



AGENDA REPORT

TO: Edward D. Reiskin
City Administrator

FROM: Joe Devries
Chief Privacy Officer

SUBJECT: Amendments to the Surveillance
Technology Ordinance

DATE: November 17, 2020

City Administrator Approval 

Date: Dec 9, 2020

RECOMMENDATION

STAFF RECOMMENDS THAT THE COUNCIL ADOPT AN 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 REGARD 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 (CEQA) EXEMPTION FINDINGS.

EXECUTIVE SUMMARY

The City's Privacy Advisory Commission (PAC) began to consider several changes and updates to the Surveillance Technology Ordinance underlying citywide restrictions on surveillance technology at the July 2, 2020 meeting. The Oakland Police Department (OPD) collaborated with the PAC and the City's Chief Privacy Officer (CPO) to share how the current regulations as well as proposed PAC recommendations would impact OPD and other City Departments. The PAC asked that OPD propose additional recommendations to align with technical details of surveillance technology operations. Those discussions resulted in the proposed amendments unanimously approved by the PAC. There were additional language changes recommended by OPD that the PAC rejected as discussed below.

BACKGROUND / LEGISLATIVE HISTORY

The City Council adopted Ordinance No.13489 C.M.S. in May 2018, adding Chapter 9.64 to the Oakland Municipal Code, establishing rules for the City's acquisition and use of surveillance equipment. This ordinance made Oakland one of the first cities in the nation to create a public process to evaluate the acquisition and use of surveillance technology. The ordinance requires PAC review and approval before any new technology can be acquired or used and requires annual reporting to the PAC and ultimately the City Council on those uses. It also requires that

City Council (or Committee)
Meeting Date

existing technology undergo a similar approval process but allows departments to continue to use those technologies while that process is completed. The process established requires departments to submit a Surveillance Impact Report and a proposed Surveillance Use Policy for each item which the PAC carefully considers, proposes modifications and then forwards to the City Council.

The process has created a working relationship between PAC Members, OPD, and other City Departments and has helped to create a better understanding of why certain technologies are important to the City and why civil liberties and protections on the use of data are needed. The existence of such an ordinance and adherence to it has helped increase public trust that the City takes issues of privacy seriously. At two years since initial adoption, the PAC began discussions about how the ordinance could be modified to add clarity to the process for all involved.

ANALYSIS AND POLICY ALTERNATIVES

OPD-PAC Agreement for Revisions to OMC 9.64

In many ways, the OPD-PAC-CPO discussions over several PAC and ad-hoc meetings allowed all involved to recommend mutually agreed upon improvements to OMC 9.64. The following list highlights OPD-PAC agreement:

- **Banning Predictive Policing Definition:** OPD held concerns that the original PAC proposal to completely ban “Predictive Policing Technology” would inadvertently restrict OPD’s use of standard software tools for crime data analysis and reporting. OPD does not use the type of predictive policing technology that raises concerns for the PAC nor has plans to acquire such systems. The revised definition under Chapter 9.64.010 “Definitions” now defines “Predictive Policing Technology” in a way that would not restrict OPD from using current crime analysis computer software.
- **Collating Race Data:** Chapter 9.64.010.1.E Definitions, “Annual Surveillance Report,” Section E requires “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 identify the race of each person that was subject to the technology’s use.” OPD staff articulated that for some technologies such as Body-Worn Cameras (BWC), it will be practically impossible to analyze the race of every individual recorded. The PAC concurred with OPD’s concerns and agreed to add the following: 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.
- **Exempting Standard Police Data Tools:** 9.64.010 – Definitions “Surveillance technology” includes several exceptions that should not be considered Surveillance Technology. OPD explained how it uses its computer-aided dispatch (CAD) Record Management System

(RMS) as well as police management systems and field-based reporting systems. The PAC agreed with OPD's assessment and the new version of the OMC exempts these tools which OPD uses daily for mission critical dispatch, documentation and oversight functions.

- Exempting Live-Scan Machines: The PAC-recommended changes to OMC 9.64 now exempts live scan machines. OPD uses an Alameda County Sheriff's Department-owned but OPD personnel-operated system exclusively for conducting sex registrant fingerprinting, court bookings, juvenile in-custody fingerprinting, and applicant fingerprinting.
- PAC and Council Notifications: OPD, the PAC and the CPO made an important improvement to OMC 9.64 in terms of how new and existing technology must be reviewed by the PAC and City Council. The original version of the Ordinance required that city departments notify the PAC before seeking outside funding (grants), and before making any purchases for surveillance technology – regardless of whether the PAC and City Council had already reviewed and adopted the required Surveillance Use Policy (SUP). This was an error in the original language and not the intent. Furthermore, the existing law did not provide clarity as to whether existing technology managed by a department could be used at all before PAC and City Council review; the intent of the original Ordinance is that departments such as OPD can continue to use “existing” surveillance technology (e.g. BWC) as long as they provide a list of existing technologies to the PAC with a proposed schedule for PAC review of the associated SUP. Chapter 9.64.020 “Privacy Advisory Commission (PAC) notification and review requirements” as well as 9.64.030 “City Council approval requirements for new and existing surveillance technology” both now clarify in the PAC-proposal that City Departments need to present funding and purchase proposals only for surveillance technology that has not already been reviewed by the PAC and with a Council adopted-SUP.
- Annual Reporting Timing: The ordinance originally required annual reports to be submitted by March 15th of every year, but this would cause a glut of reports in one month and for technologies adopted early in the year there would not be significant data to report. Now the ordinance states, by April 30th or within one year of adoption of the SUP.
- Correcting Language regarding Public Hearings: The ordinance originally had language stating that the City Council would consider a proposed technology with notification at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. This language was boilerplate language that was part of a model ordinance that was being shared across jurisdictions with a goal of assuring transparency in the approval process. The new language aligns the process with Oakland's Sunshine Ordinance and is clear that all approvals must occur at a public City Council meeting with proper noticing.

