



# AGENDA REPORT

**TO:** Sabrina B. Landreth  
City Administrator

**FROM:** Anne E. Kirkpatrick  
Chief of Police

**SUBJECT:** Facial Recognition Ordinance  
Amendment – **Supplemental Report**

**DATE:** June 17, 2019

---

City Administrator Approval

Date:

*[Signature]*  
*6/20/19*

## RECOMMENDATION

**Staff Recommends That The City Council Adopt An Ordinance Amending Chapter 9.64, Regulations on City's Acquisition And Use Of Surveillance Technology To Add The Definition Of Real-Time Face Recognition Technology Under Oakland Municipal Code, Section 9.64.010.13 And Add To Make It Unlawful For Any City Staff To Obtain, Retain, Request, Access, Or Use Any Face Recognition Technology Under Oakland Municipal Code Section 9.64.030.1.F,**

## REASON FOR SUPPLEMENTAL REPORT

The Oakland Police Department (OPD) recommends that City Council consider alternate language to Council President Kaplan's proposed ordinance amendment as follows:

Adopt An Ordinance Amending Chapter 9.64, Regulations on City's Acquisition And Use Of Surveillance Technology To Add The Definition Of Real-Time Face Recognition Technology Under Oakland Municipal Code, Section 9.64.010.13 And Add To Make It Unlawful For Any City Staff To Use Any Real-Time Face Recognition Technology Under Oakland Municipal Code Section 9.64.030.1.F (see **Attachment A** for OPD's recommended amendments).

Facial recognition technology (FRT) measures unique characteristics of individual faces; connected software can match faces from different photographic images stored in different databases. "Real-time" FRT creates matches by simultaneously connecting just-captured images to existing databases. Non-real time FRT can be used after the fact to match crime scene face images to existing repositories of mug shots. FRT can serve as powerful tool for law enforcement agencies. However, the technology is far from perfect and can lead to false positives. The Oakland City Council adopted a surveillance technology ordinance in May 2018 that requires city departments to vet any new surveillance technology such as FRT with the City's Privacy Advisory Commission (PAC) before any type of purchase. Therefore, staff recommends amendments to the proposed ordinance.

Item: \_\_\_\_\_  
Public Safety Committee  
June 25, 2019

## **BACKGROUND / LEGISLATIVE HISTORY**

The rapid pace of technological evolution and change consistently leads to new ways in which people can be tracked and observed. Online digital activities generate data points that can be connected both by human analysis as well as through data systems that use artificial intelligence and big data algorithms that sort data. Artificial intelligence and sophisticated algorithms can also be used to connect people when photographed. Faces as well as the way people walk (gait) can be analyzed with software that measures unique distinctions between people.

In the context of concern about the misuse of surveillance technology, the Oakland City Council unanimously approved the "Surveillance and Community Safety Ordinance (Surveillance Ordinance)" on May 15, 2018. The Surveillance Ordinance, developed by the Privacy Advisory Commission (PAC) is considered to be one of the strongest surveillance ordinances in the country, requiring many thresholds for the use of surveillance technology. Departments such as OPD must follow several procedures to use as well as to acquire any surveillance technology. Staff must notify the PAC before soliciting funds with the intent of purchasing any surveillance equipment. Staff must also prepare a Use Policy Report and as well as an Impact Report before seeking to purchase any new surveillance equipment. The Surveillance Use Policy Report must include the following:

- Purpose
- Authorized Use
- Data Collection (what information is collected)
- Data Access (who can access the data)
- Data Protection (how is data protected from unauthorized use)
- Data Retention (how long is the data retained by the department?)
- Public Access:
- Third Party Data Sharing (is data shared with any outside agencies)
- Training (for authorized users)
- Auditing and Oversight (internal controls to ensure proper use and security)
- Maintenance (how is the system maintained)

The Surveillance Impact Report must include the following:

- Description (of the technology)
- Purpose (why the department wants to use the technology)
- Location (where the technology would be used)
- Impact (of the technology on the public in terms of rights and expectations of privacy)
- Mitigations (to protect public privacy)
- Data Types and Sources
- Data Types and Sources
- Fiscal Cost
- Third Party Dependence
- Alternatives (are there other options to accomplish the same purpose?)
- Track Record (of other agencies using the same technology)

