MITCHELL CHYETTE [113087]
Law Office of Mitchell Chyette
125 12th Street
Suite 100-BALI
Oakland, CA 94607
Telephone: (510) 388-3748
Email: mitch@chyettelaw.com
Attorney for Petitioners

IN THE SUPERIOR COURT OF CALIFORNIA

COUNTY OF ALAMEDA

RG21111681

SECURE JUSTICE, INC., a California non-profit organization, and BRIAN HOFER, a California citizen

Petitioners,

vs

THE OAKLAND POLICE DEPARTMENT, and THE OAKLAND CITY ATTORNEY'S OFFICE,

Respondents.

Case No.

PETITION FOR WRIT OF MANDATE AND PROHIBITION

INTRODUCTION

Quis custodiet ipsos custodes?

(Who watches the watchers?)

1. "Police today increasingly rely on technologies of surveillance, data collection, inference, and prediction. These technologies include tools like body cameras, license plate readers, data analytics, and predictive crime software. All of them have in common a reliance on artificial intelligence and enormous amounts of digitized data. We can refer to these tools broadly as "police surveillance technologies." Elizabeth E. Joh, Thomas Wuil Joo, *The Harms of Policy Surveillance Technology Monopolies,* (April 26, 2021) (to be published in the Denver Law Review; available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834777.)

2. Police surveillance technologies may help reduce crime. But they also pose a clear and present threat to the civil liberties of the citizens of Oakland. The "inquiry in any given case depends ultimately on the judgment 'whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.' Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 403 (1974); see also 1 W. LaFave, Search and Seizure § 2.1(d), pp. 310-314 (2d ed. 1987)." *Florida v. Riley*, 488 U.S. 445, 700 (1989) (J. Brennan, dissenting)

3. Recognizing that a balance must be struck, on January 19, 2016, the City of Oakland ("City") enacted Ordinance No. 13349, which created a first-of-its-kind civilian oversight body of subject-matter experts—the Privacy Advisory Commission ("PAC—to advise the City Council about how best to balance the potentially harmful effects of police surveillance technology, data mining practices, and public safety. The Ordinance states:

> PAC must "Provide advice and technical assistance to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects and stores citizen data.

4. On May 15, 2018, the City enacted Ordinance No. 13489 (Oakland Municipal Code § 9.64 *et seq.*), commonly referred to as the Surveillance Technology Ordinance ("Surveillance Ordinance," Exhibit A).[1] The preamble to this ordinance outlines its purpose:

> WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Oakland's ("City") acquisition and use of surveillance technology; and
>
> WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and
>
> WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and
>
> WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and
>
> WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties including those rights guaranteed by the California and United States Constitutions; and
>
> ***
>
> WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed;

[1] Amended on January 12, 2021 (Exhibit B).

5. The Surveillance Ordinance provides that PAC is responsible for vetting surveillance technology proposals submitted by city departments.

6. The Surveillance Ordinance recognized that the Oakland Police Department (OPD) may use surveillance technologies in an approved manner under "exigent circumstances."

7. The Surveillance Ordinance requires, among other things, that:

a. The City Council draft additional ordinances establishing policies for the use of surveillance technology,

b. The City Council submit at least one proposed use policy per month for review in March, April, and May 2021,

c. The Oakland Police Department (OPD) provide the PAC with a report on its use of surveillance technology under the exigent circumstances exception,

d. That the OPD adopt policies for the use of surveillance equipment not yet covered by an approved policy, and

8. As shown below, OPD and the Oakland City Attorney (OCA) have obstructed, practically thwarting, PAC from doing its job. Along the way, they have violated the Surveillance Ordinance along with several other statutes and policies and have obstructed PAC and the City from fulfilling the purpose of the Surveillance Ordinance.

JURISDICTION AND VENUE

9. This Court has jurisdiction under article VI, section 10 of the California Constitution and Code of Civil Procedure sections 1085 and 1060.

