ORDINANCE NUMBER O-_____ (NEW SERIES)

DATE OF FINAL PASSAGE _____

AN ORDINANCE AMENDING CHAPTER 2, ARTICLE 6, DIVISION 00 OF THE SAN DIEGO MUNICIPAL CODE BY ADDING NEW SECTIONS 26.42 AND 26.43, ALL RELATING TO ESTABLISHING THE PRIVACY ADVISORY BOARD.

WHEREAS, the San Diego City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately monitored and regulated to protect the privacy and other rights of San Diego residents and visitors; and

WHEREAS, the Council proposes to create a new Charter section 43(a) citizen advisory board known as the Privacy Advisory Board to advise the Mayor and City Council on transparency, accountability, and public deliberation in the City's acquisition and usage of surveillance technology; and

WHEREAS, the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs; and

WHEREAS, while the City Council acknowledges an individuals' right to privacy, it also recognizes that surveillance technology may be a valuable tool to support community safety, investigations, and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, but also may include technology that aggregates publicly available information, which, in the aggregate or when pieced together with other information, has the potential to reveal details about a person's familial, political, professional, religious, or intimate associations; and

WHEREAS, awareness that the government may be watching may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, the City Council finds that safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before City surveillance technology is deployed; and

WHEREAS, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

WHEREAS, the City Council recognizes that prior to making a final determination on whether to approve the proposed ordinance creating the Privacy Advisory Board, the City must comply with the Meyers-Milias Brown Act (MMBA), California's collective bargaining law set forth at California Government Code sections 3500 through 3511, which is binding on the City; and

WHEREAS, the City Council also recognizes that depending on the outcome of the meet-and-confer process and the extent of any revisions to the proposed ordinance creating the Privacy Advisory Board resulting from that process, the City may be required to reintroduce the Proposed Surveillance Ordinance; NOW, THEREFORE,

BE IT ORDAINED, by the Council of the City of San Diego, as follows:

Section 1. Chapter 2, Article 6, Division 00 of the San Diego Municipal Code is amended by adding new sections 26.42 and 26.43 to read as follows:

§26.42 Privacy Advisory Board

(a) Purpose and Intent

It is the purpose and intent of the Council to establish a Privacy Advisory Board to serve as an advisory body to the Mayor and Council on policies and issues related to privacy and surveillance. The Board will provide advice intended to ensure transparency, accountability, and public deliberation in the *City's* acquisition and use of surveillance technology.

(b) There is hereby established a Privacy Advisory Board to consist of nine members, who shall serve without compensation. At least six members shall be residents of the City of San Diego. Members shall be appointed by the Mayor and confirmed by the Council.

(c) All terms appearing in italics in sections 26.42 and 26.43 have the same meaning as in Chapter 5, Article 11, Division, section 511.0101, known as the San Diego Transparent and Responsible Use of Surveillance Ordinance.

(d) Qualifications of Members

(1) All members of the Privacy Advisory Board shall be persons who have a demonstrated interest in privacy rights through work experience, civic participation, and/or political advocacy.

(2) The Mayor shall appoint the nine members from the following representative areas of organizational interest, expertise, and background:

(A) At least one attorney or legal scholar with expertise in privacy or civil rights, or a representative of an organization with expertise in privacy or civil rights;

(B) One auditor or certified public accountant;

(C) One computer hardware, software, or encryption security professional;

(D) One member of an organization that focuses on open government and transparency or an individual, such as a university researcher, with experience working on open government and transparency; and

(E) At least four members from equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.

(3) No member may have a state law prohibited financial interest, employment, or policy-making position in any commercial or for profit facility, research center, or other organization that sells data products, surveillance equipment, or otherwise profits from recommendations made by the Privacy Advisory Board.

(e) Terms

(1) Members shall serve two-year terms, and each member shall serve until a successor is duly appointed and confirmed. Members are limited to a maximum of eight consecutive years.

(2) Initial members shall be appointed in staggered terms. For the initial appointments, five members shall be appointed to an initial

term that will expire in 2021, and four members shall be appointed to an initial term that will expire in 2022. Initial appointments for less than the full term of two years shall not have the initial term count for purposes of the eight-year term limit.

(3) All terms shall expire on March 15 in the year of termination. Any vacancy shall be filled for the remainder of the unexpired term.

