APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL

ORDINANCE NO. _____C.M.S.

ORDINANCE AMENDING OAKLAND MUNICIPAL CODE CHAPTER 9.64, WHICH REGULATES THE CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY, BY (A):

(1) CLARIFYING EXISTING DEFINITIONS AND ADDING NEW ONES;

(2) CLARIFYING WHEN CITY STAFF MUST NOTIFY THE PRIVACY ADVISORY COMMISSION AND/OR SEEK CITY COUNCIL APPROVAL IN REGARDS TO THE ACQUISITION OF SURVEILLANCE TECHNOLOGY;

(3) PROHIBITING THE CITY'S USE OF BIOMETRIC SURVEILLANCE TECHNOLOGY AND PREDICTIVE POLICING TECHNOLOGY; AND

(B) ADOPTING CALIFORNIA ENVIRONMENTAL QUALITY ACT EXEMPTION FINDINGS

WHEREAS, the City of Oakland first adopted a Surveillance Technology Ordinance (codified as Oakland Municipal Code or O.M.C. Chapter 9.64) in May 2018 and City staff have been working closely with the Privacy Advisory Commission (PAC) and learning from the implementation process since that time, and have identified areas that require refinement and/or clarification; and

WHEREAS, the PAC has recommended that the definition of the Annual Surveillance Report should be revised to include information regarding the reporting of data sharing with outside entities, and information on the race of individuals that may have been identified using surveillance technology; and

WHEREAS, the use of Biometric Surveillance Technology by government agencies in real time or on a recording or photograph is a growing concern for civil liberties and privacy advocacy groups; and

WHEREAS the United States Department of Defense announced in June 2020 it was testing a new laser-based Biometric Surveillance Technology system capable of identifying people at a distance of up to 200 meters by measuring their heartbeat, and police in China are testing gait-recognition Biometric Surveillance Technology that identifies people based on how they walk; and

WHEREAS, the proposed amendments to O.M.C. Chapter 9.64 include a definition of the term Biometric Surveillance Technology and a provision banning the City's use of such technology; and

WHEREAS, there are other forms of Surveillance Technology that use biometric information, where such information is not collected in real time. Such technology is vital to traditional operations of the City's Police Department Crime Laboratory for solving serious violent crimes and needs to be distinguished from what this ordinance defines as Biometric Surveillance Technology; and

WHEREAS, Predictive Policing Technology uses arrest data that can encode patterns of racist policing behavior and as a result, are more likely to predict a high potential for crime in minority neighborhoods or among minority people and several studies have shown that these tools perpetuate systemic racism, leading to disparate arrest rates; and

WHEREAS, traditional records management systems, including computer aided dispatch systems, and field-based reporting systems, and Live Scan Machines do not pose significant civil liberty risks and should not be regulated in the same manner since they serve a critical core function of the police department; and

WHEREAS, it is important that City departments seek approval from the City Council prior to purchasing or using new surveillance technology but should not have to return repeatedly for technology that already has an approved Use Policy in place; and

WHEREAS, the Privacy Advisory Commission met with City staff on several occasions to refine the current ordinance to better protect Oaklander's Civil Liberties and improve upon the original reporting and approval processes; and

WHEREAS, the City Council has determined that this action is exempt from environmental review under the California Environmental Quality Act (CEQA) pursuant to: (1) CEQA Guidelines Section 15061(b)(3), Review for Exemptions – General Rule, in that it can be seen with certainty that there is no possibility for this action to have a significant effect on the environment; and (2) CEQA Guidelines Section 15378(b)(5), since this action does not constitute a "project" within the meaning of CEQA and instead relates to "[o]rganizational or

administrative activities of [the City] that will not result in direct or indirect physical changes in the environment."

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

SECTION 1. Recitals. The City Council finds and determines the foregoing recitals to be true and correct and hereby adopts and incorporates them into this Ordinance.

SECTION 2. Amendments to Chapter 9.64 of the Oakland Municipal Code. Oakland Municipal Code Chapter 9.64, is hereby amended as set forth below. Chapter and section numbers and titles are indicated in bold type. Additions are indicated in underline and deletions are shown as ~~strikethrough~~. Provisions of Chapter 9.64 not included herein or not shown in underline or strikethrough type are unchanged.

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance `technology that includes all the following:

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

B. Whether and how often data acquired through the use of the surveillance technology was directly 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);

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year;

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.

The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review;

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information;

G. 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;

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;

J. 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; and

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "Biometric Surveillance Technology" means any computer software that uses Face Recognition Technology or Other Remote Biometric Recognition in real time or on a recording or photograph.

~~2.~~ 3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

~~3.~~ 4. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

~~4.~~ 5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

~~5.~~ 6. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

~~6.~~ 7. "Face Recognition Technology" means an automated or semi-automated process that: (A) assists in identifying or verifying an individual based on an individual's face; or (B) identifies or logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

~~7.~~ 8. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. "Other Remote Biometric Recognition" means: (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on physiological, biological, or behavioral characteristics ascertained from a distance; (ii) uses voice recognition technology; or (iii) identifies or logs such characteristics to infer emotion, associations, activities, or the location of an individual; and (B) does not include identification based on fingerprints or palm prints that have been manually obtained during the course of a criminal investigation or detention.