After the PAC fully reviews the Surveillance Use Policy Report and Surveillance Impact Report for the technology in question, the PAC can then make a recommendation to the City Council by

Item: \_\_\_\_\_  
Public Safety Committee  
June 25, 2019

voting its approval, rejection or neutral stance position recommendation to the City Council. City departments must also present Annual Surveillance Reports for any surveillance technology approved by the PAC as well as for technologies already obtained by a city department prior to the establishment of the ordinance. Annual Surveillance Reports must address the following:

- How the surveillance technology was used
- Whether and how often data acquired through the use of the surveillance technology was shared with outside entities
- Where and how was the technology installed
- Where the technology was deployed geographically
- Summary of community complaints or concerns, and whether it is adequate in protecting civil rights and civil liberties.
- Results of any internal audits
- Information about any data breaches
- Statistics and information about public records act
- Annual cost and funding data
- Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

### ***San Francisco Surveillance Ordinance and Facial Recognition Ban***

The City of San Francisco on May 14, 2019 adopted a Surveillance Ordinance very similar to Oakland's Surveillance Ordinance. However, unlike Oakland's Surveillance Ordinance, the San Francisco Ordinance also contains the following language, "*it shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology.*"

### **ANALYSIS AND POLICY ALTERNATIVES**

Real-time FRT is starting to be used with surveillance systems in different capacities. Different United States airports are starting to implement the technology<sup>1</sup> in conjunction with the United States Department of Homeland Security. Such systems can immediately, or within seconds or minutes, connect recorded photographs to photographs stored in different databases. These systems can be used to match people in real time at the airports for antiterrorism security purposes. Current research shows that the use of real-time FRT can lead to false positives and other forms of inaccuracies<sup>2</sup>.

OPD does not currently possess real-time (or any) facial recognition technology (FRT) and has no immediate plans to purchase FRT. However, staff does believe that Oakland's current surveillance technology provides adequate thresholds for reviewing any possible future requests to test or purchase FRT. Staff also believes that non-real-time FRT, if deployed with proper safeguards, can provide important benefits to law enforcement. Non-real time FRT cannot be used to connect people as they go about their normal course of life and business. However, law

<sup>1</sup> [https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/?utm\\_term=.e34a72693a04](https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/?utm_term=.e34a72693a04)

<sup>2</sup> <https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936>

enforcement can use FRT to expedite the time-consuming manual process of connecting images from crime scenes to local mug shot databases.

The San Mateo Sheriff's Office has created an in-house facial recognition system that can scan photographs of mugshots housed in their mugshot database. The San Mateo Sheriff's Office has shared this system with the Northern California Regional Intelligence Center (NCRIC); police departments can now ask NCRIC to see if there are matches of surveillance photos with photos stored in the San Mateo database (there is no connection to statewide DMV databases, or other city or county databases). In some recent examples, NCRIC has helped the San Francisco Police Department search for matches with a robbery investigation, the San Jose Fire Department has found help with matches related to a wildfire arson investigation, the San Francisco District Attorney's Office has received help with matches related to an auto burglary investigation, and the FBI has received help with photo matching in connection with a homicide investigation. In each of these anecdotal cases, FRT was beneficial to the overall investigation.

The FRT matching process is only as good as the facial data possessed by the originating police agency - most of the time the search does not yield a match. Sometimes NCRIC analysts will get results with scores lower than ideal; results must always be used in connection with other evidence. If results are not clear even after compared with other results, then the FRT matches are disregarded, and investigators must explore other investigative avenues. FRT results are merely investigative leads to follow, and are not definitive in and of themselves. FRT analysis results should always be verified via other means and procedures. Furthermore, FRT can be used (and has) to exonerate individuals by showing that there is clearly no match with evidence from a crime scene.

The Economist magazine recently reported that Ottawa Police are piloting FRT. Ottawa police report that the system lowers the time required to identify a subject of an image from 30 days to three minutes<sup>3</sup>.

