SANNA R. SINGER
ASSISTANT CITY ATTORNEY

JAMES S. MCNEILL
ASSISTANT CITY ATTORNEY

KENNETH R. SO
DEPUTY CITY ATTORNEY

OFFICE OF

THE CITY ATTORNEY

CITY OF SAN DIEGO

MARA W. ELLIOTT

CITY ATTORNEY

1200 THIRD AVENUE, SUITE 1620
SAN DIEGO, CALIFORNIA 92101-4178
TELEPHONE (619) 236-6220
FAX (619) 236-7215

October 30, 2020

REPORT TO HONORABLE MAYOR AND MEMBERS OF THE COUNCIL

ANALYSIS OF REVISED DRAFT TRANSPARENT AND RESPONSIBLE USE OF SURVEILLANCE TECHNOLOGY ORDINANCE

INTRODUCTION

On November 10, 2020, the City Council (Council) is expected to consider an ordinance proposing a comprehensive process for the Council's approval of the City's acquisition, funding, and use of surveillance technology.

By way of background, on September 3, 2020, this Office issued its "Preliminary Analysis of Draft Transparent and Responsible Use of Surveillance Technology Ordinance" (Preliminary Analysis Memo), attached, based on the draft Surveillance Technology Ordinance (Surveillance Ordinance), which was written by the TRUST SD Coalition and presented to the Public Safety & Livable Neighborhoods Committee (PS&LN Committee) on July 15, 2020.

This Office has continued to collaborate with representatives from Councilmember Montgomery Steppe's office regarding proposed revisions and clarifications to the Surveillance Ordinance. Based on this input and guidance, this Office has prepared the attached revised drafts of the Surveillance Ordinance and Privacy Advisory Board for Council discussion.

As with our Preliminary Analysis Memo, this report will highlight policy issues associated with the proposed Surveillance Ordinance for consideration by the Council, City departments, and the public.

ANALYSIS

Our Preliminary Analysis Memo noted that the Surveillance Ordinance was largely modeled after an Oakland ordinance that establishes rules for that city's acquisition and use of surveillance equipment. We identified additional requirements contained in the draft Surveillance Ordinance that differed from the Oakland ordinance, and referenced provisions of the surveillance ordinances used by the cities of Berkeley, Davis, San Francisco, Seattle, Santa Clara County, and the Bay Area Rapid Transit (BART) District that could inform Council discussion.

This report highlights substantive revisions from the prior draft Surveillance Ordinance and discusses new or ongoing issues related to the revised language of the Surveillance Ordinance.

For ease of reference, issues identified thus far are addressed in roughly the order in which they appear in the Surveillance Ordinance:

1. **The Annual Surveillance Report**

    a. **Racial Identification Requirement.** Under Section 511.0101(a)(6), the Surveillance Ordinance no longer requires identification of the race of every individual captured by surveillance technology. It will instead require an analysis regarding whether, and to what extent, the use of surveillance technology disproportionately impacts certain groups or individuals. The City may undertake this analysis itself or use a consultant.

    b. **Public Reporting of Confidential or Sensitive Information that Could Undermine the City's Legitimate Security Interests.** The Annual Surveillance Report retains robust reporting requirements while adding language to Sections 511.0101(a)(2), (a)(4), (a)(7), (a)(8), and (a)(9), that protects the City's confidential and sensitive information. This language, for instance, protects the City from cybersecurity attacks. Council would still be informed of cybersecurity risks through closed session briefings. Section 511.0105(c). This language was added to address the City's Information Technology (IT) Department's concern about potential threats and vulnerabilities to the City's IT security.

    c. **Reporting on Public Records Act Requests.** Under Section 511.0101(a)(11), the reference to including the "response rates" of statistics and information about Public Records Act requests regarding the relevant subject surveillance technology has been clarified to include the number of Public Records Act requests and the open and close date for each of those requests.

2. **Some Definitions Have Been Clarified.** The definition of "City" under Section 511.0101(c) has been clarified to include all mayoral and independent City departments. Likewise, the definition of "City staff" under Section 511.0101(d) has been revised to be consistent with the definition of "City".

    Our Preliminary Analysis Memo sought possible clarification of the definition of "surveillance" or "surveil" under Section 511.010(k) of the Surveillance Ordinance because it differed from the definition in the Oakland ordinance and appeared to be broader. We recommended having the City's IT Department and other impacted City staff review this language. Besides Oakland, the city of Seattle is the only other jurisdiction that defines "surveillance" or "surveil." The City may want to consider

adding clarifying language. Chapter 14.18.010 of the Seattle ordinance, for instance, provides that "[i]t is not surveillance if an individual knowingly and voluntarily consented to provide the information, or had a clear and conspicuous opportunity to opt out of providing the information."

3. **Issues Related to the Definition of "Surveillance Technology."**

   a. **Included Surveillance Technology.** Under Section 511.0101(m), the definition of "Surveillance technology" includes not only the technology itself, but also the "product (e.g. audiovisual recording, data, analysis, report) of such surveillance technology." We were unable to find any other jurisdiction that broadens the definition in this manner. Section 511.0101(m) also includes language referencing examples of what is meant by software such as "scripts, code, Application Programming Interfaces." The City's IT Department can advise whether such references are inclusive and consistent with what is understood to be software.

   b. **Excluded Surveillance Technology.** Consistent with other jurisdictions, the definition of "Surveillance technology" excludes certain technologies. See Section 511.0101(m)(1). This list of excluded technology is not meant to be exhaustive. As we noted in our Preliminary Analysis Memo, as well as a memo issued on July 21, 2020, it may be beneficial to know which surveillance technology is currently being used by City departments before determining which types of technology should be excluded. Responses to this Office's July 21, 2020 memo should aid the Council's review. Among the types of technology the Council may wish to discuss are:

      i. **Drone Video Cameras and Use of Surveillance Technology for Exigent Circumstances or Large-Scale Events.** At the July 15 PS&LN Committee meeting, Councilmember Cate asked whether the Fire-Rescue Department would be able to use drone technology for an emergency if that technology had not been previously approved by the Council under the Surveillance Ordinance. The Surveillance Ordinance now contains an exception for exigent circumstances as defined under section 511.0101(g). Other cities, such as Oakland, have provisions that allow the temporary use of unapproved surveillance technology for exigent circumstances and large-scale events.

      ii. **Surveillance Technology for Monitoring City Employees.** The City uses technology such as GPS sensors to monitor the location and speed of City fleet vehicles. This is intended to ensure that City employees are properly performing their work duties and following traffic laws.

Like Seattle's ordinance, the Surveillance Ordinance now contains language that excludes surveillance technology used solely to monitor and conduct internal investigations involving City employees, contractors, and volunteers. Section 511.0101(m)(1)(K).

iii. **Routine Office Hardware.** Routine office hardware, such as credit card machines and badge readers, are excluded under Section 511.0101(m)(A) only if they will not be used for surveillance or law enforcement functions. An understanding of the Council's intent, and a definition of "law enforcement function," will help the Office analyze this provision. Routine office hardware may be used to assist law enforcement functions when there is a break-in at a City facility or financial fraud is committed in paying the City. Telephones or other routine office hardware may be used to locate or speak with witnesses in criminal cases. The San Francisco surveillance ordinance exempts office hardware commonly used by city departments for routine city business and transactions without the caveat that it not be used for surveillance or law enforcement functions.

iv. **Digital Cameras, Audio Recorders, and Video Recorders.** Digital cameras and audio and video recorders are excluded under Section 511.0101(m)(C) from the definition of surveillance technology, but only if they are not designed to be used "surreptitiously." It would be beneficial to receive policy guidance on how to define what should and should not be considered "surreptitious."

v. **Parking Ticket Devices.** "Parking Ticket Devices" are an excluded technology under Section 511.0101(m)(B). The term was clarified to include all devices used solely for parking enforcement-related purposes, including any sensors that detect if cars are parked in a parking space.

vi. **Medical Equipment.** "Medical equipment used to diagnose, treat, or prevent disease or injury" are excluded under the definition of "surveillance technology" set forth in Section 511.0101(m)(G). The language was clarified to ensure that such equipment was only exempt to the extent that it is used for medical purposes.

vii. **City Department Case Management Systems.** This language originally stated that police department case management systems were exempt, but it has been revised

to include City department case management systems because numerous City departments use case management systems.

viii. **Use of surveillance technology authorized by court order.** Council may want to consider whether to exempt the use of technology that is already subject to statutory and/or judicial oversight. The surveillance ordinance in Nashville has such a provision.

ix. **Additional Technologies.** Systems, software, databases, and data sources used for City revenue by the City Treasurer are now exempt, provided that no information from these sources is shared by the City Treasurer except as part of efforts to collect revenue owed to the City. However, IT security systems such as firewalls intended to secure City data from hackers or City databases for human resources, permit, or other purposes, could constitute "surveillance technology" under the Surveillance Ordinance. If this is not the Council's intent, exemption categories should be created for this type of technology as was done in San Francisco, Davis, Berkeley, and the BART District. San Francisco, Davis, and the BART District also include an exemption for the use of police department computer aided dispatch (CAD), LiveScan, booking, Department of Motor Vehicles (DMV), California Law Enforcement Telecommunications Systems (CLETS), 911 and related dispatch and operation or emergency services systems. Additionally, Section 2(3)(a)(7) of the BART District ordinance excludes "equipment designed to detect the presence of/or identify the source of chemical, biological, radiological, nuclear, or explosive materials." Input from impacted City departments may aid Council's discussion.

4. **Issues Related to Surveillance Impact Reports.** Section 511.0101(n) requires that a Surveillance Impact Report be submitted to the Privacy Advisory Board (Board) and the Council. This report will include information about the location of surveillance technology, the security of the data obtained from its use, and whether the surveillance technology was used or deployed in a discriminatory manner.

   a. With regard to "Location" and "Data Security" under Sections 511.0101(n)(3) and (n)(7), the Council may wish to hear from the IT Department and affected City departments regarding what level of information would raise their concerns for compromising security. For example, security cameras monitor critical City infrastructure and the City takes certain actions to thwart data breaches. Section

511.0107(n)(3) indicates that this information should be generally described. Language was added to Sections 511.0101(n)(6) and (n)(7) to allow City staff to not disclose information that would violate any applicable law or undermine the City's legitimate security interests.

b. With regard to "Impact" and "Public engagement and comments" under Sections 511.0101(n)(4) and (n)(12), a requirement was added that the City identify impacts on different segments of the population in place of the prior wording, which required analysis that would have resulted in legal conclusions.