10. Venue in this court is proper because Petitioner's claims arose in the City of Oakland, and because this is an action against Respondent. Code Civ. Proc. § 394.

PARTIES

11. Petitioner Secure Justice, Inc. ("Secure Justice") is an IRS registered non-profit organization located in Oakland, Alameda County that advocates against state abuse of power, and for a reduction in government and corporate over-reach.

12. Brian Hofer is an individual citizen of Oakland, California, the Executive Director and Chair of Secure Justice. Hs is also the Chair of the PAC.

13. Respondents Oakland Police Department and Oakland City Attorney are departments of the City of Oakland, a charter city.

A WRIT OF MANDATE/PROHIBITION IS APPROPRIATE

14. Secure Justice and Mr. Hofer are the real parties in interest in this action. Citizens of California are guaranteed a right to privacy under California Constitution, Article I, section 1. As citizens of Oakland, Petitioners have a vital interest in seeing that the OPD's use of police surveillance technology does not infringe upon that right. With the Surveillance Ordinance, the City Council set up a system of checks and balances by established PAC to advise the Council on issues relating to police surveillance technology. Petitioners thus have a substantial beneficial interest in seeing to it that PAC can perform its functions and that the OPD and OCA not interfere with PAC's role.

15. Petitioners have no legal remedy that would compel OPD and OCA to do their duty under the laws discussed below.

FIRST CAUSE OF ACTION

(Against the OPD)

Failure to Comply with the California Public Records Act

16. Petitioner incorporates by reference the allegations of the above paragraphs as though fully set forth herein.

17. OPD uses a technology called automated license plate reader ("ALPR"). This technology allows an OPD officer to use a camera to scan a scene, and the computer software artificial intelligence (AI) will identify license plate numbers. From this, the AI can inform the police officer of any information OPD has relating to the car. In addition, the AI coordinates with GPS, allowing the AI to record where and when the car was seen.

18. In 2016, OPD adopted a policy for using ALPR and ALPR data (2016 ALPR Use Policy).

19. Most ALPR use amounts to nothing more than mass surveillance—an indiscriminate collection of data about people not suspected of wrongdoing.

20. OPD has not offered to the PAC or any public any legal authority allowing it to conduct mass surveillance. OPD attempts to justify such practices by claiming that once it identifies a suspect it can use the ALPR data to investigate where the suspect has been.

21. One of PAC's functions is to address the disparate impact of the use of police surveillance technologies. The concern is that such technologies may be used against certain communities more than others. The concern is well-founded. A 2015 Electronic Frontier Foundation analysis of OPD's raw ALPR data showed that certain populations are targeted by OPD's ALPR use more than others for no obvious law enforcement purpose. A study by Stanford University's Dr. Eberhart showed OPD's vehicle-stop data demonstrated racial profiling by OPD.[2] And OPD is in its 18th year of federal monitoring due to a lengthy and horrible history of racial profiling.

22. In early 2021, PAC's review of OPD's 2016 ALPR Use Policy uncovered many deficiencies and misrepresentations. Notably, each version of the 2016 ALPR Use Policy includes a representation that OPD would perform audits of its surveillance technology use.

23. However, no such audits were produced in 2016, 2017, or 2018. When this was brought to OPD's attention during a PAC meeting on February 4, 2021, OPD admitted no such audits had been undertaken.

24. OPD then represented at that very same meeting that such audits *would* be performed going forward.

---

[2] The study showed 61% of all individuals stopped were African American, despite making up less than 25% of Oaklanders and despite similar rates of contraband being found as other races; 77% of OPD officers never discretionarily searched a white person, but 65% did so with an African American. Furthermore, 74% of OPD officers did not handcuff a white person that was ultimately not arrested, yet 72% of OPD officers did with an African American that was ultimately not arrested.

25. As of this date, no audits have been produced to the PAC.

26. The 2016 ALPR Use Policy and Civil Code section 1798.90.52 (Senate Bill 34) require that OPD maintain a record of access to the ALPR data—that is, a record of who used the database and for what purpose.