(f) Rules

(1) The Board shall adopt rules for the government of its business and procedures in compliance with the law. The Board rules shall provide that a quorum of the Privacy Advisory Board is five members.

(2) At the first regular meeting, and subsequently at the first regular meeting of each year, members of the Privacy Advisory Board shall select a chairperson and a vice chairperson.

§26.43 Privacy Advisory Board – Duties and Functions

The Privacy Advisory Board shall:

(a) Provide advice and technical assistance to the *City* on best practices to protect resident and visitor privacy rights in connection with the *City's* acquisition and use of s*urveillance technology*.

(b) Conduct meetings and use other public forums to collect and receive public input on the above subject matter.

(c) Review *Surveillance Impact Reports* and *Surveillance Use Policies* for all new and existing *surveillance technology* and make recommendations prior

to the City seeking solicitation of funds and proposals for *surveillance technology*.

(d) Submit annual reports and recommendations to the City Council regarding:

(1) The *City*'s use of *surveillance technology*; and

(2) Whether new *City surveillance technology* privacy and data retention policies should be developed, or existing policies should be amended.

(e) Provide analysis to the City Council of pending federal, state, and local legislation relevant to the *City*'s purchase and/or use of *surveillance technology*.

(f) The Privacy Advisory Board shall make reports, findings, and recommendations either to the City Manager or the City Council, as appropriate. The Board shall present an annual written report to the City Council. The Board may submit recommendations to the City Council following submission to the City Manager.

Section 2. That a full reading of this Ordinance is dispensed with prior to passage, a written copy having been made available to the Council and the public prior to the day of its passage.

Section 3. That this ordinance shall take effect and be in force on the thirtieth day from and after its final passage.

APPROVED: MARA W. ELLIOTT, City Attorney

By _____
Jennifer L. Berry
Deputy City Attorney

JLB:jvg

09/02/20
11/9/20 COR. COPY
Or.Dept: Council District 4
Doc. No.: 2516149_3

I hereby certify that the foregoing Ordinance was passed by the Council of the City of San Diego, at this meeting of _____.

ELIZABETH S. MALAND
City Clerk

By_____
Deputy City Clerk

Approved: _____ _____
(date) KEVIN L. FAULCONER, Mayor

Vetoed: _____ _____
(date) KEVIN L. FAULCONER, Mayor

ORDINANCE NUMBER O-_____ (NEW SERIES)

DATE OF FINAL PASSAGE _____

AN ORDINANCE AMENDING CHAPTER 5 OF THE SAN DIEGO MUNICIPAL CODE BY ADDING NEW ARTICLE 11, DIVISION 1, AND SECTIONS 511.0101, 511.0102, 511.0103, 511.0104, 511.0105, 511.0106, 511.0107, 511.0108, 511.0109, AND 511.0110, ALL RELATING TO TRANSPARENT AND RESPONSIBLE USE OF SURVEILLANCE TECHNOLOGY.

WHEREAS, on January 29, 2020, the City of San Diego's Sustainability Department introduced to the Public Safety and Livable Neighborhoods Committee (PS&LN Committee) a draft Council policy on Streetlight Sensor Data Use for discussion and recommendation; and

WHEREAS, the PS&LN Committee unanimously voted to reject the proposed policy and to instead move forward with a more comprehensive framework to address the City's use of surveillance technology; and

WHEREAS, on July 15, 2020, members of the TRUST SD Coalition presented a proposed draft ordinance related to the transparent and responsible use of surveillance technology (Proposed Surveillance Ordinance) to the Public Safety and Livable Neighborhoods Council Committee (PS&LN Committee) for review and approval; and

WHEREAS, the PS&LN Committee discussed the Proposed Surveillance Ordinance and voted unanimously to direct the City Attorney to work with the PS&LN Consultant and the Mayor's Office to prepare the legal review of the Surveillance Ordinance, and to draft an ordinance in the appropriate form using the substance of the ordinance docketed at the July 15, 2020 PS&LN Committee to be forwarded to the Council for discussion and consideration; and

WHEREAS, the San Diego City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately

monitored and regulated to protect an individual's right to privacy; and

WHEREAS, the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal details about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, awareness that the government may be watching may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain groups more than others, including those that are defined by a common race ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

WHEREAS, the City Council finds that safeguards, including robust transparency, oversight, and accountability measures must be in place to protect civil rights and civil liberties before the City deploys any surveillance technology; and