5. Surveillance Use Policy. Prior to approving the use of any surveillance technology as defined, City departments must bring forward a surveillance use policy pursuant to Section 511.0101(o) that details the purpose of such technology, its authorized use, as well as rules on data collection, data access, and data protection.

a. Authorized Use, Data Collection, Data Protection, and Data Access. Under Sections 511.0101(o)(2), (o)(3), (o)(4), and (o)(5), the Surveillance Ordinance requires public reporting of authorized use, data collection, data access, and data protection as it pertains to particular surveillance technology. While the ordinances of Oakland, Davis, Berkeley, and the BART District have some language related to these categories, it is not as broad as the language in the Surveillance Ordinance. To address City IT concerns regarding controls being circumvented if the information were contained in a public report, these provisions now contain language that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the City's legitimate security interests. This is similar to language in Section 6(1) of the BART District's ordinance, which includes a provision that indicates that a Surveillance Use Policy "shall be made in a manner that is informative, but that will not undermine the District's legitimate security interests."

b. Complaints. Based on direction provided by the Councilmember's office, the provision related to community complaint procedures was removed from the Surveillance Ordinance.

6. Issues Related to Board Notification and Review Requirements.

a. Board Review of Information Provided by Surveillance Technology. As noted in our Preliminary Analysis Memo, Oakland's ordinance does not require the Board to be notified or to vet *information provided* by surveillance technology; however, this would be required under the proposed Surveillance Ordinance because the definition of surveillance technology includes the "product of" surveillance technology. Given that other jurisdictions do not define surveillance technology to broadly include the "product of" the technology itself, the effect of this language is unclear. All sorts of data can be gathered from surveillance technology, including, for example, lists of names of people who entered a particular City building. If a City department was to seek access to this list of

names, it is unclear whether it would need Council approval. In addition, the Board has 90 calendar days to approve, reject, or remain neutral concerning a request to obtain surveillance technology. The Council may wish to consider a lesser period of time to avoid a backlog of requests and operational impacts on requesting departments.

b. **Procedure after Board Objects to the City Department's Proposal on Use of Surveillance Technology.** Section 511.0102(c) clarifies that the Board cannot prevent Council from hearing a proposal for the use, acquisition or funding of surveillance technology by a City department. The reason is that the Council cannot delegate its legislative authority under San Diego Charter section 11 and committees created under Charter section 43, such as the Board, are advisory only. Therefore, City staff may proceed to Council regardless of the Board's action regarding the proposed use of surveillance technology, but City staff must present to Council the result of the Board's review, including any objections to the proposed use.

c. **Community Meetings.** Section 511.0102(e)(2) now requires that City departments conduct one or more community meetings in each Council district where proposed surveillance technology will be deployed, with opportunity for public comment and written response, before going to the Council for approval of new or existing surveillance technology. The prior language required nine separate community meetings—one in each Council district regardless of whether the surveillance technology was deployed in that Council district—before a City department could proceed to the Board or Council. Based on our review of similar ordinances, this requirement appears to be unique to the Surveillance Ordinance. As noted in our Preliminary Analysis Memo, the Council may wish to discuss how to best achieve the goal of robust public engagement at a time when most public hearings are conducted virtually rather than in person. Further, this requirement may require the addition of positions, and if so, should be reviewed by the Independent Budget Analyst per the Municipal Code.

d. **Board Authority to Rank Items in Order of Potential Impact on Civil Liberties.** Section 511.0102(f) requires City staff to present a list of surveillance technology possessed or used by the City and authorizes the Board to rank the items in order of potential impact to civil liberties to provide a recommended sequence of items to be heard at Board meetings. This section of the Surveillance Ordinance also requires that City staff present at least one surveillance impact report and one surveillance use policy to the Board per month generally beginning with the highest-ranking items as determined by the Board. Language was added to clarify that the rankings are recommendations to address a scenario in which a City department needs to bring forward surveillance technology that is critical to its operational needs, but is ranked low by the Board for its potential impact on civil liberties. Pursuant to Charter sections 11 and 43, the Board performs an advisory-only function and cannot foreclose the Council from hearing a request by City staff for approval of the use of surveillance technology. The language that

has been added to this provision requires the Board to consider the operational importance of the surveillance technology in determining the ranking. Although City staff should submit proposals for the highest-ranking items, as the need arises, City staff may also submit additional proposed uses of surveillance technology for review to the Board so that such matters to be heard in a timely manner.

7. **Council Approval Requirements for New and Existing Surveillance Technology.** Section 511.0103 requires Council approval prior to the City's use of existing or new surveillance technology.

    a. **One-Year Grace Period for Continued Use of Existing Surveillance Technology.** Section 511.0109 has been added to provide a one-year grace period for the continued use of existing surveillance technology to allow the Board to be populated and for City staff to have an opportunity to identify the affected surveillance technology and to draft the required reports to seek Board review and Council approval. City management should be consulted to see if this grace period is sufficient to address operational concerns. As a side note, when the Surveillance Ordinance is adopted, it would be helpful to include in Council's motion the date upon which the grace period begins.

    b. **Provisions to Help Ensure that Appropriate Law Enforcement Functions Will Not Be Unduly Impacted.** Language has been added to the Surveillance Ordinance that provides some flexibility for City operational concerns, such as exigent circumstances, but the Council may want to consider language to ensure that appropriate law enforcement functions are not compromised. The type of language that has been added to the Surveillance Ordinance is as follows:

        i. **Allowing Temporary Use of Unapproved Technology During Exigent Circumstances.** Similar to other jurisdictions, Section 511.0104 will allow City staff to temporarily acquire and use in exigent circumstances surveillance technology that has not been previously approved by the Council in accordance with the provisions of the Surveillance Ordinance. After the exigent circumstances cease, City staff is required to provide a written report on the use of the surveillance technology and discuss such use at the next available Board meeting. Also, City staff must return the surveillance technology within 30 days of when the exigent circumstances end unless City staff initiates the process for approval consistent with the Surveillance Ordinance.

ii. **Compliance with City Charter and Applicable State Law.** Section 511.0110 has been added to clarify that nothing in the Surveillance Ordinance is intended to violate any provision of the City Charter or applicable state law and that any interpretation of any provision of the Surveillance Ordinance will be consistent with the City Charter and applicable state law.

As noted in our Preliminary Analysis Memo, surveillance ordinances of various other jurisdictions include provisions that provide some degree of flexibility to address threats to public health and safety. These include:

i. **Allowing Others to Provide Evidence or Information from Surveillance Technology to Be Used for Criminal Investigation Purposes.** Chapter 9.64.030(1)(E) of Oakland's ordinance has a provision clarifying that it does not "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." This provision, for example, would allow the public to provide security camera video footage to the San Diego Police Department (SDPD) to help solve crimes.

ii. **Exempting Law Enforcement When Performing Their Investigative or Prosecutorial Functions.** Charter section 57 provides the Chief of Police with authority over SDPD property and equipment and with all power and authority necessary for the operation and control of the SDPD. Other City departments also have charter-mandated duties, such as the City Attorney under Charter section 40 and the Fire Chief under Charter section 58. As discussed under Paragraph 11 of our Preliminary Analysis Memo, the Surveillance Ordinance cannot violate any Charter provision. To expressly avoid potential conflicts with the Charter-mandated duties of City departments, the Council and Mayor may want to consider the examples of San Francisco and Santa Clara, which exempt the District Attorney and Sheriff from the requirements of their respective surveillance ordinances when performing their investigative or prosecutorial functions. Those jurisdictions require that the District Attorney or Sheriff provide an explanation in writing of how compliance with their respective surveillance ordinance would obstruct their investigative or prosecutorial function.

iii. **Exempting a City Department's Use of Surveillance Technology to Conduct Internal Investigations or in Civil and Administrative Proceedings.** To avoid interfering with required municipal operations, Section 19B.2(1) of the San Francisco ordinance states that nothing in its Chapter 19B provisions "shall prohibit, restrict, or interfere with a Department's use of Surveillance Technology to conduct internal investigations involving City employees, contractors, and volunteers, or the City Attorney's ability to receive or use, in preparation for or in civil or administrative proceedings, information from Surveillance Technology . . . that any City agency, department, or official gathers or that any other non-City entity or person gathers."

8. **Oversight Following Council Approval.** Section 511.0105 requires that City staff annually obtain re-approval of surveillance technology that is used by the City. The Council may wish to consider whether it wants every surveillance technology to be brought forth for re-approval every year or to allow some flexibility in this regard as determined by the Council.

9. **Enforcement of Ordinance Violations.** Section 511.0106 provides a variety of remedies for violations of its provisions. Given the potential fiscal impacts to the City, the Independent Budget Analyst should review these provisions per the Municipal Code.

   a. **Private Right of Action.** Section 511.0106(a)(1) allows a private party to sue the City to enforce its provisions. As noted in our Preliminary Analysis Memo, while it is important to ensure that the provisions of the ordinance are enforced, the Council and the Mayor's office may want to consider placing conditions on this private right of action as other jurisdictions have done. See, for example, Santa Clara County, Berkeley, Seattle, the BART District, San Francisco, and Davis, which do so by requiring service of anywhere between 30 to 90 days advance written notice of any alleged violation to give them an opportunity to investigate and to cure the violation. In addition, the right to sue should attach to material violations, and not technicalities, to prevent abuse and protect the City's general fund.

   b. **Damages, Costs and Attorney Fees Awarded.** Section 511.0106(a)(2) allow an award of actual damages but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater, as well as the award of costs and reasonable attorney fees to a plaintiff who is a prevailing party. Santa Clara County limits the award of attorney fees for violations by capping it at $100 per hour, but not to exceed $7,500 in total. For a recovery of attorney fees, Santa

Clara County also requires that any violation of the Surveillance Ordinance be the result of arbitrary or capricious action or conduct of Santa Clara County employees. Berkeley also includes prior written notice before a lawsuit can be brought, and caps attorney fees at $15,000.

c. **Removal of Express Consequences to City Employees Found in Violation.** Language has been removed from the Surveillance Ordinance that would expressly subject City employees to discipline for violations. The practical effect is that even without an express provision, City employees may still be subject to discipline due to a violation of the Surveillance Ordinance. Due to the obligations imposed on City staff, the City may need to meet-and-confer with the recognized City employee organizations prior to approval of the Surveillance Ordinance.

10. **Contracts for Surveillance Technology.** The Surveillance Ordinance makes it unlawful for the City to enter into any surveillance-related contract or agreement that conflicts with its provisions and deems any provisions in any contract that conflicts with the ordinance including non-disclosure agreements to be deemed void and legally unenforceable. Given that it is legally problematic to invalidate existing contracts or contractual provisions because the City could be liable for breach of contract and resulting damages and attorney fees, language was added to the Surveillance Ordinance to clarify that this provision is only applicable to contracts or other agreements for surveillance technology entered into after the effective date of the Surveillance Ordinance. Additional language was included to make it clear that any amendment or exercise of any option to any contract after the effective date of the Surveillance Ordinance would require City staff to comply with the provisions of the Surveillance Ordinance.