27. The OPD 2016 ALPR Use Policy requires that OPD destroy the APLR data it collects six months after it is accumulated.

28. At the August 5, 2021, PAC meeting, OPD admitted in writing that "based upon legal counsel..." OPD unilaterally decided to disregard the six-month retention period in its own policy and that, beginning in 2019, they had begun retaining data for two years. OPD's unilateral adoption of an extended retention policy violated the Surveillance Ordinance provision requiring City Council approval (after vetting by the PAC) for any new use (purpose, manner, location) of police surveillance technology acquired before enactment of the Surveillance Ordinance.

29. At the August 5, 2021, PAC meeting OPD also confirmed that it was allowing the Federal Bureau of Investigation unfettered data access to the ALPR data without "following the standard data access request protocols outlined in the" ALPR policy. And OPD admitted that "current data-sharing practice does not align with limits set forth in" the ALPR policy.

30. OPD has, in effect, arrogated to itself the determination of who can access the APLR data and for how long without seeking the input or advice of PAC or the City Council.

31. In light of OPD's refusal to provide advance notice about how it is using APLR to PAC, on March 18, 2019, Mr. Hofer submitted a public record request under the Public Records Act, Govt. Code section 6250 *et seq.* (PRA) for the "record of access" documents.

32. OPD failed to respond in compliance with PRA's section 6253(c).[3]

---

[3] https://oaklandca.nextrequest.com/requests/19-1382 (contains both the request and response)

33. In April 2019, OPD represented to PAC[4] that 147 emails showed successful historical searches (or requests for such searches), attempting to justify OPD's mass surveillance practices by demonstrating the need to retain data for a lengthy period. However, OPD refused to produce the emails to PAC and told Mr. Hofer to submit a PRA request.

34. On April 16, 2019, Mr. Hofer submitted the suggested PRA request for the 147 emails.[5]

35. OPD declined to respond, violating PRA's section 6253(c).

36. In July 2021, after repeated threats of litigation, OPD attempted to partially cure its violation of the PRA by providing a limited set of emails (i.e., less than the 147 referred to) to Mr. Hofer. These emails were mostly non-responsive. They showed that most APLR database search queries were initiated within 48 hours or less of an incident (thus contradicting OPD's claim that it needed a two-year retention period). Only one email demonstrated that ALPR data had successfully assisted in the investigation of a crime.

37. In the absence of any data from OPD, and in light of OPD's resistance, misrepresentations, and misuse, PAC recommended to the City Council that OPD's use of ALPR be prohibited for two years.

38. On May 11, 2021, PAC's recommendation was heard by Oakland's Public Safety Committee. In the staff report to the Committee, OPD offered that (a) that they had always maintained the record of access and (b) that they were (only) now considering whether it was an undue burden to produce the 147 emails. OPD misstated the state laws as to record retention and record disclosure and misled the City Council about its past actions concerning ALPR.

---

[4] Orally and in writing. *See* Surveillance Ordinance's "impact statement" for the ALPR technology.

[5] https://oaklandca.nextrequest.com/requests/19-1897 (contains both the request and response)

39. After listening to public comments, and presentations from OPD and PAC, the Public Safety Committee voted unanimously to remand the issue to the PAC and directed OPD to provide "the requested information to allow for data analysis and evaluation."

40. OPD has not provided the information requested.

41. On May 12, 2021, Mr. Hofer met with almost the entire command staff of OPD, including newly appointed Chief LeRonne Armstrong and Deputy Chief Drennon Lindsey. Each OPD representative that spoke to Mr. Hofer, including Chief Armstrong and Deputy Chief Lindsey, promised that all of the missing information referenced in the PAC's recommendation to limit the use of APLR would be supplied to the PAC and that OPD desired to "reset the clock" with the PAC.