~~8.~~ 10. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a 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 city business.

11. "Predictive Policing Technology" means computer algorithms that use preexisting data to forecast or predict places or times that have a high risk of crime, or individuals or groups who are likely to be connected to a crime. This definition does not include computer algorithms used solely to visualize, chart, or map past criminal activity (e.g. heat maps).

~~9.~~ 12. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

~~10.~~ 13. "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 license plate data when combined with any other record.

~~11.~~ 14. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to

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. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; 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, biometric identification hardware or software.

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

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 surveillance or law enforcement functions;

B. Parking Ticket Devices (PTDs);

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.

H. Police department interview room cameras.

I. Police department case management <u>and records management</u> systems<u>, including computer aided dispatch systems, and field-based reporting systems</u>.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above, provided that any bundled Face Recognition Technology is only used for the sole purpose of user authentication in the regular course of conducting City business.

L. Live Scan Machines (owned by Alameda County Sheriff but operated by Oakland Police personnel.)

~~12.~~ 15. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy 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 is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. 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;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, operative or proposed contract, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

J. 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,

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

~~13.~~ 16. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

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

G. Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

H. Third Party Data Sharing: if and how other city departments, bureaus, divisions, or non-city entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the category of staff that will provide the training;

J. Auditing and Oversight: the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and

K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

17. "Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

1. Seeking or soliciting funds for new surveillance technology or to replace existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to applying for a grant; or,

2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall

otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020.3 ~~1~~.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

City staff, acting on behalf of a particular department, agency, bureau, or other subordinate division of the City, is not required to submit a new surveillance impact report and surveillance use policy, until the Privacy Advisory Commission has completed its recommendation and analysis on any outstanding surveillance technology that has been previously submitted from such department, agency, bureau, or other subordinate division of the City.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

9.64.030. - City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:

A. Accepting state or federal funds or in-kind or other donations for surveillance technology, except for surveillance technology that has already been approved by City Council and for which a corresponding use policy is in effect;

B. Acquiring new surveillance technology, or replacing existing surveillance technology that has not been previously approved by the City Council pursuant to the requirements of this Chapter, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this

Chapter. However, for surveillance technology that was acquired or was in use prior to enactment of this ordinance, such use may continue until the City Council votes to approve or reject the surveillance technology's corresponding surveillance use policy; or

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

E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process.

A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations ~~at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing~~. City Council consideration and ~~A~~approval may only occur at a public meeting that has been noticed in conformance with the Oakland Sunshine Ordinance. ~~hearing~~. City staff shall not unreasonably delay scheduling any item for City Council consideration and approval at the next earliest opportunity.

B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, 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.

C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) 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.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.

2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:

A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.

B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.

C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.

D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.

3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

9.64.040 - Oversight following City Council approval.

1. By April 30th ~~March 15th~~ of each year~~, or at the next closest regularly scheduled Privacy Advisory Commission meeting~~, or no later than one year after adoption of a

Surveillance Use Policy, city staff must present a written annual surveillance report for Privacy Advisory Commission review for each approved surveillance technology item. If city staff is unable to meet the deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.

B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology 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 the concerns.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. 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 must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

9.64.045 - Prohibition on City's acquisition and/or use of ~~face recognition technology~~ Biometric Surveillance Technology and Predictive Policing Technology.

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. Biometric Surveillance Technology; or

2. Predictive Policing Technology; or

3. Information obtained from either Biometric Surveillance Technology or Predictive Policing Technology.

~~.1. Face recognition technology; or~~

~~2. Information obtained from face recognition technology.~~

B. Only surveillance technology that uses biometric information in a manner that meets the definition of Biometric Surveillance Technology, as provided in Section 9.64.010, shall be prohibited.

C. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from ~~face recognition technology~~ Biometric Surveillance Technology or Predictive Policing Technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and

2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless retention or use of exculpatory evidence is required by law; and

~~2.~~ 3. Upon discovery of such use, City staff logs such receipt, access, or use in ~~its annual surveillance report as referenced by Section 9.64.040~~ a written report and submits such report at the next regularly scheduled meeting of the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and

4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, 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 Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, 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 other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

9.64.060 - Secrecy of surveillance technology.

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

To the extent permitted by law, the 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.

9.64.070 - Whistleblower protections.

1. 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:

A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or

B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.

2. 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 Article.

3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

SECTION 3. Severability. If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional

SECTION 4. California Environmental Quality Act. The City Council hereby finds and determines that this action is exempt from environmental review under the California Environmental Quality Act (CEQA) pursuant to: (1) CEQA Guidelines Section 15061(b)(3), Review for Exemptions – General Rule, in that it can be seen with certainty that there is no possibility for this action to have a significant effect on the environment; and (2) CEQA Guidelines Section 15378(b)(5), since this action does not constitute a "project" within the meaning of CEQA and instead relates to "[o]rganizational or administrative activities of [the City] that will not result in direct or indirect physical changes in the environment."

SECTION 5. Effective Date. This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES -FORTUNATO BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO AND PRESIDENT KAPLAN

NOES –

ABSENT –

ABSTENTION –

ATTEST: _____
ASHA REED
Acting City Clerk and Clerk of the
Council of the City of Oakland, California

Date of Attestation: _____

3006267