SEATTLE CITY COUNCIL
CENTRAL STAFF

July 26, 2017

M E M O R A N D U M

To: Gender Equity, Safe Communities and New Americans Committee
From: Amy Tsai, Council Central Staff
Subject: Surveillance (CB 118930)

SMC Chapter 14.18 requires City departments to obtain Council approval by ordinance before acquiring surveillance equipment, and it requires departments to develop operational and data management protocols that must be approved by the Council prior to the installation and deployment of that equipment. CB 118930 would update and expand the scope of the City's surveillance code. The legislation was previously summarized and discussed in Committee on April 12 and June 28.

A proposed substitute bill is undergoing final legal review as of the writing of this memo; the text of the substitute bill will be available at Committee. The main changes between the substitute bill and the current surveillance code (Chapter 14.18) include the following:

- **Scope** - The definition of surveillance equipment is expanded to include surveillance technology – specifically, any electronic device, software program, or hosted software service. The City has hundreds of devices, software programs and hosted solutions that will need to be screened for applicability to Chapter 14.18. Therefore, the substitute bill includes criteria and limiting factors for determining whether a technology meets the definition of surveillance technology. This includes, among other things, defining surveillance as being reasonably likely to raise concerns about civil liberties.

- **Community engagement** – The substitute bill provides that departments must conduct community outreach prior to Council approval. Also, a community advisory group will assist the Council in its surveillance technology police decision-making; the nature of that community advisory body is to be determined by a workgroup.

- **Exigent circumstances** – The current code allows a department to acquire or use surveillance equipment temporarily in advance of Council approval for a criminal investigation supported by reasonable suspicion, pursuant to a search warrant, or under exigent circumstances. The proposed substitute requires there to be an imminent risk of death or serious injury.

- **Oversight and enforcement** – The proposed substitute contains provisions related to oversight and enforcement that do not exist in current code.

    - The City Auditor and future Inspector General for Public Safety have review authority and should conduct annual reviews; the reviews are expected to start in 2018.
    - The Chief Technology Officer (CTO) conducts an annual equity impact assessment.
    - The CTO has the authority to order any department that is out of compliance with the requirements of Chapter 14.18 to cease acquisition or use of the surveillance technology.
    - The public has the right to sue the City for injunctive or declaratory relief for a material violation of Chapter 14.18, after a 90-day opportunity for the City department to address the concern.

- **Retrospective approval** – Unlike current code, the proposed substitute contains a process for bringing existing surveillance technologies into compliance over time. Due to the large number of technologies currently in use by the City that would need to be reviewed for applicability to Chapter 14.18, the Executive has 90 days to develop a list of surveillance technologies, and departments then submit surveillance technology approval requests to the Council at a rate of at least one per month for each affected department.

Because of the expanded scope, duties, and authorities in the proposed substitute, the proposed changes will incur greater financial costs than the current code. A fiscal note will be prepared prior to consideration by full Council.

Table 1 below summarizes the content of the proposed substitute for CB 118930 and compares its provisions to the current Chapter 14.18. Topics are grouped by related concepts. Where a bullet point is raised in one column and not in the other, there is no corresponding provision for that point.

Table 1. Comparison of Substitute CB 118930 to SMC Chapter 14.18

SMC Chapter 14.18	Substitute CB 118930
SCOPE	
• Surveillance equipment, including equipment capable of capturing or recording data; • operated by or at the direction of a City department; • that may capture activities of individuals.	• Surveillance technology, including any electronic device, software program, or hosted software solution; • acquired by or operated at the direction of a City department; • designed or primarily intended to be used to observe or analyze the movements, behavior, or actions of identifiable individuals, including license plate readers that can identify individuals when combined with other records; • reasonably likely to raise concerns about civil liberties, and weighing potential adverse impacts on disadvantaged groups

	and the likelihood that identifiable information will be shared with non-City entities.
SURVEILLANCE TECHNOLOGY EXEMPTIONS	
The following are not considered surveillance technology: • Police body-worn cameras or in-car videos • Cameras intended to record traffic patterns or traffic violations • Cameras recording activity inside or at entrances to City buildings for security purposes • Cameras installed to protect the physical integrity of City infrastructure such as reservoirs	**The following surveillance technologies are exempt from the requirements of Chapter 14.18:** • Existing exclusions (body-worn camera, etc.) are retained but language is updated and clarified. • Other exemptions are added, including technology where the data is knowingly and voluntarily provided or where the data collection has an opt-out option; and • technology that monitors only City employees in the performance of City duties.
COUNCIL APPROVAL PROCESS	
• Council approval is required prior to department acquisition of surveillance equipment; Council approval of operational protocols is required prior to deployment or installation. • The Council may also require that data management protocols be approved by ordinance prior to operating surveillance equipment. • The Council may approve the acquisition and operation, approve only the acquisition with operations to be approved by future Council action, deny the acquisition or use, or take other actions.	• Council approval of acquisition and an accompanying Surveillance Impact Report (SIR) is required prior to department acquisition of surveillance technology. The SIR contains elements similar to the operational and data management protocols in current code, as described below. • A department may acquire and use approved surveillance technology only in accordance with the terms in the SIR. All SIRs must be posted to the City's web site.
• A public outreach plan for each affected community with opportunity for public meetings and comment is to be included in operational protocols as part of the request to Council for approval.	• The department must conduct community outreach occur prior to Council approval.
	• The Executive must submit a quarterly list to the Council identifying all technology for

