

**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 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 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 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