42. The missing information was *not* provided.

43. On May 23, 2021, Mr. Hofer submitted a PRA request for all writings pertaining to the May 11th OPD ALPR staff report, and further provided the names of all OPD agents identified on the written documents to aid in the search of records.

44. On May 28, 2021, OPD responded by closing the request and stating that no responsive documents had been found—which is obviously untrue since the staff report itself, which was provided to the PAC, would have been within the scope of the PRA request.[6]

45. On July 31, 2021, Mr. Hofer submitted a PRA request asking for the "guidelines and procedures to comply with the requirements of Civil Code section 1798.90.5 et seq." per the OPD 2016 ALPR use policy. Per OPD's policy, the Bureau of Services Deputy Chief was to develop such guidelines.

46. OPD did not respond to this request.

47. On July 31, 2021, Mr. Hofer submitted a PRA request for the annual reports required under Government Code section 12525.5 *et seq.* (AB 953, the Racial

[6] https://oaklandca.nextrequest.com/requests/21-4581

and Identity Profiling Act"). Annual reports for 2020 and 2021 were due under this law.

48. OPD has not provided the annual report for 2021 and has stated in writing that they did not create it as required by law.

49. OPD is making it impossible for PAC, and, by extension, the City Council, to perform its oversight function to protect the citizens of Oakland from undue violation of their right to privacy. The records of how OPD uses the APLR, what its policies are toward the use of APLR, and who has access to APLR data are essential to PAC's oversight framework and important to the public's concerns for privacy. OPD's actions violate the Surveillance Ordinance and the corresponding use policies.

WHEREFORE Petitioners request the Court issue a writ of mandate as follows:

a. Compel OPD to provide the requested public records per Request Nos. 19-1382, 19-1897, and 21-4581; or in the alternative if such records were never created, compel OPD to create the required records and disclose them to Petitioners as requested.

b. Compel OPD to destroy APLR data older than six months, or to submit for public comment a request to change the 2016 ALPR Use policy and abide by the City Council's decision on that issue.

c. Compel OPD to maintain a record of access to the APLR database.

d. Compel OPD to maintain a record of access to all future police surveillance technology databases.

e. Compel OPD to provide the record of access to PAC upon request.

SECOND CAUSE OF ACTION

OPD's Violations of Surveillance Ordinance (O.M.C. § 9.64 *et seq.*)

50. Petitioner incorporates by reference the allegations of the above paragraphs as though fully set forth herein.

Exigent Circumstances Violations

51. The Surveillance Ordinance's section 9.64.035 allows OPD to use police surveillance technology without prior approval only in narrow exigent circumstances. Each use must be reported to the PAC for discussion and possible recommendations to the City Council.

52. Exigent circumstances are defined by the Surveillance Ordinance as "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." O.M.C., § 9.64.010 6.

53. On January 7, 2020, OPD used an Unmanned Aerial System or "drone"—a type of police surveillance technology—during a pre-planned search warrant operation. The pre-planned nature, and presence of a search warrant contra-indicate any "imminent" or emergency need, as OPD clearly had time to coordinate the operation and obtain a search warrant. In addition, OPD's own report states that the "suspects were ordered outside, detained without incident, and taken into custody," confirming that no exigent circumstances as defined arose during the operation. The drone was used to shine a light on the outside of a building.

54. On June 24, 2020, OPD used a drone again during an investigation into a missing person's report for a 12-year-old girl. OPD's report identified no imminent threat of death or serious physical injury, and essentially, they flew the drone around various streets looking for someone with similar clothing. No one was identified by the drone. Fortunately, the girl was later found.

55. Neither of the January 7, 2020, nor the June 24, 2020, exigent circumstances reports was submitted to the City Council in violation of O.M.C. § 9.64.035 2 D.

56. To be clear, Petitioners do not object to the use of police surveillance technology where there are indeed exigent circumstances. Petitioners object to OPD's refusal to follow up with reports to the PAC, so the PAC can evaluate whether, indeed, the technology is being used for such purposes.