11. **Conflicts with City Charter and Meet-and-Confer.** As discussed above in paragraph 7(b)(ii), the Surveillance Ordinance must be interpreted in a manner that does not prevent a City department from fulfilling its Charter-mandated responsibilities. Further, given that the City's Human Resources Department has determined that meet-and-confer is necessary, the most expeditious way to proceed with the Surveillance Ordinance is to agendize a Council meeting to allow the Council to finalize the language in the Surveillance Ordinance so that meet-and-confer can occur. Once meet-and-confer is completed, this Office could incorporate any revisions to the Surveillance Ordinance that arise from meet-and-confer. If the Council meeting to finalize the language of the Surveillance Ordinance includes Council approval of the introduction of the ordinance, the Surveillance Ordinance may need to be re-introduced at City Council depending on the extent of the changes to the ordinance arising from meet-and-confer discussions.

CONCLUSION

Although the language of the Surveillance Ordinance was revised to clarify its provisions, there are still provisions in the Surveillance Ordinance that would benefit from further discussion, clarification, and possible revision. We look forward to receiving further guidance and input from the Council, City staff, and the public.

MARA W. ELLIOTT, CITY ATTORNEY

By */s/ Kenneth R. So*
Kenneth R. So
Deputy City Attorney

KRS:cm
RC-2020-6
Doc. No. 2516195
Attachments
cc: Aimee Faucett, Chief of Staff, Mayor's Office and Interim Chief Operating Officer
Jeff Sturak, Assistant Chief Operating Officer
Jonathan Behnke, Chief Information Officer
Andrea Tevlin, Independent Budget Analyst
Douglas Edwards, Personnel Director
Kyle Elser, Interim City Auditor
Stacey Fulhorst, Ethics Commission Director
Elizabeth Maland, City Clerk
Abby Jarl-Veltz, Assistant Director, Human Resources

Office of
The City Attorney
City of San Diego

MEMORANDUM
MS 59

(619) 236-6220

DATE: September 3, 2020

TO: Honorable Mayor and Members of the Council

FROM: City Attorney

SUBJECT: Preliminary Analysis of Draft Transparent and Responsible Use of Surveillance Technology Ordinance

---

INTRODUCTION

On January 29, 2020, the City of San Diego's Sustainability Department introduced to the Public Safety & Livable Neighborhoods Committee (PS&LN Committee) a draft Council policy on Streetlight Sensor Data Use for consideration and adoption. The PS&LN Committee unanimously voted to reject the proposed policy and to instead move forward with a more comprehensive framework to address the City's use of surveillance technology. This approach was based in part on concerns about the potential for surveillance technology to invade privacy and discriminate against certain individuals or groups. In addition, PS&LN Committee members and public speakers identified a need for the Council policy to cover new and evolving surveillance technologies.

On July 15, 2020, the PS&LN Committee heard a presentation from the TRUST SD Coalition, which wrote the draft Transparent and Responsible Use of Surveillance Technology Ordinance (Surveillance Ordinance) and a draft ordinance establishing a Privacy Advisory Commission (PAC) that would provide recommendations to the City Council (Council) on the use of surveillance technology. The PS&LN Committee asked this Office to provide legal review in advance of Council consideration of each ordinance. This memorandum provides a preliminary analysis of the Surveillance Ordinance.

On July 21, 2020, two memoranda were separately issued concerning the Surveillance Ordinance. The first memorandum was issued by this Office and requested that the Mayor's Office and independent City departments provide information on all surveillance technology now in use to inform our legal analysis of the Surveillance Ordinance. The second memorandum was issued by PS&LN Committee member Councilmember Chris Cate (Cate Memo) to PS&LN Committee Chair Councilmember Monica Montgomery. The Cate Memo sought clarification on

various provisions of the Surveillance Ordinance and asked additional questions. The majority of issues raised by the Cate Memo require additional input from policy makers such as the Council, the Mayor, and City departments. This input has not yet been received and is not considered in this preliminary analysis.

The Office's goal in reviewing the Surveillance Ordinance is to highlight policy issues for discussion by the Council, City departments, and the public that will further the PS&LN Committee's goal of providing oversight of surveillance technology while protecting public health and safety. In addition, to the extent possible, this memorandum clarifies and addresses issues raised in the Cate Memo.

PRELIMINARY ANALYSIS

While largely modeled after an Oakland ordinance that establishes rules for that city's acquisition and use of surveillance equipment, the Surveillance Ordinance contains additional requirements that the Oakland ordinance does not. This memorandum will highlight differences between the Surveillance Ordinance and the Oakland ordinance to provide context on various issues. It will also reference provisions of the surveillance ordinances of the cities of Berkeley, Davis, San Francisco, Seattle, as well as Santa Clara County, and the Bay Area Rapid Transit (BART) District that may inform Council discussion.

At this juncture, a number of provisions of the Surveillance Ordinance require additional policy direction from the Council and input from the Mayor's Office and affected City departments. This policy direction will allow this Office to fully complete the legal review and finalize the draft language for the Surveillance Ordinance.

For ease of reference, issues identified thus far are addressed in roughly the order in which they appear in the Surveillance Ordinance:

1. **Issues Related to the Annual Surveillance Report**

    a. **Requirement to Report Sharing of Data with Internal Entities.** Section 1(2)(B) sets forth the requirement that the Annual Surveillance Report includes whether and how often data acquired through the use of surveillance technology was shared with internal or external entities. In our review, this requirement is unique to the Surveillance Ordinance. Ordinances in jurisdictions such as Oakland, San Francisco, Davis, and the BART District impose similar requirements only on sharing data with outside entities.

    b. **Requirement of the Annual Surveillance Report to Identify the Race of Each Individual Captured by Surveillance Technology.** Section 1(2)(F) of the Surveillance Ordinance sets forth the requirement in the Annual Surveillance Report that the analysis "shall identify the race of each person that was subject to the technology's use." In our review, this requirement is unique to the Surveillance Ordinance, and expands surveillance operations beyond their current

scope. For example, identifying the race of every individual captured by every camera would require City staff to continuously monitor and review surveillance camera footage to identify the race of any and all individuals picked up by the camera, a process that could lead to concerns about racial profiling. The City currently does not have staff that continuously monitors all of its surveillance cameras, or staff trained in using surveillance technology for the purpose of racial identification. Per the San Diego Municipal Code (Municipal Code), this requirement should be analyzed and reviewed by City management and the Independent Budget Analyst to determine the fiscal impact to the City and whether additional positions will need to be created to address this requirement. Further research after policy direction has been provided on the proposed use of this racial identification data is also needed to ensure that the City's identification processes do not lead to claims of unlawful profiling or discrimination.

c. Requirement of the Annual Surveillance Report to Include System Access and Data Breach Information. The Annual Surveillance Report also includes reporting provisions that in our review are unique to the Surveillance Ordinance including the following:

i. "A list of any software updates, hardware upgrades, or system configuration changes accompanied by a description of altered or improved functionality that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change." Section 1(2)(D).

ii. "Description of all methodologies used to detect incidents of data breaches or unauthorized access;" Section 1(2)(I).

Input from the City's Information Technology (IT) Department will help the City determine if the inclusion of the information noted in Sections 1(2)(D) and (I) of the Surveillance Ordinance is of a detail that could pose potential threats and vulnerabilities to the City's IT security.

d. Requirements of the Annual Surveillance Report That Need Clarification. The Annual Surveillance Report also includes provisions that are unclear, including the following:

i. Under Section 1(2)(G), there is a reference to "confidential personnel file information" that cannot legally be included in the Annual Surveillance Report and a requirement for reporting each "omission and its cause." This requirement is unique to the Surveillance Ordinance. Since personnel file information is confidential by law, it is not clear what can be reported. In addition, the Cate Memo sought

clarification of who would field and review community complaints or concerns about surveillance technology and whether there are adequate protections of civil rights and liberties.

ii. Under Section 1(2)(K), there is a reference to including the "response rates" of statistics and information about Public Records Act requests regarding the relevant subject surveillance technology. The term "response rates" should be defined. Input from the City's Communications Department may be helpful in establishing how responses are tracked on NextRequest.

2. **Various Definitions Could Use Clarification.** It is unclear whether the definition of "City" is intended is to include all City departments or only those specifically mentioned in the San Diego Charter (Charter). It is also unclear whether it is meant to include wholly-owned City entities like the San Diego Housing Commission. Likewise, the definition of "City staff" under Section 1(4) of the Surveillance Ordinance should be drafted consistently with the definition of "City" because currently it refers to City personnel under the City Administrator, which this Office understands to mean the City Manager or Mayor, thereby excluding independent City departments.

   Some portions of the definition of "surveillance" or "surveil" under Section 1(9) of the Surveillance Ordinance are included in the Oakland ordinance, but there is different language elsewhere that defines what is meant by the term "individuals." The Oakland ordinance states that "[i]ndividuals include those whose identity can be revealed by license plate data when combined with any other record." In contrast, the Surveillance Ordinance under Section 1(9) states that "[i]ndividuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user ids, unique digital identifier, or data traces left by the individual." The Surveillance Ordinance's definition appears broader, but the practical effect is unclear to us. We recommend having the City's IT Department and other impacted City staff review this language. Besides Oakland, the city of Seattle is the only other jurisdiction that defined "surveillance" or "surveil." Chapter 14.18.010 of the Seattle ordinance provides additional clarification stating that "[i]t is not surveillance if an individual knowingly and voluntarily consented to provide the information, or had a clear and conspicuous opportunity to opt out of providing the information."