	which a determination was made that it is not surveillance technology subject to Chapter 14.18. • The Council may at any time designate that a technology is or is not surveillance technology subject to Chapter 14.18.
OPERATING PROTOCOLS/ SURVEILLANCE IMPACT REPORT	
Operating protocols must include the following: • A description of purpose and use • Type of equipment	**The SIR must include the following:** • A description of purpose, use, and intended benefits • A description and general capabilities, including reasonably foreseeable surveillance capabilities outside the proposed scope of use
	• A description of costs and any cost savings
• How and when the department will use the equipment, including continuously or under specific circumstances, and installed permanently or temporarily • Specific location if affixed to a structure • Specific deployment and authorization protocols if acquiring drones • Whether monitoring will be in real time or by review of historical recordings	• How and when the technology will be used and by whom, including continuously or under specific circumstances, and installed permanently or temporarily
	• A description of any additional rules that will govern use, including any legal standard for use, such as for purposes of a criminal investigation supported by reasonable suspicion • If the technology is a physical object, markings must clearly identify the responsible department, or else explain why that would render the surveillance ineffective.
• A description of how and when data will be collected and retained, and who will have access • Description of training for equipment operators • Assigning a lead department with responsibility for ensuring compliance	• How the department will ensure personnel are knowledgeable about data management protocols and able to ensure compliance with the use and data management policy

with protocols if more than one department will have access	• Identify specific unit responsible for ensuring compliance with data retention requirements
• Whether the department will share the equipment or data with any other government entity	• Whether the department will share with any other non-City entity, and if so, how it is necessary and what restrictions will be placed on the sharing; including the department's procedures for ensuring non-City entity compliance with any such restrictions • Non-City entity use by contract requires contractor to be bound by SIR terms.
• Privacy and anonymity rights affected and mitigation plans • A public outreach plan for each affected community with opportunity for public meetings and comment	• Impacts on civil rights, anonymity, and first amendment rights, disparate impacts, and a mitigation plan • A description of past and planned future community engagement
DATA MANAGEMENT PROTOCOLS/ SURVEILLANCE IMPACT REPORT	
Data management protocols must include the following: • A description of the data storage system • Retention period • How data will be stored and allow department and City Auditor to search, locate, and determine that specific data that was collected was properly deleted	**The SIR must also include the following:** • How data will be securely stored; • Retention period • Methods for storing data must allow department and auditors to search, locate, and determine that specific data that was collected was properly deleted
• How data may be accessed, who can authorize access, who will be allowed to request access, and for what reasons • When and how data management compliance audits will be conducted. • Have a viewer's log or other comparable method to track viewings • A description of which individuals have access to make copies and how copies will be tracked	• How data may be accessed, who can authorize access, and for what reasons What protections will be used to provide an audit trail if the surveillance technology has such mechanisms, such as a viewer's log • How data will be retained and deleted; what auditing procedures will be implemented to ensure proper retention • If the technology will be operated by another entity on the City's behalf, the SIR must describe the other entity's access and applicable protocols.

COUNCIL APPROVAL EXCEPTIONS	
• A department may temporarily acquire or use of surveillance equipment for the purpose of a criminal investigation supported by reasonable suspicion, pursuant to a warrant, or under exigent circumstances as defined in case law (exception does not apply to drones) without prior Council approval.	• A department may temporarily acquire or use surveillance technology in the event of an emergency that poses imminent and serious risk of death or substantial bodily harm in order to reduce that risk
	• A department may share data pursuant to court order, subpoena, or as otherwise required by law, notwithstanding the contents of an approved SIR • A department may perform technical upgrades needed to mitigate threats that materially change surveillance capabilities without prior Council approval, but subsequent Council approval is required • Seattle Municipal Court and the Seattle Public Library are exempt.
OVERSIGHT	
	• The Chief Technology Officer (CTO) prepares an annual community equity impact assessment; • The Council may direct the CTO to prepare a privacy and civil liberties impact assessment for any proposed technology, or the Inspector General for Public Safety may do so for the Seattle Police Department. • City Auditor and Inspector General for SPD may conduct annual reviews of how the technology or data were used, whether scope has changed, who had access, summary of any complaints, results of any internal audits, costs, and equity impacts.
ENFORCEMENT	
	• The Chief Technology Officer has the authority to order any department that is out of compliance with the requirements of Chapter 14.18 to cease use of the surveillance technology or its data.

	• A person who is surveilled and injured by a material violation of the Chapter may file for injunctive or declaratory relief or a writ of mandate; City has 90-day opportunity to correct.
RETROSPECTIVE APPROVAL OF EXISTING TECHNOLOGIES	
	• City departments have 90 days to identify list of existing surveillance technologies. Each department requests retroactive approval for existing technology at a rate of at least one per month.
COMMUNITY ADVISORY FUNCTION	
	• The Executive shall convene a workgroup by September 15, 2017, to recommend how to utilize community expertise to advise the Council. Recommendations are due December 31, 2017. In the interim, the Council will utilize the expertise of the Community Technology Advisory Board.

cc: Kirstan Arestad, Central Staff Director
Dan Eder, Central Staff Deputy Director