WHEREAS, the City Council has considered the Proposed Surveillance Ordinance in the form drafted by the Office of the City Attorney, which was heard at the Council meeting on November 10, 2020, and the Council wishes to incorporate any additional modifications approved by the Council from that meeting; and

WHEREAS, the City Council recognizes that prior to making a final determination on whether to approve the Proposed Surveillance Ordinance, the City must comply with the Meyers-Milias Brown Act (MMBA), California's collective bargaining law set forth at California Government Code sections 3500 through 3511, which is binding on the City; and

WHEREAS, the City Council also recognizes that depending on the outcome of the meet-and-confer process and the extent of any revisions to the Proposed Surveillance Ordinance resulting from that process, the City may be required to reintroduce the Proposed Surveillance Ordinance; NOW, THEREFORE,

BE IT ORDAINED, by the Council of the City of San Diego, as follows:

Section 1. That Chapter 5 of the San Diego Municipal Code is amended by adding new Article 11, Division 1, and sections 511.0101, 511.0102, 511.0103, 511.0104, 511.0105, 511.0106, 511.0107, 511.0108, 511.0109, and 511.0110, to read as follows:

Article 11: Transparent and Responsible Use of Surveillance Technology

Division 1: Approval Process for Use of Surveillance Technology

§511.0101 Definitions

For purposes of this Division, the following definitions shall apply and appear in italicized letters:

(a) *Annual Surveillance Report* means a written report concerning a specific *surveillance technology* that includes all of the following:

(1) A description of how the *surveillance technology* was used, including the type and quantity of data gathered or analyzed by the *surveillance technology*;

(2) Whether and how often data acquired through the use of the *surveillance technology* was shared with any internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and justification for the disclosure(s), except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(3) Where applicable, a description of the physical objects to which the *surveillance technology* hardware was installed without revealing the specific location of such hardware; for *surveillance technology* software, a breakdown of what data sources the *surveillance technology* was applied to;

(4) A list of any software updates, hardware upgrades, or system configuration changes accompanied by a description of altered or improved functionality that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change, except that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the legitimate security interests of the *City*;

(5) Where applicable, a description of where the *surveillance technology* was deployed geographically, by each *police area* in the relevant year;

(6) A summary of community complaints or concerns about the *surveillance technology*, and an analysis of its *Surveillance Use Policy* and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the *surveillance technology* disproportionately impacts certain groups or *individuals*.

(7) The results of any internal audits or investigations relating to *surveillance technology*, any information about violations of the *Surveillance Use Policy*, and any actions taken in response. To the extent that the public release of such information is prohibited by law, *City staff* shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

(8) Information about any data breaches or other unauthorized access to the data collected by the *surveillance technology*, including information about the scope of the breach and the actions taken in response, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(9) A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(10) Information, including crime statistics, that helps the community assess whether the *surveillance technology* has been effective at achieving its identified purposes;

(11) Statistics and information about Public Records Act requests regarding the relevant subject *surveillance technology*, including response rates, such as the number of Public Records Act requests on such *surveillance technology* and the open and close date for each of these Public Records Act requests;

(12) Total annual costs for the *surveillance technology*, including personnel and other ongoing costs, and what source of funding will fund the *surveillance technology* in the coming year; and

(13) Any requested modifications to the *Surveillance Use Policy* and a detailed basis for the request.

(b) *Board* means the Privacy Advisory Board established by Chapter 2, Article 6, Division 4 of the Municipal Code.

(c) *City* means any department, unit, program, and subordinate division of the City of San Diego as a municipal corporation.

(d) *City staff* means *City* personnel authorized by the City Manager or appropriate *City* department head to seek City Council approval of *Surveillance Technology* in conformance with this Division.

(e) *Community meeting* means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of *surveillance technology* on disadvantaged groups.

(f) *Continuing agreement* means a written agreement that automatically renews unless terminated by one or more parties.

(g) *Exigent circumstances* means a *City* department's good faith belief that an emergency involving danger of death or serious physical injury to any *individual*, or imminent danger of significant property damage, requires the use of *surveillance technology*.

(h) *Facial recognition technology* means an automated or semi-automated process that assists in identifying or verifying an *individual* based on an *individual's* face.

(i) *Individual* means a natural person.

(j) *Personal communication device* means a mobile telephone, a personal digital assistant, a wireless capable tablet, and a similar wireless two-way communications or portable internet-accessing device, whether procured or subsidized by the *City* or personally owned, that is used in the regular course of *City* business.