Failure to Submit New Technology Policies for Review

57. The Surveillance Ordinance applies not only to police surveillance technology that might be acquired in the future but also to equipment already in the possession of city departments before the enactment of the Surveillance Ordinance.

58. OPD is obliged by the Surveillance Ordinance to draft policies for the use of such technologies.

59. The PAC and commissioners work with OPD to identify and rank various technologies in order of concern as to their ability to invade people's privacy. The list and rankings have been in place for years. Upon information and belief, there are approximately seven technologies OPD is using for which (a) OPD has not submitted an explanation to PAC as to whether they are police surveillance technologies, or (b) OPD has not submitted for review its use policies.

Using Police Surveillance Technology in an Unapproved Manner

60. The Surveillance Ordinances requires that OPD obtain City Council approval, after PAC review, for any new uses of surveillance technology not previously approved. O.M.C. § 9.64.030 1 C.

61. One such technology was ShotSpotter. It is an acoustic surveillance system that attempts to triangulate the location of gunfire, ostensibly to direct resources to the scene of the incident more quickly.

62. On November 19, 2019, the City Council adopted DGO I-20—a use policy for ShotSpotter.

63. DGO I-20 B 1 states that only OPD personnel will have access to the ShotSpotter system. Section C 3 states that release of information to any third party requires a "need to know and right to know," requires submission of a written request justifying the need for the data from OPD, and the OPD-approved request must be retained and provided in its annual report to the PAC and City Council.

64. In May and June 2021, the PAC reviewed the inaugural ShotSpotter annual report. In Section B, which pertains to third-party data disclosures, OPD stated that personnel from the Federal Alcohol Tobacco and Firearms Agency (ATF) have direct access to the ShotSpotter system. No need to know/right to know or written requests came into play; these agencies have ongoing login access and do not make written requests for access."

65. When OPD's Bruce Stoffmacher, who wrote the annual report, was questioned about ATF's access, he explained that this was part of the Memorandum of Understanding ('MOU") between OPD and ATF that created an OPD/ATF task force, and that the MOU had been previously approved by the City Council on or about November 2018.

66. The PAC and the City Council reviewed the MOU before it was adopted. The MOU does not refer to ShotSpotter, or gunshot detecting technology; there was no discussion during the PAC or City Council reviews about allowing the ATF unfettered access to ShotSpotter data. The OPD is well aware that third-party data access is consistently a point of concern in all police surveillance technology use policies, and that different parties may have different values—for instance, whether the data will be used in federal immigration enforcement. If the OPD thought the MOU covered the access to the ShotSpotter data without any request for access, it had ample opportunity to bring this to the PAC's and the City Council's attention.

67. In answering the questions about the MOU in May/June 2021, Mr. Stoffmacher could not identify any provision in the MOU that would justify giving ATF unfettered access and refused to answer related questions.

WHEREFORE, Petitioner requests the Court issue a writ:

a. Compelling OPD to refrain from using the exigent circumstances exception without actual exigent circumstances,

b. Compelling OPD to report within 24 hours to PAC about any use of police surveillance technology used under the exigent circumstances exception.

c. Forbidding OPD from allowing ATF or any other state or federal agency or organization from using OPD's police surveillance technology without first obtaining the approval of the City Council.

d. Compelling OPD to submit for approval to PAC and the City Council the new police surveillance technologies it has under consideration before the technologies are implemented.

THIRD CAUSE OF ACTION

OPD's Violation of the Racial and Identity Profiling Act (A.B. 953)

68. Petitioner incorporates by reference the allegations of the above paragraphs as though fully set forth herein.

69. Pursuant to Government Code section 12525.5 *et seq.*, the City and OPD are required to provide annual reports to the California Attorney General specifying all stops made, certain demographic information about the people stopped, and the results of such stops.

70. These reports are critical for PAC, Secure Justice and Oaklanders in general to ascertain whether its police department is behaving appropriately.