3. **Issues Related to the Definition of "Surveillance Technology."** The definition of "Surveillance technology" under Section 1(10) of the Surveillance Ordinance is ambiguous and should be clarified. To address a question raised in the Cate Memo, the definition of "Surveillance technology" applies to all City departments and entities captured under the definition of "City" in Section 1(3) of the Surveillance Ordinance, not just the San Diego Police Department (SDPD).

a. **Included Surveillance Technology.** Under Section 1(10), the definition of "Surveillance technology" includes the "product (e.g. audiovisual recording, data, analysis, report) of such surveillance technology." In our review, this definition is unique to the Surveillance Ordinance. Elsewhere in the Surveillance Ordinance, other language is used that distinguishes between the actual technology and the data or information produced from the technology. In crafting a durable policy that anticipates new and emerging surveillance technology, it may be more efficient to keep the distinction clear and, where applicable, reference both technology and information. Section 1(10) also includes language referencing examples of what is meant by software such as "scripts, code, Application Programming Interfaces." The City's IT Department can advise whether such references are inclusive and consistent with what is understood to be software.

b. **Excluded Surveillance Technology.** The definition of "Surveillance technology" sets forth a list of technology under Section 1(10)(A) that is not considered "surveillance technology" for purposes of the Surveillance Ordinance. The listed technologies are those excluded by other jurisdictions. It may be beneficial to know which surveillance technology is currently being used by City departments before determining which types of technology should be excluded. Responses to this Office's July 21, 2020 memo should aid the Council's review. Among the types of technology the Council may wish to discuss are:

    i. **Drone Video Cameras and Use of Surveillance Technology for Exigent Circumstances or Large-Scale Events.** At the July 15 PS&LN Committee meeting, Councilmember Cate asked whether the Fire-Rescue Department would be able to use drone technology for an emergency if that technology had not been previously approved by the Council under the Surveillance Ordinance. The Surveillance Ordinance currently contains no exception for exigent circumstances. Other cities such as Oakland have provisions that allow the temporary use of unapproved surveillance technology for exigent circumstances and large-scale events.

    ii. **Surveillance Technology for Monitoring City Employees.** The City uses technology such as GPS sensors to monitor the location and speed of City fleet vehicles. This is intended to ensure that City employees are properly performing their work duties and following traffic laws. Seattle's ordinance excludes technology used to monitor its employees, contractors, and volunteers. The Surveillance Ordinance does not.

iii. **Routine Office Hardware.** Routine office hardware such as credit card machines and badge readers are excluded under Section 1(10)(A)(1) of the Surveillance Ordinance only if they will not be used for surveillance or law enforcement functions. An understanding of the Council's intent, and a definition of "law enforcement function," will help the Office analyze this provision. Routine office hardware may be used to assist law enforcement functions when there is a break-in at a City facility or financial fraud is committed in paying the City. Telephones or other routine office hardware may be used to locate or speak with witnesses in criminal cases. The San Francisco surveillance ordinance exempts office hardware commonly used by city departments for routine city business and transactions without the caveat in the Surveillance Ordinance.

iv. **Digital Cameras, Audio Recorders, and Video Recorders.** Digital cameras and audio and video recorders are excluded under Section 1(10)(A)(3) of the Surveillance Ordinance from the definition of surveillance technology, but only if they are not designed to be used surreptitiously. It would be beneficial to receive policy guidance on how to define what should and should not be considered surreptitious.

v. **Parking Ticket Devices.** "Parking Ticket Devices" are an excluded technology under Section 1(10)(A)(2) of the Surveillance Ordinance. The term should be defined with input from the Treasurer, the SDPD, and other involved departments if the intent is to exclude every or only certain technology that is used for parking enforcement-related purposes, such as sensors that detect if cars are parked in a parking space.

vi. **Medical Equipment.** "Medical equipment used to diagnose, treat, or prevent disease or injury" are excluded under the definition of "surveillance technology" set forth in Section 1(10)(A)(7) of the Surveillance Ordinance, unless the equipment "generates information that can be used to identify individuals." In our review, the requirement is unique to the Surveillance Ordinance. The Council may wish to consider whether the need for prior approval of medical equipment by the Council under this ordinance could hamper efforts to diagnose and treat people in emergency situations or other health situations.

vii. **Additional Technologies.** IT security systems such as firewalls intended to secure City data from hackers or City databases for payroll, human resources, permit, accounting, or fiscal purposes, could constitute "surveillance technology" under the Surveillance Ordinance. If this is not the Council's intent, exemption categories should be created for this type of technology as was done in San Francisco, Davis, Berkeley, and the BART District. San Francisco, Davis, and the BART District also include an exemption for the use of police department computer aided dispatch (CAD), LiveScan, booking, Department of Motor Vehicles (DMV), California Law Enforcement Telecommunications Systems (CLETS), 911 and related dispatch and operation or emergency services systems. Additionally, Section 2(3)(a)(7) of the BART District ordinance excludes "equipment designed to detect the presence of/or identify the source of chemical, biological, radiological, nuclear, or explosive materials." Input from impacted City departments may aid Council's discussion.

4. **Issues Related to Surveillance Impact Reports.** Section 1(12) of the Surveillance Ordinance requires that a Surveillance Impact Report be submitted to the PAC and the Council. Among other things, this report will have information about the location of surveillance technology and the security of the data obtained from its use. This report will also include information on whether the surveillance technology was used or deployed in a discriminatory manner.

   a. With regard to "Location" and "Data Security" under Sections 1(12)(C) and (G) of the Surveillance Ordinance, the Council may wish to hear from the IT Department and affected City departments regarding what level of information would raise their concerns for comprising security. For example, security cameras monitor critical City infrastructure and the City takes certain actions to thwart data breaches.

   b. With regard to "Impact" and "Public engagement and comments" under Sections 1(12)(D) and (L) of the Surveillance Ordinance, using the legal terms "disparate impact" and "viewpoint-based" in public reports may create liability to the City if there are findings of disparate impacts or viewpoint-based discrimination. There may be alternative yet informative ways of reporting this data.

5. **Issues Related to the Requirements for Completing a Surveillance Use Policy.** Prior to approving the use of any surveillance technology as defined, City departments must bring forward a surveillance use policy pursuant to Section 1(13) of the Surveillance Ordinance that details the purpose of such technology, its authorized use, as well as rules

   on data collection, data access, and data protection. It also includes a requirement to detail a complaint procedure so the public can register complaints or concerns as well as submit questions about the use of a specific surveillance technology.

   a. **Authorized Use.** As it pertains to authorized use under Section 1(13)(B), the Surveillance Ordinance requires a description of "[t]he specific uses that are authorized, the rules and processes required prior to such use, as well as a description of controls used to prevent or detect circumvention of those rules and processes." While the ordinances of Oakland, Davis, Berkeley, and the BART District do require a description of authorized use, they do not require "a description of controls used to prevent or detect circumvention of those rules and processes." The Council may wish to hear from the IT Department and affected City departments about how controls can be circumvented if the information were contained in a public report.

   b. **Data Collection.** Under Section 1(13)(C), the Surveillance Ordinance requires reporting on "[t]he information that can be collected, captured, recorded, intercepted or retained by the surveillance technology, as well as data that might be inadvertently collected during the authorized uses of the surveillance technology and what measures will be taken to minimize and delete such data." This provision is broader than the data collection provisions in the ordinances of Oakland, Davis, Berkeley, and the BART District. The Council may wish to hear from the IT Department and affected City departments whether there could be any unintended consequences from requiring this information to be reported in the policy.

   c. **Data Access and Data Protection.** Under Sections 1(13)(D) and (E), the Surveillance Ordinance requires "a description of controls used to prevent or detect circumvention of rules and processes" related to data access as well as "[t]he safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms" related to data protection. While the ordinances of Oakland, Davis, Berkeley, and the BART District include provisions for data access and data protection, they do not include a requirement to disclose a description of controls used to prevent or detect circumvention of rules and processes and the Office did not find any such provision in any other ordinance reviewed. In addition, Section 6(1) of the BART

District's ordinance includes a provision that indicates that a Surveillance Use Policy "shall be made in a manner that is informative, but that will not undermine the District's legitimate security interests." The City's IT Department should provide input because it may have a security concern with publicly divulging this information.

d. Complaints. The Surveillance Ordinance under Section 1(13)(L) requires that there be procedures put in place to allow the public to register complaints or concerns or to submit questions about the deployment or use of specific surveillance technology along with how it will be ensured that each question and complaint is responded to in a timely manner. In our review, this requirement is unique to the Surveillance Ordinance. Per the Municipal Code, this requirement should be analyzed and reviewed by City management and the Independent Budget Analyst to determine the fiscal impact to the City and whether additional positions will need to be created to address this requirement.

6. **Issues Related to PAC Notification and Review Requirements.** The provisions under Section 2 of the Surveillance Ordinance require that City departments allow the PAC to vet the proposed use and associated use policy of existing or new surveillance technology prior to Council review. The proposed language under Section 2(1)(A) states in relevant part: "City staff shall notify the Chair of the Privacy Advisory Commission prior to: 1. Seeking or soliciting funds for surveillance technology or the information it provides . . . 3. Otherwise, formally or informally, facilitating or implementing surveillance technology in collaboration with other entities, including city entities." The Cate Memo requests that the Surveillance Ordinance clarify how individual departments notify the Chair of the PAC prior to solicitation of City funds and proposals for surveillance technology. In particular, the Cate Memo asks whether individual departments need to go through a single point-of-contact or department to handle these requests.

   a. PAC Review of Information Provided by Surveillance Technology. While Oakland's ordinance has a PAC, it does not require the PAC to be notified or to vet information provided by surveillance technology as is required under Section 2(1)(A)(1) and (2) of the Surveillance Ordinance. In fact, by calling out the information from surveillance technology specifically, it conflicts with the definition of surveillance technology, which already includes the product of surveillance technology. Inclusion of this language regarding "or the information it provides" also makes the requirements of the ordinance vague as to when the PAC must be notified. For example, there are all sorts of data that can be gathered from surveillance technology such as lists of names of person who entered a particular City building. If a City department was to seek access to this list of names, it is unclear whether it would need Council approval.

b. PAC Review of Facilitating or Implementing Surveillance Technology. It is unclear what is meant by "facilitating" surveillance technology or the term "city entities" as those terms are used in Section 2(1)(A)(3) of the Surveillance Ordinance. The Cate Memo requests clarification that "other entities" include other municipalities and governmental organizations and that "city entities" means the various City departments and divisions within the City of San Diego. Oakland's ordinance does not have the language in sub-paragraph 3 at all.

c. Procedure after PAC Objects to the City Department's Proposal on Use of Surveillance Technology. Section 2(C) of the Surveillance Ordinance allows City staff to proceed and seek Council approval of the proposed use of surveillance technology if the PAC does not make a recommendation. The Cate Memo seeks clarification as to what would happen if the PAC recommends against the City department proposal. Similarly, the Cate Memo seeks clarification on Section 2(2)(B) of the Surveillance Ordinance related to what City staff shall present to Council as it relates to PAC modifications and whether City staff can object to recommendations made by the PAC regarding surveillance use policies. The Surveillance Ordinance should clarify that the PAC cannot prevent a City department from proceeding to Council, as the Council cannot delegate its legislative authority under Charter section 11 and committees created under Charter section 43 such as the PAC are advisory only.

The Cate Memo further asks if the Surveillance Ordinance conflicts with the Mayor's existing authority to enter into contracts under a certain dollar amount. The Surveillance Ordinance does not conflict with that authority. Rather, it carves out a subset of contracts that involve surveillance technology that would be subject to Council approval rather than Mayoral approval and a framework for the PAC to provide recommendations to the Council.

d. Community Meetings. Under Sections 2(2)(A) and 2(3)(A), the Surveillance Ordinance requires that City departments complete one or more community meetings in each Council district with opportunity for public comment and written response before going to the Council for approval of new or existing surveillance technology. Essentially, this requirement would require nine separate community meetings before a City department could proceed to the PAC or Council. In our review, this requirement is unique to the Surveillance Ordinance. The Council may wish to discuss how to best achieve the goal of robust public engagement at a time when most public hearings are conducted online rather than in person. Further, this requirement may require the addition of positions and if so, should be reviewed by the Independent Budget Analyst per the Municipal Code.

e. **PAC Authority to Rank Items in Order of Potential Impact on Civil Liberties.** Section 2(3)(C) of the Surveillance Ordinance requires City staff to present a list of surveillance technology possessed or used by the City and authorizes the PAC to rank the items in order of potential impact to civil liberties. The Cate Memo requests clarification on the PAC's ranking system. This section of the Surveillance Ordinance also requires that City staff present at least one surveillance impact report and one surveillance use policy to the PAC per month beginning with the highest-ranking items as determined by the PAC. The Council may wish to address the potential for conflicts when City departments need to bring forward surveillance technology that are critical to the operational needs of City departments, but are ranked low by the PAC for their potential impact on civil liberties.