(k) *Police area* refers to each of the geographic districts assigned to a San Diego Police Department captain or commander.

(l) *Surveillance* or *surveil* means to observe or analyze the movements, behavior, data, or actions of *individuals*. *Individuals* include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the *individual*.

(m) *Surveillance technology* means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any *individual* or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such *surveillance technology*. Examples of *surveillance technology* include the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; *facial recognition technology*; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; and video cameras that record audio or video and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, and biometric identification hardware or software.

(1) *Surveillance technology* does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a *surveillance technology* beyond what is set forth below or used beyond a purpose as set forth below:

(A) Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any public *surveillance* or law enforcement functions related to the public;

(B) Parking ticket devices used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;

(C) Manually-operated, non-wearable, handheld digital 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;

(D) *Surveillance* devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

(E) Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect *surveillance* data, such as radios and email systems;

(F) *City* databases 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;

(G) Medical equipment used to diagnose, treat, or prevent disease or injury, provided that any information obtained from this equipment is used solely for medical purposes;

(H) Police department interview room cameras;

(I) *City* department case management systems;

(J) *Personal communication devices* that have not been modified beyond stock manufacturer capabilities in a manner described above;

(K) *Surveillance technology* used by the *City* solely to monitor and conduct internal investigations involving *City* employees, contractors, and volunteers;

(L) Systems, software, databases, and data sources used for revenue collection on behalf of the *City* by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other *City* department or third-party except as part of efforts to collect revenue that is owed to the *City*.

(n) *Surveillance Impact Report* means a publicly posted written report including, at a minimum, the following:

(1) Description: Information describing the *surveillance technology* and how it works, including product descriptions from manufacturers;

(2) Purpose: Information on the proposed purposes(s) and outcomes for the *surveillance technology*;

(3) Location: The physical or virtual location(s) where it may be deployed, using general descriptive terms, and crime statistics for any location(s);

(4) Impact: An assessment of the *Surveillance Use Policy* for the particular *surveillance technology* and whether it is adequate in protecting civil rights and liberties and whether the *surveillance technology* was used or deployed, intentionally or inadvertently, in a manner that may disproportionately affect marginalized communities;

(5) Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;

(6) Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the *surveillance technology*, including open source data, scores, reports, logic or algorithm used, and any additional information derived therefrom, except that no

confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(7) Data Security: Information about the controls that will be designed and implemented to ensure that security objectives are achieved to safeguard the data collected or generated by the *surveillance technology* from unauthorized access or disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(8) Fiscal Cost: The forecasted, prior, and ongoing fiscal costs for the *surveillance technology*, including initial purchase, personnel, and other ongoing costs, and any current or potential sources of funding;

(9) Third Party Dependence: Whether use or maintenance of the *surveillance technology* will require data gathered by the *surveillance technology* to be handled or stored by a third-party vendor at any time;

(10) Alternatives: 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; and,

(11) Track Record: A summary of the experience, if any, other entities, especially government entities, have had with the proposed *surveillance technology*, including, if available, quantitative information about the effectiveness of the proposed *surveillance technology* in achieving its stated purpose in other jurisdictions, and any known adverse information about the *surveillance technology* such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the *surveillance technology*.

(12) Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and *City* departmental responses given, and *City* departmental conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of *surveillance technology*.

(o) *Surveillance Use Policy* means a publicly-released and legally enforceable policy for use of the *surveillance technology* that at a minimum specifies the following:

(1) Purpose: The specific purpose(s) that the *surveillance technology* is intended to advance;

(2) Use: The specific uses that are authorized and the rules and processes required prior to such use, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(3) Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the *surveillance technology*, as well as data that might be inadvertently collected during the authorized uses of the *surveillance technology* and what measures will be taken to minimize and delete such data. Where applicable, any data sources the *surveillance technology* will rely upon, including open source data, should be listed. In the reporting of such information, no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(4) Data Access: The job classification of *individuals* who can access or use the collected information, and the rules and processes required prior to access or use of the information, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(5) Data Protection: The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(6) 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;

(7) Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants;

(8) Third Party Data Sharing: If and how information obtained from the *surveillance technology* can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

(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 procedures used to ensure that the *Surveillance Use Policy* is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the *surveillance technology* or access to information collected by the *surveillance 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; and

(11) Maintenance: The procedures used to ensure that the security and integrity of the *surveillance technology* and collected information will be maintained.

§511.0102 Board Notification and Review Requirements

(a) *City staff* shall notify the Chair of the *Board* by written memorandum along with providing a *Surveillance Use Policy* and a *Surveillance Impact Report* prior to:

(1) seeking or soliciting funds for *surveillance technology*, including but not limited to applying for a grant;

(2) soliciting proposals with any entity to acquire, share, or otherwise use *surveillance technology*; or

(3) formally or informally facilitating in a meaningful way or implementing *surveillance technology* in collaboration with other entities, including *City* ones;

(b) Upon notification by *City staff*, the Chair of the *Board* shall place the request on the agenda at the next *Board* meeting for discussion and possible action. At this meeting, *City staff* shall inform the *Board* of the need for the funds or equipment, or shall otherwise justify the action for which *City staff* will seek City Council approval pursuant to section 511.0103. The *Board* may make a recommendation to the City Council by voting for approval to proceed, objecting to the proposal, recommending that the *City staff* modify the proposal, or taking no action.

(c) If the *Board* votes to approve, object, or modify the proposal, *City staff* may proceed and seek City Council approval of the proposed *surveillance technology* initiative pursuant to the requirements of section 511.0103. *City staff* shall present to City Council the result of the *Board's* review, including any objections to the proposal.

(d) If the *Board* does not make its recommendation on the item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may proceed to the City Council for approval of the item.

(e) City staff shall seek *Board* review for new *surveillance technology* before seeking City Council approval under section 511.0103.

(1) Prior to seeking City Council approval under section 511.0103, *City staff* shall submit a *Surveillance Impact Report* and a *Surveillance Use Policy* for the proposed new *surveillance technology* initiative to the *Board* for its review at a publicly noticed meeting. The

Surveillance Impact Report and *Surveillance Use Policy* must address the specific subject matter specified for each document as set forth in section 511.0101.

(2) Prior to submitting the *Surveillance Impact Report*, *City staff* shall complete one or more *community meetings* in each City Council district where the proposed *surveillance technology* is deployed, with opportunity for public comment and written response. The City Council may condition its approval of the proposed *surveillance technology* on *City staff* conducting additional community engagement before approval, or after approval as a condition of approval.

(3) The *Board* shall recommend that the City Council adopt, modify, or reject the proposed *Surveillance Use Policy*. If the *Board* proposes that the *Surveillance Use Policy* be modified, the *Board* shall propose such modifications to *City staff*. *City staff* shall present such modifications to City Council when seeking City Council approval under section 511.0103.

(4) If the *Board* does not make its recommendation on the item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may seek City Council approval of the item.

(f) *City staff* shall seek *Board* review for the use of existing *surveillance technology* before seeking City Council approval.

(1) Prior to seeking City Council approval for existing *surveillance technology* used by the *City* under section 511.0103, *City staff* shall submit a *Surveillance Impact Report* and *Surveillance Use Policy* for each existing *surveillance technology* to the *Board* for its review at a publicly noticed meeting. The *Surveillance Impact Report* and *Surveillance Use Policy* shall address the specific subject matters set forth for each document in section 511.0101.

(2) Prior to submitting the *Surveillance Impact Report, City staff* shall complete one or more *community meetings* in each City Council district where the proposed *surveillance technology* is deployed with opportunity for public comment and written response. The City Council may condition its approval on *City staff* conducting additional outreach before approval, or after approval as a condition of approval.

(3) Prior to submitting the *Surveillance Impact Report* and proposed *Surveillance Use Policy* as described above, *City staff* shall present to the *Board* a list of *surveillance technology* possessed or used by the *City*.

(4) The *Board* shall rank the items in order of potential impact to civil liberties to provide a recommended sequence for items to be heard at *Board* meetings. The *Board* shall take into consideration input from *City staff* on the operational importance of the *surveillance technology* in determining the ranking to allow such matters to be heard in a timely manner.

(5) Within 60 calendar days of the *Board's* action in section 511.0102(f)(3), *City staff* shall submit at least one *Surveillance Impact Report* and proposed *Surveillance Use Policy* per month to the *Board* for review, generally beginning with the highest-ranking items as determined by the *Board*, and continuing thereafter each month until a *Surveillance Impact Report* and *Surveillance Use Policy* has been submitted for each item on the list.

(6) If the *Board* does not make its recommendation on any item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may proceed to the City Council for approval of the item pursuant to section 511.0103.