71. Neither the City nor OPD has produced the required report for 2021.

72. Mr. Hofer requested such information in his PRA requests, but OPD refused to respond to the requests.

WHEREFORE, Petitioner requests the Court issue a writ of mandate

a. Respond to Mr. Hofer's PRA request in full, and

b. Require that OPD provide the annual reports as required by law.

FOURTH CAUSE OF ACTION

OCA's Refusal to Advise PAC

73. Petitioner incorporates by reference the allegations of the above paragraphs as though fully set forth herein.

74. Section 401(6) of Oakland's city charter states that the "City Attorney...shall advise all...commissions...on legal matters referred to him or her and shall render written legal opinions when the same are requested in writing by...any...commission of the City. He or she shall draft such ordinances...as directed by the Council or requested by the Mayor or City Administrator or any official board or commission of the City."

75. In March 2017, Deputy Attorney Sotelo told PAC that the Office of City Attorney (OCA) would not advise PAC on any legal issues. PAC asked OCA to confirm this in writing, but OCA simply refused to respond.

76. From late 2018 through the spring of 2019, Mr. Sotelo occasionally attended PAC meetings. His legal advice was requested on at least five occasions, as reflected by the March 7, 2019, and April 4, 2019, minutes. The OCA never responded to these requests.

77. On March 27, 2019, Mr. Hofer inquired about the outstanding requests for advice to OPD. OPD replied that it was not OPD's responsibility and copied Mr. Sotelo on his email reply.

78. The OCA never responded.

79. On March 11, 2020, PAC submitted a request to OCA for a written legal opinion as to the legality of OPD's participation in the FBI's Joint Terrorism Task Force.

80. The OCA never responded.

81. On March 16, 2021, PAC submitted a request for a written legal opinion as to whether the Surveillance Ordinance enforcement and oversight mechanisms were incorporated into a grant application known as the "Chinatown Camera" proposal.

82. The OCA never responded.

83. Section 3 of the 2018 Surveillance Ordinance amendment requires that within "180 days" of May 15, 2018, three use policies adopted before the enactment of the Surveillance Ordinance be converted into one or more ordinances to comport with the Surveillance Ordinance provisions and to ensure that the previous policies were enforceable.

84. OCA has neither drafted nor presented the City Council with any such ordinances.

85. OCA's refusal to provide legal advice or assistance to PAC hampers PAC's ability to do its job. It is substantially more difficult for PAC to evaluate the right to privacy with the use of police surveillance technology without being able to consider the legal ramifications of such technology.

WHEREFORE, Petitioner requests the Court issue a writ of mandate:

a. Compelling OCA to advise PAC whenever a legal question is submitted to it;

b. Compelling OCA to prepare the ordinances specified by section 3 of the Surveillance Ordinance;

c. To the extent OCA determines that it has a conflict of interest in advising PAC, to appoint independent counsel to perform its statutory role.

PRAYER FOR RELIEF

WHEREFORE, Petitioner requests that this Court:

A. Issue a writ of mandate and/or prohibition as specified above,

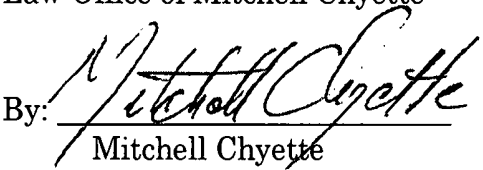
B. Award Petitioners their attorney's fees and costs as provided by the Surveillance Ordinance and Civil Code section 1021.5

C. Award Petitioners their costs,

D. Order such other relief as the Court deems just.

Dated: September 2, 2021

Law Office of Mitchell Chyette

By: 

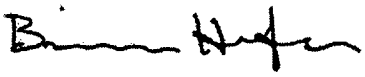
Mitchell Chyette

Attorney for Secure Justice and Brian Hofer

VERIFICATION

I, Brian Hofer, am one of the Petitioners in this action and I am the CEO of Secure Justice, Inc. and am authorized to execute this verification on its behalf. I have read the foregoing Petition for Writ of Mandate and I hereby verify that based on my personal knowledge the facts alleged are true.