City-PAC Differences on Revisions to OMC 9.64

There were additional changes recommended by OPD that the PAC chose not to include in its recommendation. The following list highlights these recommendations:

- **Data Sharing Reporting:** 9.64.010.1.B “Definitions. Annual. Data Sharing”: This section requires departments to disclose in the surveillance technology annual report, “Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities and the name of any recipient entity. OPD promoted adding **if known and if practicable** to those requirements due to the large number of times OPD may share information about evidence and suspects regularly with other neighbor police departments. OPD cannot always track such data sharing and therefore there is a risk that OPD cannot functionally comply with this Ordinance section. The Council could choose to add this language or, as the Annual Reports begin to be submitted, staff and the PAC will need to monitor this to see if any City department appears to inadvertently violate the reporting requirement for any technology. The argument against adding this language is that it could be misused by a department that was not careful in tracking any data sharing with outside agencies. The City’s adopted Privacy Principles require that data only be used for the purpose it was collected and sharing that data with an outside entity could allow for data to be used for a different purpose.
- **Biometric Definition:** 9.64.010.2 – defines “Biometric Surveillance Technology.” 9.64.045 later bans “biometric surveillance technology.” Then 9.64.010.14. defines “Surveillance Technology” and uses the word biometric as an aspect of “surveillance technology” that is not banned but regulated. This double use of “biometric” could be confusing and finding alternative language to add more clarity to these Ordinance sections could be helpful. At this time there is not alternate language that is being recommended. However, an additional edit was provided in Section 9.64.045 clarifying that the intent of the new provision prohibiting Biometric Surveillance Technology is not to prohibit *any* type of surveillance technology that uses biometric information, but rather only surveillance technology that meets the definition of that term as provided in the ordinance. As with the prior item, the PAC and OPD will need to monitor this potential problem to see if future revisions are needed.
- **Providing Contracts:** 9.64.010.15.H “Definitions, Surveillance Impact Report (SIR), Fiscal Cost” requires that staff include in the SIR, “the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract, and any current or potential sources of funding.” Staff explained to the PAC that a department may seek to develop a Surveillance Use Policy before developing a budget, requesting technology product costing, or have a detailed contract to share with the PAC. For example, both the Department of Transportation (DOT) and OPD developed a policy for unpiloted aerial systems (drones) and the PAC voted to recommend the policy to the City Council. However, neither department had secured final funding nor has a contract to share at the time of this report. Staff therefore recommends flexibility in the reporting requirement for this SIR section. The argument in favor of requiring this is it gives the PAC a sense of the likely cost of a technology or the entity with which the City intends to contract which may influence the PACs recommendation. As stated above, a department may wish to seek

authorization to acquire and use a technology long before ever applying for grant funds, selecting a vendor, or contemplating annual costs. As new technology is considered, the CPO will monitor whether this requirement hinders the timely adoption of a Use Policy.

FISCAL IMPACT

There are no direct fiscal impacts associated with the adoption of these ordinance amendments however, simplifying when a department must appear before the PAC could reduce staff time associated with the process.

PUBLIC OUTREACH / INTEREST

The PAC met publicly and discussed this item at its July, August, and September meetings.

COORDINATION

OPD, the City Administrator's Office, and the City Attorney's Office worked in partnership with the PAC on these amendments.

SUSTAINABLE OPPORTUNITIES

Economic: There are no economic opportunities identified in this report.

Environmental: There are no environmental opportunities identified in this report.

Race & Equity: The Surveillance Technology Ordinance provides residents with a public process to evaluate how the City monitors its residents. Having such a process indicates that the City is responding appropriately to concerns about civil liberties and privacy during a time of rapidly evolving technology. By establishing safeguards to prevent potential abuse of technology, the City strengthens residents' faith in local government and allows for robust public dialogue and increased trust.

ACTION REQUESTED OF THE CITY COUNCIL

STAFF RECOMMENDS THAT THE COUNCIL ADOPT AN 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

For questions regarding this report, please contact Joe DeVries, Chief Privacy Officer at (510)238-3083.

Respectfully submitted,



Joe DeVries
Chief Privacy Officer