SEATTLE CITY COUNCIL
CENTRAL STAFF

M E M O R A N D U M

To:	Gender Equity, Safe Communities and New Americans Committee
From:	Amy Tsai, Council Staff
Date:	June 28, 2017
Subject:	Surveillance Technology and Data Acquisition (CB 118930)

CB 118930 would replace the current code provisions related to surveillance equipment, SMC Chapter 14.18, with a new chapter regulating the acquisition of surveillance technology and surveillance data. A first hearing on CB 118930 was held on April 12, 2017. Since then, a stakeholder group comprised of the Mayor's Office, Seattle Police Department, Seattle Department of Information Technology, ACLU, and Council staff have continued to discuss policy issues and challenges associated with updating the City's surveillance code. Main issues under discussion are summarized in this memo.

Background

This section recaps background information provided at the first GESCNA hearing on CB 118930.

SMC Chapter 14.18, Acquisition and Use of Surveillance Equipment, was adopted in 2013 by Ordinance 124142 following public reaction to the City's acquisition of drones and the installation of video cameras along Seattle's waterfront[1] and downtown. Later that year, a wireless mesh network installed downtown by the Seattle Police Department was deactivated in its test phase in response to public criticism over privacy concerns.[2]

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.

In the fall of 2016, the Seattle Police Department's purchase and use of a social media tracking tool, Geofeedia, came under public scrutiny, re-raising issues of public safety versus people's privacy rights.[3] Geofeedia was a social media tracking software purchased by the Seattle Police Department for about $14,000 to support criminal investigations, but the acquisition did not

[1] Seattle Times (Jan. 31, 2013). Waterfront surveillance cameras stir privacy fears. http://old.seattletimes.com/html/latestnews/2020260670_waterfrontcamerasxml.html; http://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program/

[2] Government Technology (Nov. 18, 2013). Seattle police to shut off wi-fi after privacy backlash. http://www.govtech.com/public-safety/Seattle-Police-to-Shut-Off-Wi-Fi-After-Privacy-Backlash.html

[3] The Stranger (Sept. 28, 2016). How the Seattle Police secretly – and illegally – purchased a tool for tracking your social media posts. http://www.thestranger.com/news/2016/09/28/24585899/how-the-seattle-police-secretlyand-illegallypurchased-a-tool-for-tracking-your-social-media-posts

undergo a public vetting process with the Seattle Department of Information Technology or the Council. The situation highlighted that Seattle's surveillance code was created to address surveillance "equipment," a definition that is need of updating in light of the surveillance capabilities of today's technologies, including software and cloud-based services. Updating the surveillance code has also provided an opportunity to examine other areas for improvement, as detailed below.

Provisions of CB 118930

As discussed at the April 12 GESCNA meeting, CB 118930 would revamp and update the City's surveillance code as follows:

- Any department seeking to acquire new surveillance technology or surveillance data must obtain Council approval by ordinance in advance of acquisition;
- Surveillance technology or surveillance data must be used in accordance with a Council-approved Surveillance Impact Report;
- Exemptions to this process are specified;
- Oversight provisions include an annual reporting requirement;
- Existing surveillance technologies or surveillance data that have not had prior Council approval are to be submitted for Council approval at a rate of one per month per department; and
- Individuals injured by a violation of the chapter may bring a suit for injunctive, declaratory, or other such non-monetary relief.

Issue Identification

Some of the main issues identified by the stakeholder group that have not yet been resolved are as follows:

- Surveillance data acquisition and data sharing
- Community engagement
- Reporting
- Enforcement

1. Surveillance data acquisition and data sharing

CB 118930 requires Council approval for surveillance data acquisition in addition to surveillance technology.[4] Surveillance data is data that comes from surveillance technology. The scope of CB 118930 includes regulation of the City's acquisition of surveillance technology and surveillance data from non-City entities, as well as the City's sharing of its surveillance technology or surveillance data with non-City entities.

[4] Current code applies only to surveillance equipment.

The breadth of what is covered by the legislation (i.e., how broadly surveillance technology and surveillance data are defined, what exemptions apply, which entities are covered), and the requirements placed on the sharing or receiving entity (e.g., Council approval, community involvement, data management requirements, and annual reporting) are key elements to the legislation that have significant implications for how departments operate and the resources required to implement and maintain the legislation.

For instance, SPD has regular, frequent, surveillance data sharing that occurs in the course of multijurisdictional criminal investigations without formal agreements regarding how each jurisdiction will collect, make use of, or protect privacy for, shared surveillance data. Under CB 118930, the Council would approve operational protocols for each acquisition that specify the terms under which SPD can share that data with other jurisdictions and the requirements to be placed on other jurisdictions for using Seattle's data. The stakeholder group has spent a significant amount of time discussing how to protect privacy and civil liberty interests of individuals with restrictions on surveillance data acquisition (both City-generated data and data that the City acquires from non-City entities) that will not have an undue chilling effect on criminal law enforcement activities.

2. Community engagement

SMC 14.18.20.H requires that a department's proposed operational protocols to the Council must include, "A public outreach plan for each community in which the department intends to use the surveillance equipment that includes opportunity for public meetings, a public comment period, and written agency response to these comments." As discussed on April 12, the community engagement requirements for CB 118930 are under continuing development. Several possibilities have been discussed by the stakeholder group, including requiring some opportunity for community public meetings prior to Council approval and some role for a community advisory board with surveillance expertise. Community engagement will have an associated departmental cost that will need to be weighed by the Council, but is a means of building community trust in government acquisition and use of surveillance tools.

3. Reporting

There is a requirement of annual reporting of surveillance technology or data use by each department. There is also an annual equity impact assessment examining any disproportionate impact on communities that is to be presented annually in GESCNA. The stakeholder group has been examining the reporting requirements for their level of detail and resource demands on departments, and how best to achieve effective oversight.

4. Enforcement

CB 118930 contains an enforcement provision that allows any person injured by a violation of the Chapter to institute proceedings against the City for injunctive relief, declaratory relief, writ

of mandate, or evidence suppression. The details around this provision are the subject of continuing analysis.

Next Steps

Amendment language is being prepared for committee consideration that addresses the issues identified above.

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