7. **Council Approval Requirements for New and Existing Surveillance Technology.** The Surveillance Ordinance requires Council approval prior to the City's use of existing or new surveillance technology.

   a. **No Grace Period for Continued Use of Existing Surveillance Technology.** As noted in the Cate Memo, Section 3(1)(A) of the Surveillance Ordinance would require all City departments to cease using existing surveillance technology until Council approval is obtained. There is no grace period or opportunity for City staff to accelerate the review process or to utilize surveillance technology without first going before the PAC and the Council. The ACLU's model surveillance technology ordinance upon which this Surveillance Ordinance was in part based recommends including a grace period of 90 days following the effective date of the ordinance. Other cities have allowed slightly longer grace periods, such as Davis, which provides 120 days, and San Francisco and Santa Clara, which provide 180 days with a possible 90-day extension. The BART District also provides for a 180-day grace period and the granting of extensions. City management should analyze the operational impacts of the immediate prohibition on the use of surveillance technology upon the ordinance's approval and recommend whether a grace period is necessary and, if so, an appropriate duration.

   b. **Requirement for Council Approval of Use of Information that Surveillance Technology Provides.** This provision under Section 3(1)(C) creates ambiguity with the proposed definition of "surveillance technology" under Section 1(10) which already includes "the product of surveillance technology." Furthermore, it is unclear what the scope of this approval entails. For example, if a City department wanted a list of names of City employees who accessed a certain City location generated from a security camera or access reader, that request for the list

of names arguably would need to be approved even though the surveillance technology itself has already been approved. In addition, the Cate Memo seeks a definition for the term "using" under Section 3(1)(C) of the Surveillance Ordinance.

c. Requirement for Council Approval for Agreements Between City Departments to Use Surveillance Technology or the Information It Provides. It is not clear whether City departments enter into agreements with each other to use or share surveillance technology and information from surveillance technology. If they do, the Surveillance Ordinance would appear to require that those agreements be approved even when the surveillance technology itself has been pre-approved by the Council in a Surveillance Use Policy that specifies authorized use and data access. In our review, this requirement is unique to the Surveillance Ordinance. Oakland's ordinance only requires agreements with non-City entities to obtain Council approval.

d. The Cate Memo Seeks Clarification of Section 3(2)(B) of the Surveillance Ordinance. This provision sets forth the standard that a determination must be made that the benefits to the community of surveillance technology outweigh the costs. The Cate Memo asked whether the Council would make this determination. From the language of the Surveillance Ordinance, it appears that it is intended that the Council make this determination.

e. The Cate Memo Would Consider Revising Section 3(2)(C) to More Clearly State the Process When the PAC Fails to Make a Recommendation. This point is similar to the concerns raised above in Paragraph 6(c) of this memorandum.

f. The Surveillance Ordinance Lacks Provisions to Help Ensure that Appropriate Law Enforcement Functions Will Not Be Unduly Impacted. Ordinances of various other jurisdictions include provisions that provide some degree of flexibility to address threats to public health and safety. These include:

i. **Allowing Others to Provide Evidence or Information from Surveillance Technology to Be Used for Criminal Investigation Purposes.** Chapter 9.64.030(1)(E) of Oakland's ordinance has a provision clarifying that it does not "prevent, restrict, or interfere with any person from 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." This provision, for example, would allow the public to provide security camera video footage to the SDPD to help solve crimes.

ii. **Allowing Temporary Use of Unapproved Technology During Exigent Circumstances or Large-Scale Events.** Recognizing that there may be logistical delay in going through the approval process and that there may be immediate threats to public health and safety that will need response, the ordinances of Oakland and a number of other jurisdictions such as San Francisco, Berkeley, Seattle, and the BART District include a provision that gives those cities the ability to temporarily use unapproved surveillance technology during exigent circumstance or large-scale events. An example raised at PS&LN Committee was the use of Fire-Rescue Department drones during a brushfire. Typically, such provisions in other jurisdictions require that the surveillance technology be used solely to respond to these circumstances and that the use must cease when the exigent circumstances or large-scale event end. They further require a report on the use of the surveillance technology at the next available PAC meeting.

iii. **Exempting Law Enforcement When Performing Their Investigative or Prosecutorial Functions.** Charter section 57 provides the Chief of Police with authority over SDPD property and equipment and with all power and authority necessary for the operation and control of the SDPD. Other City deparatments also have charter-mandated duties such as the City Attorney under Charter section 40 and the Fire Chief under Charter section 58. As discussed more fully under Paragraph 11 of this memorandum, the Surveillance Ordinance cannot violate any Charter provision. To expressly avoid potential conflicts with the Charter-mandated duties of City departments, the Council and Mayor may want to consider the examples of San Francisco and Santa Clara, which exempt the District Attorney and Sheriff from the requirements of their respective surveillance ordinances when performing their investigative or prosecutorial functions. Those jurisdictions require that the District Attorney or Sheriff provide an explanation in writing of how compliance with their respective surveillance ordinance would obstruct their investigative or prosecutorial function.

iv. **Exempting a City Department's Use of Surveillance Technology to Conduct Internal Investigations or in Civil and Administrative Proceedings.** To avoid interfering with required municipal operations, Section 19B.2(1) of the San Francisco ordinance states that nothing in its Chapter 19B provisions "shall prohibit, restrict, or interfere with a Department's use of Surveillance Technology to conduct internal investigations involving City employees, contractors, and volunteers, or the City Attorney's ability to receive or use, in preparation for or in civil or administrative proceedings, information from Surveillance Technology . . . that any City agency, department, or official gathers or that any other non-City entity or person gathers."

g. **Requirement to Post Surveillance Impact Reports and Surveillance Use Policies to the City's Website.** This requirement, set forth under Section 3(3) of the Surveillance Ordinance, makes it even more important to ensure that confidential and security-sensitive information is not included in these documents. This requirement is not found in the Oakland ordinance, but something similar is found in the ordinances of San Francisco and Seattle.

8. **Oversight Following Council Approval.** Section 4 of the Surveillance Ordinance requires that City staff follow up on an annual basis to obtain re-approval of surveillance technology that is used by the City. The Council may wish to consider whether it wants every surveillance technology to be brought forth for re-approval every year.

9. **Enforcement of Ordinance Violations.** Section 5 of the Surveillance Ordinance provides a variety of remedies for violations of its provisions. Given the potential fiscal impacts to the City, the Independent Budget Analyst should review these provisions per the Municipal Code.

   a. **Private Right of Action.** Section 5(1)(A) of the Surveillance Ordinance allows a private party to sue the City to enforce its provisions. It also includes a cause of action against a City department, but only the City of San Diego as a municipal entity has the capacity to sue or be sued. Individual City departments are not separate legal entities from the City itself and cannot be sued. While it is important to ensure that the provisions of the ordinance are enforced, the Council and the Mayor's Office may want to consider placing limitations on this private right of action as other jurisdictions have done. For example, Santa Clara County, Berkeley, Seattle, and the BART District specifically limit a private right of

action for members of the public. They do so by requiring service of 90 days advance written notice of any alleged violation to give them an opportunity to investigate and to cure the violation. San Francisco and Davis require 30 days prior written notice before a private lawsuit can be brought.

b. **Damages, Costs and Attorney's Fees Awarded.** Sections 5(1)(B) and (C) of the Surveillance Ordinance allow an award of actual damages but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater, as well as the award of costs and reasonable attorney fees to a plaintiff who is a prevailing party. Santa Clara County limits the award of attorney fees for violations that are the result of arbitrary or capricious action or conduct of Santa Clara County employees and caps such attorney fees at $100 per hour, but not to exceed $7,500 in total. Berkeley also includes prior written notice before a lawsuit can be brought, but caps attorney fees at $15,000.

c. **Consequences to City Employees Found in Violation.** Section 5(1)(D) of the Surveillance Ordinance provides that City employees can be disciplined for violations with consequences that could include retraining, suspension, or termination. To address an issue identified in the Cate Memo, the City will need to meet-and-confer with the recognized City employee organizations prior to approval of the ordinance.

10. **Secrecy of Surveillance Technology.** The Surveillance Ordinance makes it unlawful for the City to enter into any surveillance-related contract or agreement that conflicts with its provisions and deems any provisions in any existing or future contract that conflict with the ordinance including non-disclosure agreements to be deemed void and legally unenforceable. In our review, this provision is unique to the Surveillance Ordinance. It is legally problematic to invalidate existing contracts or contractual provisions because the City could be liable for breach of contract and have to pay damages and possible attorneys' fees.

11. **The Cate Memo Asks Whether the Process Outlined for Council Approval for New and Existing Surveillance Technologies Conflicts with City Charter Section 57 Relating to the SDPD and Police Authority.** Overall, the Council has the authority in its legislative capacity to enact public policy and to spend public funds under Charter sections 11 and 11.1. At the same time, the exercise of such authority through the enactment of this ordinance must be harmonized with the Charter so that any authority that the Council exercises in its legislative capacity does not impermissibly infringe on the administrative functions and Charter-mandated duties of other City officials. Overall, the Mayor is responsible for supervising "the administration of the affairs of the City." San Diego Charter § 28. As it pertains specifically to the Police Chief, Charter section 57 provides the Chief with all power and authority necessary for the operation and control of the SDPD.

An act will be characterized as legislative if it prescribes a new policy or plan; whereas it is administrative in its nature if it merely pursues a plan already adopted by the legislative body itself, or some power superior to it. 5 McQuillin Muni. Corp. § 16.53 (3d ed. 2015). *See also Reagan v. City of Sausalito*, 210 Cal. App. 2d 618, 621 (1962); *McKevitt v. City of Sacramento*, 55 Cal. App. 117, 124 (1921); *Valentine v. Town of Ross*, 39 Cal. App. 3d 954, 957 (1974). The distinction between legislative and executive authority is not always clear, and in some cases, may even overlap.