***Recommended amendments to proposed changes to Chapter 9.64 "Regulations on City's Acquisition And Use Of Surveillance Technology"***

OPD understands the concerns of the PAC, leading to a request to ban any use of FRT. As stated above, OPD could not purchase or use any type of FRT without first going to the PAC and producing a Use Policy Report and as well as an Impact Report – and then the PAC would still have the option of recommending or not recommending the particular FRT to the City Council. Therefore, staff does not believe that any ban is needed in Oakland given the current surveillance technology restrictions. However, OPD believes that a more restrictive ban on only "real-time" FRT would send a strong message about the understandable concerns of FRT, while still providing the possibility of OPD using FRT at some point in the future. Additionally, OPD believes that it is not in the City's best interest to make it unlawful to "obtain, retain, request, or access" FRT evidence obtained from other law enforcement agencies – as suggested by the proposed ban. NCRIC, the Federal Bureau of Investigation, the Alameda County Sherriff, or some other police agency may have evidence from FRT that can help OPD with a crime investigation. In such cases OPD would only use the FRT evidence in conjunction with other

<sup>3</sup> <https://www.economist.com/united-states/2019/05/23/america-is-turning-against-facial-recognition-software>

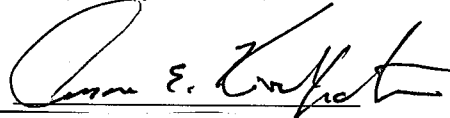
evidence. An outright ban on the accessing or obtaining such types of evidence may limit the ability of OPD's Criminal Investigations Division (CID) to solve homicide, robbery and other violent crimes in the future. Staff therefore recommends amendments to proposed changes to the Ordinance in Chapter 9.64 "Regulations on City's Acquisition And Use Of Surveillance Technology" (**Attachment A** to this report).

**ACTION REQUESTED OF THE CITY COUNCIL**

Staff Recommends That The City Council Adopt An Ordinance Amending Chapter 9.64, Regulations on City's Acquisition And Use Of Surveillance Technology To Add The Definition Of Real-Time Face Recognition Technology Under Oakland Municipal Code, Section 9.64.010.13 And Add To Make It Unlawful For Any City Staff To Use Any Real-Time Face Recognition Technology Under Oakland Municipal Code Section 9.64.030.1.F

For questions regarding this report, please contact Bruce Stoffmacher, Acting Police Services Manager, Training Division, at (510) 238-6976.

Respectfully submitted,



Anne E. Kirkpatrick  
Chief of Police  
Oakland Police Department

Reviewed by:  
James Bassett, Captain  
OPD, Criminal Investigations Division

Omar Daza-Quiroz, Sergeant  
OPD, Intel Unit

Prepared by:  
Bruce Stoffmacher, Acting Police Services  
Manager OPD, Training Division, Research and  
Planning

Attachments (1)  
A: OPD Proposed Changes to OMC Chapter 9.64

Item: \_\_\_\_\_  
Public Safety Committee  
June 25, 2019

## OAKLAND CITY COUNCIL

ORDINANCE NO. \_\_\_\_\_ C.M.S.

INTRODUCED BY COUNCIL PRESIDENT KAPLAN

---

**ORDINANCE AMENDING OAKLAND MUNICIPAL CODE CHAPTER 9.64  
TO PROHIBIT THE CITY OF OAKLAND FROM ACQUIRING AND/OR  
USING REAL-TIME FACE RECOGNITION TECHNOLOGY**

**WHEREAS**, according to the American Civil Liberties Union (ACLU), "facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them"; and

**WHEREAS**, Georgetown Law's Center on Privacy and Technology (CPT) issued a report "Garbage in and Garbage Out" in May 2019, detailing how law enforcement agencies across the country are feeding facial recognition software flawed data stating "when blurry or flawed photos of suspects have failed to turn up good leads, analysts have instead picked a celebrity they thought looked like the suspect, then run the celebrity's photo through their automated face recognition system looking for a lead" and that there are "no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads"; and

**WHEREAS**, in a 2018 report by the MIT Lab, "Gender Shades: Intersection Accuracy Disparities in Commercial Gender Classification," the study concluded, using a data set of 1,270 people, that facial recognitions systems worked best on white males and failed most often with the combination of female and dark-skin individuals with error rates of up to 34.7%; and

