APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL

ORDINANCE NO. 13563 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 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; and

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 and/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. <u>"Face Recognition Technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.</u>

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 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. 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, SEP 17 2019

PASSED BY THE FOLLOWING VOTE:

AYES - FORTUNATO BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO AND PRESIDENT KAPLAN — 7

NOES – Ø

ABSENT – Ø

ABSTENTION – Ø

Excused – 1 Thao

ATTEST: _____
LATONDA SIMMONS
City Clerk and Clerk of the Council of the City of Oakland, California

Introduction Date

JUL 16 2019

Date of Attestation: _____

NOTICE AND DIGEST

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

This ordinance amends Oakland Municipal Code Chapter 9.64 to prohibit the City of Oakland from acquiring and/or using face recognition technology. The ordinance also defines the term "Face Recognition Technology."