An example of such an overlap involves the sharing of responsibility between the Mayor and Council for the budgeting process. The Mayor is the chief budget officer of the City, responsible for the annual preparation of a balanced budget and the presentation of the proposed budget to the Council with the power to veto the actions of the Council. San Diego Charter §§ 28, 69, and 265. The Council holds public hearing(s) on the proposed budget and is responsible for adopting it. In the process, the Council may increase or decrease any item or add or remove any item provided that the budget must remain balanced. Within this framework, the Mayor and Council must ensure that the budget is adequate to allow each City department to carry out their duties under the Charter. As this Office has previously advised, "[c]ourts will not uphold budget cuts in the office of an elected official that prevent that official from carrying out his or her mandated duties." 2008 City Att'y MOL 53 (2008-9; Apr. 29, 2008).

Similarly, the Council can enact a process for its approval of new and existing surveillance technology. As the Charter is the controlling authority for the allocation of power within the City, however, the Council cannot exercise its legislative authority in such a way as to prevent the Mayor and City departments from performing their Charter-mandated duties, including the use of surveillance technology that is required for the Mayor and City departments to perform their Charter-mandated duties.

In addition, meet-and-confer obligations may be triggered if the City requires its employees to work without access to certain existing surveillance technology that allows them to be able to perform their jobs more effectively or keeps them safe in the performance of their duties.

12. **The Cate Memo Asks Whether It is "Feasible" to Have City Staff Seek Council Approval on All New and Existing Surveillance Technology.** This is a policy and operational question that will have to be addressed by City management.

CONCLUSION

A number of provisions in the Surveillance Ordinance would benefit from further discussion, clarification, and possible revision to ensure that legitimate concerns about the widespread use of mass surveillance technology are appropriately addressed while avoiding unintended consequences. We look forward to discussing the issues discussed in this memorandum and receiving guidance and input from the Council, City staff, and the public.

MARA W. ELLIOTT, CITY ATTORNEY

By */s/ Ken So*
Ken So
Deputy City Attorney

KRS:soc:ccm
MS-2020-24
Doc. No. 2467286
cc: Aimee Faucett, Chief of Staff, Mayor's Office
Kris Michell, Chief Operating Officer
Jeff Sturak, Assistant Chief Operating Officer
Jonathan Behnke, Chief Information Officer
Andrea Tevlin, Independent Budget Analyst
Douglas Edwards, Personnel Director
Kyle Elser, Interim City Auditor
Stacey Fulhorst, Ethics Commission Director
Elizabeth Maland, City Clerk

ORDINANCE NUMBER O-_____ (NEW SERIES)

DATE OF FINAL PASSAGE _____

AN ORDINANCE AMENDING CHAPTER 5 OF THE SAN DIEGO MUNICIPAL CODE BY ADDING NEW ARTICLE 11, DIVISION 1, AND SECTIONS 511.0101, 511.0102, 511.0103, 511.0104, 511.0105, 511.0106, 511.0107, 511.0108, 511.0109, AND 511.0110, ALL RELATING TO TRANSPARENT AND RESPONSIBLE USE OF SURVEILLANCE TECHNOLOGY.

WHEREAS, on January 29, 2020, the City of San Diego's Sustainability Department introduced to the Public Safety and Livable Neighborhoods Committee (PS&LN Committee) a draft Council policy on Streetlight Sensor Data Use for discussion and recommendation; and

WHEREAS, the PS&LN Committee unanimously voted to reject the proposed policy and to instead move forward with a more comprehensive framework to address the City's use of surveillance technology; and

WHEREAS, on July 15, 2020, members of the TRUST SD Coalition presented a proposed draft ordinance related to the transparent and responsible use of surveillance technology (Proposed Surveillance Ordinance) to the Public Safety and Livable Neighborhoods Council Committee (PS&LN Committee) for review and approval; and

WHEREAS, the PS&LN Committee discussed the Proposed Surveillance Ordinance and voted unanimously to direct the City Attorney to work with the PS&LN Consultant and the Mayor's Office to prepare the legal review of the Surveillance Ordinance, and to draft an ordinance in the appropriate form using the substance of the ordinance docketed at the July 15, 2020 PS&LN Committee to be forwarded to the Council for discussion and consideration; and

WHEREAS, the San Diego City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately monitored and regulated to protect an individual's right to privacy; and

WHEREAS, the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, 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 details about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, awareness that the government may be watching may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain 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, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

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

WHEREAS, the City Council has considered the Proposed Surveillance Ordinance in the form drafted by the Office of the City Attorney, which was heard at the Council meeting on November 10, 2020, and the Council wishes to incorporate any additional modifications approved by the Council from that meeting; and

WHEREAS, the City Council recognizes that prior to making a final determination on whether to approve the Proposed Surveillance Ordinance, the City must comply with the Meyers-Milias Brown Act (MMBA), California's collective bargaining law set forth at California Government Code sections 3500 through 3511, which is binding on the City; and

WHEREAS, the City Council also recognizes that depending on the outcome of the meet-and-confer process and the extent of any revisions to the Proposed Surveillance Ordinance resulting from that process, the City may be required to reintroduce the Proposed Surveillance Ordinance; NOW, THEREFORE,

BE IT ORDAINED, by the Council of the City of San Diego, as follows:

Section 1. That Chapter 5 of the San Diego Municipal Code is amended by adding new Article 11, Division 1, and sections 511.0101, 511.0102, 511.0103, 511.0104, 511.0105, 511.0106, 511.0107, 511.0108, 511.0109, and 511.0110, to read as follows:

Article 11: Transparent and Responsible Use of Surveillance Technology

Division 1: Approval Process for Use of Surveillance Technology

§511.0101 Definitions

For purposes of this Division, the following definitions shall apply and appear in italicized letters:

(a) *Annual Surveillance Report* means a written report concerning a specific *surveillance technology* that includes all of the following:

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

(2) Whether and how often data acquired through the use of the *surveillance technology* was shared with any internal or external entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and justification for the disclosure(s), except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(3) Where applicable, a description of the physical objects to which the *surveillance technology* hardware was installed without revealing the specific location of such hardware; for *surveillance technology* software, a breakdown of what data sources the *surveillance technology* was applied to;

(4) A list of any software updates, hardware upgrades, or system configuration changes accompanied by a description of altered or improved functionality that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change, except that no confidential or sensitive information should be disclosed that would violate any applicable law or undermine the legitimate security interests of the *City*;

(5) Where applicable, a description of where the *surveillance technology* was deployed geographically, by each *police area* in the relevant year;

(6) A summary of community complaints or concerns about the *surveillance technology*, and an analysis of its *Surveillance Use Policy* and whether it is adequate in protecting civil rights and civil liberties. The analysis shall consider whether, and to what extent, the use of the *surveillance technology* disproportionately impacts certain groups or *individuals*.

(7) The results of any internal audits or investigations relating to *surveillance technology*, any information about violations of the *Surveillance Use Policy*, and any actions taken in response. To the extent that the public release of such information is prohibited by law, *City staff* shall provide a confidential report to the City Council regarding this information to the extent allowed by law.

(8) 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, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(9) A general description of all methodologies used to detect incidents of data breaches or unauthorized access, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(10) Information, including crime statistics, that helps the community assess whether the *surveillance technology* has been effective at achieving its identified purposes;

(11) Statistics and information about Public Records Act requests regarding the relevant subject *surveillance technology*, including response rates, such as the number of Public Records Act requests on such *surveillance technology* and the open and close date for each of these Public Records Act requests;

(12) Total annual costs for the *surveillance technology*, including personnel and other ongoing costs, and what source of funding will fund the *surveillance technology* in the coming year; and

(13) Any requested modifications to the *Surveillance Use Policy* and a detailed basis for the request.

(b) *Board* means the Privacy Advisory Board established by Chapter 2, Article 6, Division 4 of the Municipal Code.

(c) *City* means any department, unit, program, and subordinate division of the City of San Diego as a municipal corporation.

(d) *City staff* means *City* personnel authorized by the City Manager or appropriate *City* department head to seek City Council approval of *Surveillance Technology* in conformance with this Division.

(e) *Community meeting* means a publicly held meeting that is accessible, noticed at least seventy-two hours in advance in at least two languages, for the purpose of educating communities, answering questions, and learning about potential impacts of *surveillance technology* on disadvantaged groups.

(f) *Continuing agreement* means a written agreement that automatically renews unless terminated by one or more parties.

(g) *Exigent circumstances* means a *City* department's good faith belief that an emergency involving danger of death or serious physical injury to any *individual*, or imminent danger of significant property damage, requires the use of *surveillance technology*.

(h) *Facial recognition technology* means an automated or semi-automated process that assists in identifying or verifying an *individual* based on an *individual's* face.

(i) *Individual* means a natural person.

(j) *Personal communication device* means a mobile telephone, a personal digital assistant, a wireless capable tablet, and a similar wireless two-way communications or portable internet-accessing device, whether procured or subsidized by the *City* or personally owned, that is used in the regular course of *City* business.

(k) *Police area* refers to each of the geographic districts assigned to a San Diego Police Department captain or commander.

(l) *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 data or combinations of data, such as license plate data, images, IP addresses, user identifications, unique digital identifiers, or data traces left by the *individual*.

(m) *Surveillance technology* means any software (e.g., scripts, code, Application Programming Interfaces), electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to observe, 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. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such *surveillance technology*. Examples of *surveillance technology* include the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; *facial recognition technology*; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; and 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, and biometric identification hardware or software.

(1) *Surveillance technology* does not include devices, software, or hardware, unless they have been equipped with, or are modified to become or include, a *surveillance technology* beyond what is set forth below or used beyond a purpose as set forth below:

(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 public *surveillance* or law enforcement functions related to the public;

(B) Parking ticket devices used solely for parking enforcement-related purposes, including any sensors embedded in parking sensors to detect the presence of a car in the space;

(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, provided that any information obtained from this equipment is used solely for medical purposes;

(H) Police department interview room cameras;

(I) *City* department case management systems;

(J) *Personal communication devices* that have not been modified beyond stock manufacturer capabilities in a manner described above;

(K) *Surveillance technology* used by the *City* solely to monitor and conduct internal investigations involving *City* employees, contractors, and volunteers;

(L) Systems, software, databases, and data sources used for revenue collection on behalf of the *City* by the City Treasurer, provided that no information from these sources is shared by the City Treasurer with any other *City* department or third-party except as part of efforts to collect revenue that is owed to the *City*.