**WHEREAS**, the ACLU in 2018, tested a face recognition tool, called "Rekognition," and the software incorrectly matched 28 members of Congress, identifying them as people who had been arrested for a crime; and

**WHEREAS**, at May 2019 World Economic Forum, George Soros warned of the Chinese government's use of artificial intelligence as an "unprecedented danger" in their monitoring and targeting members of the Uighurs, a Muslim minority group in China; and

**WHEREAS**, a Stanford study used face recognition technology to see if it could determine sexual orientation of participants and this raises ethical concerns on the use of this technology as a tool for persecution of historically disenfranchised groups; and

**WHEREAS**, in 2018, the South Wales Police used face recognition software on 170,000 people at a Real Madrid versus Juventus football game and out of 2,470 potential matches with possible criminals, 92% or 2,297 were incorrect; and

**WHEREAS**, in Baltimore, Maryland, police agencies used face recognition technology to target activists in the aftermath of Freddie Gray's death by law enforcement; and

**WHEREAS**, in Sri Lanka, authorities using face recognition technology misidentified an American student as a terrorist responsible for killing 300 people in April 2019, widely circulating her image before having to issue an apology; and

**WHEREAS**, an 18-year-old college student Ousmane Bah, is suing Apple and its contractor, Security Industry Specialists, for allegedly relying on facial recognition systems that misidentified him as a serial shoplifter; and

**WHEREAS**, police forces in Great Britain are using facial recognition software at festivals and in malls and public spaces and are currently facing legal challenges; and

**WHEREAS**, the New York City Police Department is currently facing a lawsuit on their use of face recognition technology; and

**WHEREAS**, United States Representative Alexandria Ocasio-Cortez expressed concerns at a May 2019 House Oversight Committee hearing on facial recognition technology about "the harvesting of facial recognition data without the consent or knowledge of individuals amid the rise of fascism and authoritarianism"; and

**WHEREAS**, in adopting the City of Oakland's Surveillance and Community Safety Ordinance (Ordinance No. 13489 CMS, codified as Chapter 9.64 of the Oakland Municipal Code), the Oakland City Council (City Council) found that "strong consideration" is required on behalf of the City Council on the "impact such technologies may have on civil rights and civil liberties"; and

**WHEREAS**, on May 2, 2019, the City of Oakland's Privacy Advisory Commission voted unanimously to support a proposal that would ban the City of Oakland's use of face recognition technology based on empirical evidence on misidentification, concerns around privacy, and studies of misuse by police departments; and

**WHEREAS**, the City Council finds that ethical dilemmas exist around privacy and the intrusiveness of face recognition technology, the lack of parameters set for the use of this technology by police departments, and that a multitude of studies show that algorithms have gender and race bias;

**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. Purpose and Intent.** It is the purpose and intent of this Ordinance to prohibit the City's acquisition or use of any Face Recognition Technology.

**Section 3. 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. 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 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;
  - 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. "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. "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. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.
5. "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. "Real-Time Face Recognition Technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face in real-time or within a very short period of time.
7. "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.
8. "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.
9. "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. "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. "Surveillance Technology" means any software, electronic device, system utilizing an electronic device, or similar 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.
  - A. "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:
    1. 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;
    2. Parking Ticket Devices (PTDs);
    3. 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;
    4. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
    5. 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;
    6. 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.
    7. Medical equipment used to diagnose, treat, or prevent disease or injury.
    8. Police department interview room cameras.
    9. Police department case management systems.
    10. Police department early warning systems.
    11. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

12. "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 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, 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. "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;
- 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.

**9.64.045. Prohibition on City's Acquisition and/or Use of Real-Time Face Recognition 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. Real-time Face Recognition Technology; or
  - 2. Information obtained from Face Recognition Technology.
- B. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from Face Recognition 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 logs such receipt, access, or use in its Annual Surveillance Report as referenced by Section 9.64.040. Such report shall not include any personally identifiable information or other information the release of which is prohibited by law.

**SECTION 4. 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 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. effective immediately upon 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: \_\_\_\_\_

LATONDA SIMMONS

City Clerk and Clerk of the Council of the City of  
Oakland, California

Date of Attestation: \_\_\_\_\_