§511.0103 City Council Approval for New and Existing Surveillance Technology

(a) *City staff* shall obtain City Council approval prior to any of the following:

(1) accepting local, state, federal funds or in-kind or other donations for *surveillance technology*;

(2) acquiring new *surveillance technology*, including but not limited to procuring such technology without the exchange of 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 City Council pursuant to the requirements of this Division; or

(4) entering into a *continuing agreement* or other written agreement to acquire, share or otherwise use *surveillance technology.*

(b) City Council Approval Process

(1) After the *Board* notification and review requirements in section 511.0102 have been satisfied, *City staff* seeking City Council approval shall schedule a date for City Council consideration of the proposed *Surveillance Impact Report* and proposed *Surveillance Use Policy*.

(2) The City Council shall only approve any action as provided in this Division after first considering the recommendation of the *Board*, and subsequently making a determination that the benefits to the community of the *surveillance technology* outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

(3) For approval of existing *surveillance technology* for which the *Board* does not make its recommendation within 90 calendar days of review as provided in section 511.0102(f)(5), if the City Council has not reviewed and approved such item within four City Council meetings from when the item was initially scheduled for City Council consideration, the *City* shall cease its use of the *surveillance technology* until such review and approval occurs.

(c) Unless otherwise provided in this Division, *Surveillance Impact Reports* and *Surveillance Use Policies* are public records. *City staff* shall make all *Surveillance Impact Reports* and *Surveillance Use Policies*, as updated from time to time, available to the public as long as the *City* uses the *surveillance technology*.

(d) *City staff* shall post all *Surveillance Impact Reports* and *Surveillance Use Policies* to the *City's* website with an indication of its current approval status and the planned City Council date for action.

§511.0104 Use of Unapproved Surveillance Technology During Exigent Circumstances

(a) *City staff* may temporarily acquire or use *surveillance technology* in a manner not in compliance with this Division only in a situation involving *exigent circumstances*.

(b) If *City staff* acquires or uses a *surveillance technology* in a situation involving *exigent circumstances*, *City staff* shall:

(1) immediately report in writing the use of the *surveillance technology* and its justifications to the City Council and the *Board*;

(2) use the *surveillance technology* solely to respond to the *exigent circumstances*;

(3) cease using the *surveillance technology* when the *exigent circumstances* end;

(4) only keep and maintain data related to the *exigent circumstances* and dispose of any data that is not relevant to an ongoing investigation or the *exigent circumstances*; and

(5) Following the end of the *exigent circumstances*, report the temporary acquisition or use of the *surveillance technology* for *exigent circumstances* to the *Board* in accordance with section 511.0102 at its next meeting for discussion and possible recommendation to the City Council.

(c) Any *surveillance technology* acquired in accordance with *exigent circumstances* shall be returned within 30 calendar days following when the *exigent circumstances* end, unless *City staff* initiates the process set forth for the use of the *surveillance technology* by submitting a *Surveillance Use Policy* and *Surveillance Impact Report* for *Board* review within this 30-day time period. If *City staff* is unable to meet the 30-day deadline, *City staff* shall notify the City Council, who may grant an extension. In the event that *City staff* complies with the 30-day deadline or the deadline as may be extended by the City Council, *City staff* may retain possession of the *surveillance technology*, but may only use such *surveillance technology* consistent with the requirements of this Division.

§511.0105 Oversight Following City Council Approval

(a) For each approved *surveillance technology* item, *City staff* shall present an *Annual Surveillance Report* for the *Board* to review within one year after the date of City Council final passage of such *surveillance technology* and annually thereafter as long as the *surveillance technology* is used.

(b) If *City staff* is unable to meet the annual deadline, *City staff* shall notify the *Board* in writing of *City staff's* request to extend this period, and the reasons for that request. The *Board* may grant a single extension of up to 60 calendar days to comply with this provision.

(1) After review of the report by the *Board*, *City staff* shall submit the *Annual Surveillance Report* to the City Council.

(2) The *Board* shall recommend to the City Council that the benefits to the community of the *surveillance technology* in question outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the *surveillance technology* cease; or, propose modifications to the corresponding *Surveillance Use Policy* that will resolve any identified concerns.

(3) If the *Board* does not make its recommendation on the item within 90 calendar days of submission of the *Annual Surveillance Report* to the *Board* Chair, *City staff* may proceed to the City Council for approval of the *Annual Surveillance Report*.