(n) *Surveillance Impact Report* means a publicly posted written report including, at a minimum, the following:

(1) Description: Information describing the *surveillance technology* and how it works, including product descriptions from manufacturers;

(2) Purpose: Information on the proposed purposes(s) and outcomes for the *surveillance technology*;

(3) Location: The physical or virtual location(s) where it may be deployed, using general descriptive terms, and crime statistics for any location(s);

(4) Impact: An assessment of the *Surveillance Use Policy* for the particular *surveillance technology* 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 may disproportionately affect marginalized communities;

(5) Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each identified impact;

(6) 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, except that no

confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(7) Data Security: Information about the controls that will be designed and implemented to ensure that security objectives are achieved to safeguard the data collected or generated by the *surveillance technology* from unauthorized access or disclosure, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(8) Fiscal Cost: The forecasted, prior, and ongoing fiscal costs for the *surveillance technology*, including initial purchase, personnel, and other ongoing costs, and any current or potential sources of funding;

(9) Third Party Dependence: Whether use or maintenance of the *surveillance technology* will require data gathered by the *surveillance technology* to be handled or stored by a third-party vendor at any time;

(10) 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,

(11) Track Record: A summary of the experience, if any, other entities, especially government entities, have had with the proposed *surveillance technology*, including, if available, quantitative information about the effectiveness of the proposed *surveillance technology* in achieving its stated purpose in other jurisdictions, and any known adverse information about the *surveillance technology* such as unanticipated costs, failures, or civil rights and civil liberties abuses, existing publicly reported controversies, and any court rulings in favor or in opposition to the *surveillance technology*.

(12) Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and *City* departmental responses given, and *City* departmental conclusions about potential neighborhood impacts and how such impacts may differ as it pertains to different segments of the community that may result from the acquisition of *surveillance technology*.

(o) *Surveillance Use Policy* means a publicly-released and legally enforceable policy for use of the *surveillance technology* that at a minimum specifies the following:

(1) Purpose: The specific purpose(s) that the *surveillance technology* is intended to advance;

(2) Use: The specific uses that are authorized and the rules and processes required prior to such use, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(3) Data Collection: The information that can be collected, captured, recorded, intercepted, or retained by the *surveillance technology*, as well as data that might be inadvertently collected during the authorized uses of the *surveillance technology* and what measures will be taken to minimize and delete such data. Where applicable, any data sources the *surveillance technology* will rely upon, including open source data, should be listed. In the reporting of such information, no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(4) Data Access: The job classification of *individuals* who can access or use the collected information, and the rules and processes required prior to access or use of the information, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(5) Data Protection: The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms, except that no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the *City*;

(6) 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;

(7) Public Access: A description of how collected information can be accessed or used by members of the public, including criminal defendants;

(8) Third Party Data Sharing: If and how information obtained from the *surveillance technology* can be used or accessed, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

(9) Training: The training required for any individual authorized to use the *surveillance technology* or to access information collected by the *surveillance technology*;

(10) Auditing and Oversight: The procedures used 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 *surveillance technology* or access to information collected by the *surveillance 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

(11) Maintenance: The procedures used to ensure that the security and integrity of the *surveillance technology* and collected information will be maintained.

§511.0102 Board Notification and Review Requirements

(a) *City staff* shall notify the Chair of the *Board* by written memorandum prior to:

(1) seeking or soliciting funds for *surveillance technology*, including but not limited to applying for a grant;

(2) soliciting proposals with any entity to acquire, share, or otherwise use *surveillance technology*; or

(3) formally or informally facilitating in a meaningful way or implementing *surveillance technology* in collaboration with other entities, including *City* ones;

(b) Upon notification by *City staff*, the Chair of the *Board* shall place the request on the agenda at the next *Board* meeting for discussion and possible action. At this meeting, *City staff* shall inform the *Board* of the

need for the funds or equipment, or shall otherwise justify the action for which *City staff* will seek City Council approval pursuant to section 511.0103. The *Board* may make a recommendation to the City Council by voting for approval to proceed, objecting to the proposal, recommending that the *City staff* modify the proposal, or taking no action.

(c) If the *Board* votes to approve, object, or modify the proposal, *City staff* may proceed and seek City Council approval of the proposed *surveillance technology* initiative pursuant to the requirements of section 511.0103. *City staff* shall present to City Council the result of the *Board's* review, including any objections to the proposal.

(d) If the *Board* does not make its recommendation on the item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may proceed to the City Council for approval of the item.

(e) City staff shall seek *Board* review for new *surveillance technology* before seeking City Council approval under section 511.0103.

(1) Prior to seeking City Council approval under section 511.0103, *City staff* shall submit a *Surveillance Impact Report* and a *Surveillance Use Policy* for the proposed new *surveillance technology* initiative to the *Board* for its review at a publicly noticed meeting. The *Surveillance Impact Report* and *Surveillance Use Policy* must address the specific subject matter specified for each document as set forth in section 511.0101.

(2) Prior to submitting the *Surveillance Impact Report*, *City staff* shall complete one or more *community meetings* in each City Council district where the proposed *surveillance technology* is deployed, with opportunity for public comment and written response. The City Council may condition its approval of the proposed *surveillance technology* on *City staff* conducting additional community engagement before approval, or after approval as a condition of approval.

(3) The *Board* shall recommend that the City Council adopt, modify, or reject the proposed *Surveillance Use Policy*. If the *Board* proposes that the *Surveillance Use Policy* be modified, the *Board* shall propose such modifications to *City staff*. *City staff* shall present such modifications to City Council when seeking City Council approval under section 511.0103.

(4) If the *Board* does not make its recommendation on the item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may seek City Council approval of the item.

(f) *City staff* shall seek *Board* review for the use of existing *surveillance technology* before seeking City Council approval.

(1) Prior to seeking City Council approval for existing *surveillance technology* used by the *City* under section 511.0103, *City staff* shall submit a *Surveillance Impact Report* and *Surveillance Use Policy*

for each existing *surveillance technology* to the *Board* for its review at a publicly noticed meeting. The *Surveillance Impact Report* and *Surveillance Use Policy* shall address the specific subject matters set forth for each document in section 511.0101.

(2) Prior to submitting the *Surveillance Impact Report*, *City staff* shall complete one or more *community meetings* in each City Council district where the proposed *surveillance technology* is deployed with opportunity for public comment and written response. The City Council may condition its approval on *City staff* conducting additional outreach before approval, or after approval as a condition of approval.

(3) Prior to submitting the *Surveillance Impact Report* and proposed *Surveillance Use Policy* as described above, *City staff* shall present to the *Board* a list of *surveillance technology* possessed or used by the *City*.

(4) The *Board* shall rank the items in order of potential impact to civil liberties to provide a recommended sequence for items to be heard at *Board* meetings. The *Board* shall take into consideration input from *City staff* on the operational importance of the *surveillance technology* in determining the ranking to allow such matters to be heard in a timely manner.

(5) Within 60 calendar days of the *Board's* action in section 511.0102(f)(3), *City staff* shall submit at least one *Surveillance Impact Report* and proposed *Surveillance Use Policy* per month to

the *Board* for review, generally beginning with the highest-ranking items as determined by the *Board*, and continuing thereafter each month until a *Surveillance Impact Report* and *Surveillance Use Policy* has been submitted for each item on the list.

(6) If the *Board* does not make its recommendation on any item within 90 calendar days of notification to the *Board* Chair pursuant to section 511.0102(a), *City staff* may proceed to the City Council for approval of the item pursuant to section 511.0103.

§511.0103 City Council Approval for New and Existing Surveillance Technology

(a) *City staff* shall obtain City Council approval prior to any of the following:

(1) accepting local, state, federal funds or in-kind or other donations for *surveillance technology*;

(2) acquiring new *surveillance technology*, including but not limited to procuring such technology without the exchange of consideration;

(3) using new *surveillance technology*, or using existing *surveillance technology*, for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Division; or

(4) entering into a *continuing agreement* or other written agreement to acquire, share or otherwise use *surveillance technology*.

(b) City Council Approval Process

(1) After the *Board* notification and review requirements in section 511.0102 have been satisfied, *City staff* seeking City Council

approval shall schedule a date for City Council consideration of the proposed *Surveillance Impact Report* and proposed *Surveillance Use Policy*.

(2) The City Council shall only approve any action as provided in this Division after first considering the recommendation of the *Board*, 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.

(3) For approval of existing *surveillance technology* for which the *Board* does not make its recommendation within 90 calendar days of review as provided in section 511.0102(f)(5), 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.

(c) Unless otherwise provided in this Division, *Surveillance Impact Reports* and *Surveillance Use Policies* are public records. *City staff* shall make all *Surveillance Impact Reports* and *Surveillance Use Policies*, as updated from time to time, available to the public as long as the *City* uses the *surveillance technology*.

(d) *City staff* shall post all *Surveillance Impact Reports* and *Surveillance Use Policies* to the *City's* website with an indication of its current approval status and the planned City Council date for action.

§511.0104 Use of Unapproved Surveillance Technology During Exigent Circumstances

(a) *City staff* may temporarily acquire or use *surveillance technology* in a manner not in compliance with this Division only in a situation involving *exigent circumstances*.

(b) If *City staff* acquires or uses a *surveillance technology* in a situation involving *exigent circumstances*, *City staff* shall:

(1) immediately report in writing the use of the *surveillance technology* and its justifications to the City Council and the *Board*;

(2) use the *surveillance technology* solely to respond to the *exigent circumstances*;

(3) cease using the *surveillance technology* when the *exigent circumstances* end;

(4) only keep and maintain data related to the *exigent circumstances* and dispose of any data that is not relevant to an ongoing investigation or the *exigent circumstances*; and

(5) Following the end of the *exigent circumstances*, report the temporary acquisition or use of the *surveillance technology* for *exigent circumstances* to the *Board* in accordance with section 511.0102 at its next meeting for discussion and possible recommendation to the City Council.

(c) Any *surveillance technology* acquired in accordance with *exigent circumstances* shall be returned within 30 calendar days following when the *exigent circumstances* end, unless *City staff* initiates the process set forth for the use of the *surveillance technology* by submitting a *Surveillance Use Policy* and *Surveillance Impact Report* for *Board* review within this 30-day time period. If *City staff* is unable to meet the 30-day deadline, *City staff* shall notify the City Council, who may grant an extension. In the event that *City staff* complies with the 30-day deadline or the deadline as may be extended by the City Council, *City staff* may retain possession of the *surveillance technology*, but may only use such *surveillance technology* consistent with the requirements of this Division.

§511.0105 Oversight Following City Council Approval

(a) For each approved *surveillance technology* item, *City staff* shall present an *Annual Surveillance Report* for the *Board* to review within one year after the date of City Council final passage of such *surveillance technology* and annually thereafter as long as the *surveillance technology* is used.

(b) If *City staff* is unable to meet the annual deadline, *City staff* shall notify the *Board* in writing of *City staff's* request to extend this period, and the reasons for that request. The *Board* may grant a single extension of up to 60 calendar days to comply with this provision.

(1) After review of the report by the *Board*, *City staff* shall submit the *Annual Surveillance Report* to the City Council.

(2) The *Board* shall recommend to the City Council that the benefits to the community of the *surveillance technology* in question 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 any identified concerns.

(3) If the *Board* does not make its recommendation on the item within 90 calendar days of submission of the *Annual Surveillance Report* to the *Board* Chair, *City staff* may proceed to the City Council for approval of the *Annual Surveillance Report*.

(4) 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 511.0103 for that particular *surveillance technology* and the pertinent *Board* recommendation, including whether the City Council approved or rejected the proposal, and required changes to a proposed *Surveillance Use Policy* before approval.

(c) Based upon information provided in the *Annual Surveillance Report* and after considering the recommendation of the *Board*, the *City* shall revisit its cost benefit analysis as provided in section 511.0103(b)(2) 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 shall cease. Alternatively, the City Council may require modifications to a particular *Surveillance Use Policy* that will resolve any concerns with the use of a particular *surveillance technology*.

(d) *City staff* shall provide an annual report to City Council in closed session as permitted by state law on cybersecurity threats involving *surveillance technology* and how the *City* is managing risk to include the following:

(1) a list and description of any major *surveillance technology* updates that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change;

(2) information about any data breaches or unauthorized access to the data collected by the *surveillance tech*nology, including information about the scope of the breach and the actions taken in response; and

(3) a description of the standards and industry best practices that the *City* uses to detect incidents of data breaches or unauthorized access to *surveillance technology*.

§511.0106 Enforcement

(a) Violations of this Division are subject to the following remedies:

(1) Any material violation of this Division, or of a *Surveillance Use Policy* promulgated pursuant to this Division, 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 Division. An action instituted under this paragraph shall be brought against the *City*, and, if

necessary, to effectuate compliance with this Division 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 Division to the extent permitted by law.

(2) Any person who has been subjected to the use of *surveillance technology* in material violation of this Division, or of a material violation of a *Surveillance Use Policy*, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Division or of a *Surveillance Use Policy* promulgated under this Division, may institute proceedings in the Superior Court of the State of California against the *City* 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).

(3) A court may award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under sections 511.0106(a)(1) or (2).

§511.0107 Contracts for Surveillance Technology

It shall be unlawful for the *City* to enter into any contract or other agreement for *surveillance technology* after the effective date of this Division that conflicts with the provisions of this Division. Any conflicting provisions in any such contract or agreement, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Any amendment or exercise of any option to any contract after the effective date of this Division to obtain or use *surveillance*

technology shall require *City staff* to comply with the provisions of this Division. To the extent permitted by law, the *City* shall publicly disclose all of its *surveillance technology* contracts, including all related non-disclosure agreements executed after the effective date of this Division.

§511.0108 Whistleblower Protections

(a) 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:

(1) the employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of *surveillance technology* or *surveillance* data based upon a good faith belief that the disclosure evidenced a violation of this Division; or

(2) the employee or applicant was perceived to, about to, had assisted in or had participated in any proceeding or action to carry out the purposes of this Division.

(b) 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 Division.

(c) Any employee or applicant who is injured by a violation of section 511.0108 may institute a proceeding for monetary damages and injunctive relief against the *City* in any court of competent jurisdiction.

§511.0109 Grace Period for Use of Existing Surveillance Technology

The requirement for *City staff* to seek approval for the use of existing *surveillance technology* shall take effect one year after the effective date of this Division. *Surveillance technology* is considered existing if the City possessed, used, or has a contract in force and effect for the use of *surveillance technology* before the effective date of this Division.

§511.0110 Compliance with City Charter or Applicable State Law

Nothing in this Division is intended to violate any provision of the City Charter or applicable state law nor should any provision of this Division be interpreted in such a manner.

Section 2. That a full reading of this ordinance is dispensed with prior to passage, a written copy having been made available to the Council and the public prior to the day of its passage.

Section 3. That this ordinance shall take effect and be in force thirty days from and after its final passage.

APPROVED: MARA W. ELLIOTT, City Attorney

By _____
Kenneth R. So
Deputy City Attorney

KRS:cm
October 23, 2020
Or.Dept:CD-4
Doc. No.: 2516197

I hereby certify that the foregoing Ordinance was passed by the Council of the City of San Diego, at this meeting of _____.

ELIZABETH S. MALAND
City Clerk

By_____
Deputy City Clerk

Approved: _____ _____
(date) KEVIN L. FAULCONER, Mayor

Vetoed: _____ _____
(date) KEVIN L. FAULCONER, Mayor

ORDINANCE NUMBER O-_____ (NEW SERIES)

DATE OF FINAL PASSAGE _____

AN ORDINANCE AMENDING CHAPTER 2, ARTICLE 6, DIVISION 00 OF THE SAN DIEGO MUNICIPAL CODE BY ADDING NEW SECTIONS 26.42 AND 26.43, ALL RELATING TO ESTABLISHING THE PRIVACY ADVISORY BOARD.

WHEREAS, the San Diego City Council (City Council) finds that the use of surveillance technology is important to protect public health and safety, but such use must be appropriately monitored and regulated to protect the privacy and other rights of San Diego residents and visitors; and

WHEREAS, the Council proposes to create a new Charter section 43(a) citizen advisory board known as the Privacy Advisory Board to advise the Mayor and City Council on transparency, accountability, and public deliberation in the City's acquisition and usage of surveillance technology; and

WHEREAS, the use of open data associated with surveillance technology offers benefits to the City, but those benefits must also be weighed against the costs; and

WHEREAS, while the City Council acknowledges the privacy rights of residents and visitors, it also recognizes that surveillance technology may be a valuable tool to support community safety, investigations, and prosecution of crimes; and

WHEREAS, the San Diego Police Department and other City departments are responsible for protecting the public health and safety of San Diego residents and charged with a mission to serve and protect City residents, and in doing so, must not indiscriminately monitor, harass, or intimidate them; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information, but also may include

technology that aggregates publicly available information, which, in the aggregate or when pieced together with other information, has the potential to reveal details about a person's familial, political, professional, religious, or intimate associations; and

WHEREAS, awareness that the government may be watching may chill associational and expressive freedoms; and

WHEREAS, the City Council recognizes that data from surveillance technology can be used to intimidate and oppress certain 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, the City Council finds that decisions relating to the City's use of surveillance technology should occur with strong consideration 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 safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before City surveillance technology is deployed; and

WHEREAS, the City Council finds that decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input; and

WHEREAS, the City Council recognizes that prior to making a final determination on whether to approve the proposed ordinance creating the Privacy Advisory Board, the City must

comply with the Meyers-Milias Brown Act (MMBA), California's collective bargaining law set forth at California Government Code sections 3500 through 3511, which is binding on the City; and

WHEREAS, the City Council also recognizes that depending on the outcome of the meet-and-confer process and the extent of any revisions to the proposed ordinance creating the Privacy Advisory Board resulting from that process, the City may be required to reintroduce the Proposed Surveillance Ordinance; NOW, THEREFORE,

BE IT ORDAINED, by the Council of the City of San Diego, as follows:

Section 1. Chapter 2, Article 6, Division 00 of the San Diego Municipal Code is amended by adding new sections 26.42 and 26.43 to read as follows:

§26.42 Privacy Advisory Board

(a) Purpose and Intent

It is the purpose and intent of the Council to establish a Privacy Advisory Board to serve as an advisory body to the Mayor and Council on policies and issues related to privacy and surveillance. The Board will provide advice intended to ensure transparency, accountability, and public deliberation in the *City's* acquisition and use of surveillance technology.

(b) There is hereby established a Privacy Advisory Board to consist of nine members, who shall serve without compensation. At least six members shall be residents of the City of San Diego. Members shall be appointed by the Mayor and confirmed by the Council.

(c) All terms appearing in italics in sections 26.42 and 26.43 have the same meaning as in Chapter 5, Article 11, Division, section 511.0101, known as the San Diego Transparent and Responsible Use of Surveillance Ordinance.

(d) Qualifications of Members

(1) All members of the Privacy Advisory Board shall be persons who have a demonstrated interest in privacy rights through work experience, civic participation, and/or political advocacy.

(2) The Mayor shall appoint the nine members from the following representative areas of organizational interest, expertise, and background:

(A) At least one attorney or legal scholar with expertise in privacy or civil rights, or a representative of an organization with expertise in privacy or civil rights;

(B) One auditor or certified public accountant;

(C) One computer hardware, software, or encryption security professional;

(D) One member of an organization that focuses on open government and transparency or an individual, such as a university researcher, with experience working on open government and transparency; and

(E) At least four members from equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance,

including communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.

(e) Terms

(1) Members shall serve two-year terms, and each member shall serve until a successor is duly appointed and confirmed. Members are limited to a maximum of eight consecutive years.

(2) Initial members shall be appointed in staggered terms. For the initial appointments, five members shall be appointed to an initial term that will expire in 2021, and four members shall be appointed to an initial term that will expire in 2022. Initial appointments for less than the full term of two years shall not have the initial term count for purposes of the eight-year term limit.

(3) All terms shall expire on March 15 in the year of termination. Any vacancy shall be filled for the remainder of the unexpired term.

(f) Rules

(1) The Board shall adopt rules for the government of its business and procedures in compliance with the law. The Board rules shall provide that a quorum of the Privacy Advisory Board is five members.

(2) At the first regular meeting, and subsequently at the first regular meeting of each year, members of the Privacy Advisory Board shall select a chairperson and a vice chairperson.

§26.43 Privacy Advisory Board – Duties and Functions

The Privacy Advisory Board shall:

(a) Provide advice and technical assistance to the *City* on best practices to protect resident and visitor privacy rights in connection with the *City's* acquisition and use of s*urveillance technology*.

(b) Conduct meetings and use other public forums to collect and receive public input on the above subject matter.

(c) Review *Surveillance Impact Reports* and *Surveillance Use Policies* for all new and existing *surveillance technology* and make recommendations prior to the City seeking solicitation of funds and proposals for *surveillance technology*.

(d) Submit annual reports and recommendations to the City Council regarding:

(1) The *City*'s use of *surveillance technology*; and

(2) Whether new *City surveillance technology* privacy and data retention policies should be developed, or existing policies should be amended.

(e) Provide analysis to the City Council of pending federal, state, and local legislation relevant to the *City*'s purchase and/or use of *surveillance technology*.

(f) The Privacy Advisory Board shall make reports, findings, and recommendations either to the City Manager or the City Council, as appropriate. The Board shall present an annual written report to the City

Council. The Board may submit recommendations to the City Council following submission to the City Manager.

Section 2. That a full reading of this Ordinance is dispensed with prior to passage, a written copy having been made available to the Council and the public prior to the day of its passage.

Section 3. That this ordinance shall take effect and be in force on the thirtieth day from and after its final passage.

APPROVED: MARA W. ELLIOTT, City Attorney

By _____
Jennifer L. Berry
Deputy City Attorney

JLB:jvg
09/02/20
Or.Dept: Council District 4
Doc. No.: 2515606_2

I hereby certify that the foregoing Ordinance was passed by the Council of the City of San Diego, at this meeting of _____.

ELIZABETH S. MALAND
City Clerk

By_____
Deputy City Clerk

Approved: _____ _____
(date) KEVIN L. FAULCONER, Mayor

Vetoed: _____ _____
(date) KEVIN L. FAULCONER, Mayor