permitted by law, the City 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 City of ########, 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 city 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 City of ######## 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 City'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 Definitions

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

(a) "Annual Surveillance Report" means an annual written report concerning a specific surveillance technology. 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 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 City Council 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) A summary of all requests for City Council approval for the use of the 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.

(b) 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.
(c) “City Department” means any City department and its officers and employees.
(d) “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.
(e) “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) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;
(5) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
(6) An assessment identifying with specificity (1) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and (2) what specific, affirmative measures will be implemented to safeguard the public from those potential adverse impacts.
(7) 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
(8) 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.

(f) “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.

(1) “Surveillance technology” includes, but is not limited to: international mobile subscriber identity (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers; closed-circuit television cameras; gunshot detection hardware and services; video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; mobile DNA capture technology; biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; software designed to monitor social media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network.

(2) “Surveillance technology” does not include the following devices, hardware or software:

i. 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;

ii. 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;

iii. 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;

iv. Information technology security systems, including firewalls and other cybersecurity systems;

v. Physical access control systems, employee identification management systems, and other physical control systems;

vi. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

vii. 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;

viii. 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;

ix. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

x. 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;
xi. Parking Ticket Devices;
xii. Police department interview room, holding cell, and police department internal security audio/video recording systems;
xiii. 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;
xiv. Police department early warning systems.

(g) "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 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 that 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 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.

(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.

1.11 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 City 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 _____, 2020, and PASSED AND ADOPTED by the City

Council of the City of ####### on this _____ day of _____, 2020, by the following vote: