

ORDINANCE NUMBER O- 21711 (NEW SERIES)

DATE OF FINAL PASSAGE AUG 08 2023

AN ORDINANCE AMENDING CHAPTER 2, ARTICLE 10,
DIVISION 1, OF THE SAN DIEGO MUNICIPAL CODE BY
AMENDING SECTIONS 210.0101 AND 210.0109, RELATING
TO TRANSPARENT AND RESPONSIBLE USE OF
SURVEILLANCE TECHNOLOGY.

WHEREAS, by San Diego Ordinance O-21514 (Aug. 10, 2022), the City Council
(Council) of the City of San Diego (City) adopted rules related to the City's acquisition and use
of surveillance technology; and

WHEREAS, the ordinance is codified in the San Diego Municipal Code at Chapter 2,
Article 10, Division 1, sections 210.0101 through 210.0110, and is titled "Transparent and
Responsible Use of Surveillance Technology" (TRUST Ordinance); and

WHEREAS, in adopting the TRUST Ordinance, the Council recognized that the use of
surveillance technology is important to protect public health and safety, but its use must be
appropriately monitored and regulated to protect an individual's right to privacy; and

WHEREAS, the Council found 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 Council also found 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, by San Diego Ordinance O-21446 (April 12, 2022), the Council established
the Privacy Advisory Board to review City proposals to acquire and use surveillance technology
and make recommendations to the City Council and the Mayor; and

WHEREAS, under the TRUST Ordinance, City staff must prepare a Surveillance Impact Report and Surveillance Use Policy and present them to the Privacy Advisory Board for discussion and recommendation prior to a determination by the Council; and

WHEREAS, the Privacy Advisory Board began meeting on March 15, 2023; and

WHEREAS, as part of the TRUST Ordinance, the Council initially established a one-year grace period before requiring Council authorization of the City's existing surveillance technology following the required review by the Privacy Advisory Board; and

WHEREAS, the Mayor has identified more than 300 items of existing surveillance technology requiring review under the TRUST Ordinance process; and

WHEREAS, the Council wishes to extend the grace period to four years from the initial effective date of the TRUST Ordinance, which is September 9, 2026, which will allow additional time for City staff to gather the information needed and present the documents to the Privacy Advisory Board for review and the Council for determination; and

WHEREAS, under this amendment to the TRUST Ordinance, the new grace period will end September 9, 2026; and

WHEREAS, the Office of the City Attorney has drafted this Ordinance based on the information provided by City staff, including information provided by affected third parties and verified by City staff, with the understanding that this information is complete, true, and accurate; NOW, THEREFORE,

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

Section 1. That Chapter 2. Article 10, Division 1, of the San Diego Municipal Code is amended by amending sections 210.0101 and 210.0109, to read as follows:

Article 10: Transparent and Responsible Use of Surveillance

Technology

Division 1: Approval Process for Use of Surveillance

Technology

§210.0101 Definitions

For purposes of this Division, the following definitions 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 elements.
 - (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 types of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosures, 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 the hardware; for *surveillance*

technology software, a breakdown of the data sources applied or related to the *surveillance technology*.

- (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) [No change in text.]
- (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 California Public Records Act requests regarding the specific *surveillance technology*, including response rates, such as the number of California Public Records Act requests on the *surveillance technology* and the open and close date for each of these California 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.
 - (13) [No change in text.]
- (b) *Board* means the Privacy Advisory Board established by Chapter 2, Article 6, Division 00, section 26.42, of this Municipal Code.

- (c) *City* means any department, unit, program, or subordinate division of the City of San Diego as a municipal corporation.
- (d) *City staff* means *City* personnel engaged in administrative activities in *City* departments under the City Manager or independent department director, who must seek City Council approval of *surveillance technology* in accordance with this Division. *City* personnel assigned to federal task force activities by the Chief of Police or designee are exempt from the requirements of this Division related to the acquisition, use, reporting, and contractual obligations, solely to the extent of their duties and work related to their assignment to the federal task force.
- (e)-(i) [No change in text.]
- (j) *Personal communication device* means a mobile telephone, a personal digital assistant, a wireless capable tablet, or 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)-(l) [No change in text.]
- (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 the *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 the following devices, software, or hardware:

(A)-(B) [No change in text.]

(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 or audio recordings or both;

(D)-(E) [No change in text.]

(F) *City* databases, software, or enterprise systems used by *City staff* to manage internal operations or to prepare and retain legally required records and information related to internal *City* operational activities, including *City* payroll,

accounting, and other fiscal operations; *City* marketing,
donor, media, and constituent relations; and
communications initiated by *individuals* directed to *City*
staff to request *City* services, file complaints, or
communicate information about *City* services;

(G)-(J) [No change in text.]

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

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

(n) *Surveillance Impact Report* means a publicly released written report that
includes all of the following elements.

- (1) Description: Information describing the *surveillance technology*
and how it works, including product descriptions from
manufacturers.
- (2) Purpose: Information on the proposed purposes and outcomes for
the *surveillance technology*.

- (3) Location: The physical or virtual locations where the *surveillance technology* may be deployed, using general descriptive terms, and crime statistics for the locations.
- (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 from the *surveillance technology*, 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 means to achieve the proposed purpose considered, including alternative means that do not involve the use of *surveillance technology*, 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.
- (11) Track Record: A summary of the experience, if any, of other entities, especially government entities, 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 the impacts may differ as they pertain 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 the use of the *surveillance technology* that includes all of the following elements.

- (1) Purpose: The specific purposes that the *surveillance technology* is intended to advance.
- (2) Use: The specific uses that are authorized and the rules and processes required prior to the 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 the data. Where applicable, any data sources the *surveillance technology* will rely upon, including open source data, should be listed. In the reporting of this 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 the retention period is appropriate to further the purposes, 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 accessed or used, 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 identification of internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the *surveillance technology* and access to information collected by the *surveillance technology*, technical measures to monitor for misuse, identification of any independent person or entity with oversight authority, and the

legally enforceable sanctions for violations of the policy.

(11) [No change in text.]

§ 210.0109 Grace Period for Use of Existing Surveillance Technology

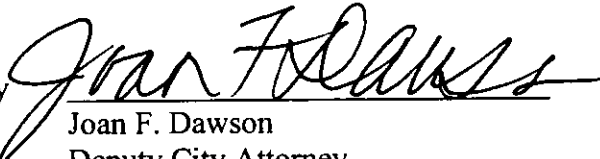
The requirement for *City staff* to seek approval for the use of existing *surveillance technology* takes effect September 9, 2026, which is four years after the effective date of this Division. This grace period allows *City staff* and the *Privacy Advisory Board* to fully implement the necessary procedures to comply with 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 September 9, 2022, the effective date of this Division.

Section 2. That the Council intends this Ordinance to apply prospectively.

Section 3. 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 4. 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 
Joan F. Dawson
Deputy City Attorney

JFD:cm:jvg
July 11, 2023
July 14, 2023 COR. COPY
July 17, 2023 COR. COPY 2
Or.Dept: Office of the Mayor
Doc. No.: 3359303_2

I hereby certify that the foregoing Ordinance was passed by the Council of the City of
San Diego, at this meeting of AUG 01 2023.

DIANA J.S. FUENTES
City Clerk

By Kristell Medina
Deputy City Clerk

Approved: 8/8/23
(date)

Todd Gloria
TODD GLORIA, Mayor

Vetoed: _____
(date)

TODD GLORIA, Mayor

STRIKEOUT ORDINANCE

OLD LANGUAGE: ~~Struck Out~~

NEW LANGUAGE: Double Underline

ORDINANCE NUMBER O-_____ (NEW SERIES)

DATE OF FINAL PASSAGE _____

AN ORDINANCE AMENDING CHAPTER 2, ARTICLE 10,
DIVISION 1, OF THE SAN DIEGO MUNICIPAL CODE BY
AMENDING SECTIONS 210.0101 AND 210.0109, RELATING
TO TRANSPARENT AND RESPONSIBLE USE OF
SURVEILLANCE TECHNOLOGY.

Article 10: Transparent and Responsible Use of Surveillance

Technology

Division 1: Approval Process for Use of Surveillance

Technology

§210.0101 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 elements:
- (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)-types~~ of data

disclosed, under what legal ~~standard(s)~~ standards the information was disclosed, and the justification for the disclosure(s) disclosures, 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;₂

- (3) Where applicable, a description of the physical objects to which the *surveillance technology* hardware was installed without revealing the specific location of ~~such the~~ hardware; for *surveillance technology* software, a breakdown of ~~what the~~ data sources applied or related to the *surveillance technology* ~~was applied to~~;₂
- (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;₂
- (5) Where applicable, a description of where the *surveillance technology* was deployed geographically, by each *police area* in the relevant year;₂

- (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) [No change in text.]
- (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 California Public Records Act requests regarding the ~~relevant subject specific~~ surveillance technology, including response rates, such as the number of California Public Records Act requests on ~~such the~~ surveillance technology and the open and close date for each of these California 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) [No change in text.]
- (b) *Board* means the Privacy Advisory Board established by Chapter 2, Article 6, Division 00, section 26.42, of the ~~this~~ this Municipal Code.
- (c) *City* means any department, unit, program, ~~and or~~ subordinate division of the City of San Diego as a municipal corporation.
- (d) *City staff* means *City* personnel ~~authorized by~~ engaged in administrative activities in City departments under the City Manager or ~~appropriate City independent department head to~~ director, who must seek City Council approval of ~~Surveillance Technology in conformance~~ surveillance technology in accordance with this Division. *City* personnel assigned to federal task force activities by the Chief of Police or designee are exempt from the requirements of this Division related to the acquisition, use, reporting, and contractual obligations, solely to the extent of their duties and work related to their assignment to the federal task force.

(e)-(i) [No change in text.]

(j) *Personal communication device* means a mobile telephone, a personal digital assistant, a wireless capable tablet, ~~and~~ or 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) -(l) [No change in text.]

(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~~ the *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~~ the following devices, software, or hardware:

(A)-(B) [No change in text.]

- (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~~ or audio recordings or both;

(D)-(E) [No change in text.]

- (F) *City* databases ~~that do not contain any data or other,~~ software, or enterprise systems used by *City* staff to manage internal operations or to prepare and retain legally required records and information collected, captured, recorded, retained, processed, intercepted, or analyzed by *surveillance technology*, including related to internal *City* operational activities, including *City* payroll, accounting, ~~or~~ and other fiscal databases operations; *City* marketing, donor, media, and constituent relations; and communications initiated by *individuals* directed to *City* staff to request *City*

services, file complaints, or communicate information
about City services;

(G)-(J) [No change in text.]

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

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

(n) *Surveillance Impact Report* means a publicly ~~posted~~ released written report ~~including, at a minimum, that includes all of the following:~~ elements.

- (1) Description: Information describing the *surveillance technology* and how it works, including product descriptions from manufacturers; ;
- (2) Purpose: Information on the proposed ~~purposes(s)~~ purposes and outcomes for the *surveillance technology*; ;
- (3) Location: The physical or virtual ~~location(s)~~ locations where ~~it the~~

surveillance technology may be deployed, using general descriptive terms, and crime statistics for ~~any location(s); the~~ locations.

- (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~~ the *surveillance technology*, 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)~~ means to achieve the proposed purpose considered, including alternative means that do not involve the use of *surveillance technology*, 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, of 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 the~~ impacts may differ as it ~~pertains they~~ pertain to different segments of the community that may result from the acquisition of *surveillance technology*.

- (o) *Surveillance Use Policy* means a ~~publicly-~~ publicly released and legally enforceable policy for the use of the *surveillance technology* that ~~at a minimum, specifies~~ includes all of the following elements.

- (1) Purpose: The specific ~~purposes(s)-~~ purposes 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 the~~ 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~~ the data. Where applicable, any data sources the *surveillance technology* will rely upon, including open source data, should be listed. In the reporting of ~~such~~ this 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~~ the retention period is appropriate to further the ~~purpose(s)~~ purposes, 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 or used, 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 identification of internal personnel assigned to ensure compliance with the policy,

internal recordkeeping of the use of the *surveillance technology* ~~or~~
and access to information collected by the *surveillance technology*,
technical measures to monitor for misuse, identification of any
independent person or entity with oversight authority, and the
legally enforceable sanctions for violations of the policy; and.

(11) [No change in text.]

§ 210.0109 Grace Period for Use of Existing Surveillance Technology

The requirement for *City staff* to seek approval for the use of existing *surveillance technology* ~~shall~~ takes effect September 9, 2026, which is four one-years after the effective date of this Division. This grace period allows *City staff* and the *Privacy Advisory Board* to fully implement the necessary procedures to comply with 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 September 9, 2022, the effective date of this Division.

JFD:cm:jvg
July 11, 2023
July 14, 2023 COR. COPY
July 17, 2023 COR. COPY 2
Or.Dept: Office of the Mayor
Doc. No.: 3359438_3

Passed by the Council of The City of San Diego on AUG 01 2023, by the following vote:

Councilmembers	Yeas	Nays	Not Present	Recused
Joe LaCava	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jennifer Campbell	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stephen Whitburn	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monica Montgomery Steppe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Marni von Wilpert	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kent Lee	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Raul A. Campillo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vivian Moreno	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sean Elo-Rivera	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Date of final passage AUG 08 2023.

AUTHENTICATED BY:

(Seal)

TODD GLORIA
Mayor of The City of San Diego, California.

DIANA J.S. FUENTES
City Clerk of The City of San Diego, California.

By Kristell Medina, Deputy

I HEREBY CERTIFY that the foregoing ordinance was not finally passed until twelve calendar days had elapsed between the day of its introduction and the day of its final passage, to wit, on

JUL 18 2023, and on AUG 08 2023.

I FURTHER CERTIFY that said ordinance was read in full prior to passage or that such reading was dispensed with by a vote of five members of the Council, and that a written copy of the ordinance was made available to each member of the Council and the public prior to the day of its passage.

(Seal)

DIANA J.S. FUENTES
City Clerk of The City of San Diego, California.

By Kristell Medina, Deputy

Office of the City Clerk, San Diego, California

Ordinance Number O-21711