Executed this 1st day of September 2021 in Oakland, California, I declare under penalty of perjury that the foregoing is true.



Brian Hofer,
on behalf of Secure Justice

EXHIBIT A.

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2018 APR 26 PM 3:03

APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

AMENDED AT THE APRIL 24, 2018 PUBLIC SAFETY COMMITTEE

OAKLAND CITY COUNCIL

ORDINANCE NO. 13489 C.M.S.

ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Oakland's ("City") acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

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

SECTION 1. This Ordinance shall be known as the Surveillance and Community Safety Ordinance.

SECTION 2. Oakland Municipal Code Chapter 9.64, is hereby added as set forth below (chapter and section numbers are indicated in **bold type.**

Chapter 9.64 REGULATIONS ON CITY'S ACQUISTION AND USE OF SURVEILLANCE TECHNOLOGY

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 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 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. "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.

7. "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.

8. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

9. "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.

10. "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.

6. "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).

7. "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.

9.64.020 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 surveillance technology, 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 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 9.64.020.1.C., City staff shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to 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.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 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;
B. Acquiring new surveillance technology, 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 ordinance; 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. Approval may only occur at a public hearing.
B. The City Council shall only approve any action as provided in this Chapter 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 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 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 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 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. On March 15th of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, 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 March 15th 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 90 days of submission shall enable the City entity to proceed to the City Council for approval of the Annual Surveillance Report.

   D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

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.

9.64.050. Enforcement

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

   A. Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, 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 Ordinance. 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 Ordinance 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 Ordinance, to the extent permitted by law.
   B. Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, 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 $1,000 or $100 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 Ordinance 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 Ordinance, 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 Ordinance; 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 Ordinance.

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 Ordinance.
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. Existing Surveillance Use Policies for the Domain Awareness Center, Forward Looking Infrared Thermal Imaging Camera System, and Cell Site Simulator, Must Be Adopted as Ordinances.

Within 180 days of the effective date of this ordinance, City staff shall return to City Council with an ordinance or ordinances adopting and codifying the following surveillance use policies under the Oakland Municipal Code: the Domain Awareness Center (DAC) Policy for Privacy and Data Retention (Resolution No. 85638 C.M.S., passed June 2, 2015); the Forward Looking Infrared Thermal Imaging Camera System (FLIR) Privacy and Data Retention Policy (Resolution No. 85807 C.M.S., passed October 6, 2015); and the Cell Site Simulator Policy (Resolution No. 86585 C.M.S., passed February 7, 2017) .

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.

IN COUNCIL, OAKLAND, CALIFORNIA, MAY 15 2018

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL-WASHINGTON, GALLO, GIBSON MCELHANEY, GUILLÉN, KALB, KAPLAN - 7

NOES - Ø

ABSENT - Ø

ABSTENTION - Ø

1 Excused - Reid

Introduction Date

MAY 01 2018

ATTEST: _____

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

Date of Attestation: May 18, 2018

EXHIBIT B.

APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL

ORDINANCE NO. 13635 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, JAN 12 2021

PASSED BY THE FOLLOWING VOTE:

AYES -FORTUNATO BAS, GALLO, GIBSON MCELHANEY, KALB, REID, TAYLOR, THAO AND PRESIDENT KAPLAN — 8

NOES – Ø

ABSENT – Ø

ABSTENTION – Ø

ATTEST: _____

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

Introduction Date
DEC 15 2020

Date of Attestation: January 20, 2021

3006267

NOTICE AND DIGEST

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

This Ordinance would amend Oakland Municipal Code Chapter 9.64 to clarify existing definitions, add new definitions, and prohibit certain kinds of new surveillance technology. It also adopts California Environmental Quality Act exemption findings. Upon final adoption on second reading this ordinance will become effective immediately if it receives six or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.