(4) In addition to the above submission of any *Annual Surveillance Report*, *City staff* shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to section 511.0103 for that particular *surveillance technology* and the pertinent *Board* recommendation, including whether the City Council approved or rejected the proposal, and required changes to a proposed *Surveillance Use Policy* before approval.

(c) Based upon information provided in the *Annual Surveillance Report* and after considering the recommendation of the *Board*, the *City* shall revisit its cost benefit analysis as provided in section 511.0103(b)(2) and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the *City's* use of the *surveillance technology* shall cease. Alternatively, the City Council may require modifications to a particular *Surveillance Use Policy* that will resolve any concerns with the use of a particular *surveillance technology*.

(d) *City staff* shall provide an annual report to City Council in closed session as permitted by state law on cybersecurity threats involving *surveillance technology* and how the *City* is managing risk to include the following:

(1) a list and description of any major *surveillance technology* updates that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change;

(2) information about any data breaches or unauthorized access to the data collected by the *surveillance tech*nology, including information about the scope of the breach and the actions taken in response; and

(3) a description of the standards and industry best practices that the *City* uses to detect incidents of data breaches or unauthorized access to *surveillance technology*.

§511.0106 Enforcement

(a) Violations of this Division are subject to the following remedies:

(1) Any material violation of this Division, or of a *Surveillance Use Policy* promulgated pursuant to this Division, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Division. An action instituted under this paragraph shall be brought against the *City*, and, if necessary, to effectuate compliance with this Division or a *Surveillance Use Policy* (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Division to the extent permitted by law.

(2) Any person who has been subjected to the use of *surveillance technology* in material violation of this Division, or of a material violation of a *Surveillance Use Policy*, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Division or of a *Surveillance Use Policy* promulgated under this Division, may institute proceedings in the Superior Court of the State of California against the *City* and shall be entitled to recover actual damages (but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater).

(3) A court may award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under sections 511.0106(a)(1) or (2).

§511.0107 Contracts for Surveillance Technology

It shall be unlawful for the *City* to enter into any contract or other agreement for *surveillance technology* after the effective date of this Division that conflicts with the provisions of this Division. Any conflicting provisions in any such contract or agreement, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Any amendment or exercise of any option to any contract after the effective date of this Division to obtain or use *surveillance technology* shall require *City staff* to comply with the provisions of this Division. To the extent permitted by law, the *City* shall publicly disclose all of its *surveillance technology* contracts, including all related non-disclosure agreements executed after the effective date of this Division.

§511.0108 Whistleblower Protections

(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 *surveillance technology* or *surveillance* data based upon a good faith belief that the disclosure evidenced a violation of this Division; or

(2) the employee or applicant was perceived to, about to, had assisted in or had participated in any proceeding or action to carry out the purposes of this Division.

(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 Division.

(c) Any employee or applicant who is injured by a violation of section 511.0108 may institute a proceeding for monetary damages and injunctive relief against the *City* in any court of competent jurisdiction.

§511.0109 Grace Period for Use of Existing Surveillance Technology

The requirement for *City staff* to seek approval for the use of existing *surveillance technology* shall take effect one year after the effective date of this Division. *Surveillance technology* is considered existing if the City possessed, used, or has a contract in force and effect for the use of *surveillance technology* before the effective date of this Division.

§511.0110 Compliance with City Charter or Applicable State Law

Nothing in this Division is intended to violate any provision of the City Charter or applicable state law nor should any provision of this Division be interpreted in such a manner.

Section 2. That a full reading of this ordinance is dispensed with prior to passage, a written copy having been made available to the Council and the public prior to the day of its passage.

Section 3. That this ordinance shall take effect and be in force thirty days from and after its final passage.

APPROVED: MARA W. ELLIOTT, City Attorney

By _____
Kenneth R. So
Deputy City Attorney

KRS:cm
October 23, 2020
November 6, 2020 COR. COPY
Or.Dept:CD-4
Doc. No.: 2522043

I hereby certify that the foregoing Ordinance was passed by the Council of the City of San Diego, at this meeting of _____.

ELIZABETH S. MALAND
City Clerk

By_____
Deputy City Clerk

Approved: _____ _____
(date) KEVIN L. FAULCONER, Mayor

Vetoed: _____ _____
(date) KEVIN L. FAULCONER, Mayor