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:	April 12, 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 that imposes controls over the acquisition of surveillance technology and surveillance data. This is a first hearing on CB 118930. The purpose of the hearing is to provide an overview of the bill as introduced and identify policy areas where the language will be further refined with input from the Mayor's Office, departments, ACLU, and the Council.

Background

An inherent tension exists between the use of surveillance technology as a public safety tool and the public's right to privacy, free speech and association, and equal protection. 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 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

[1] Seattle Times (Jan. 31, 2013). Waterfront surveillance cameras stir privacy fears. http://old.seattletimes.com/html/latestnews/2020260670_waterfrontcamerasxml.html
[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

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.

Provisions of CB 118930

CB 118930 would revamp and update the City's surveillance code. Specifically,

- 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.

Analysis

The inherent tension between surveillance technology and privacy was summarized by the International Association of Chiefs of Police (IACP) in its analysis of the privacy impacts of using license plate readers.[4] License plate readers capture license plate numbers that are viewable by the general public, but data systems provide date, time and location information that can allow the tracking of vehicle movements, such as to doctors' offices or staging areas for political protests.

IACP notes that this type of information could have a chilling effect on social and political activities; the risk is that individuals will become more cautious in the exercise of their protected rights because they consider themselves to be under constant surveillance. Other privacy concerns include expanding data uses beyond the original purposes, sharing data with third parties beyond reasonable expectations, and heightening individuals' vulnerability to crime by revealing their identities, habits, and locations. Furthermore, if data is not carefully controlled, data breaches or misuse beyond the original stated purposes has the potential to erode community trust in government.

Crafting surveillance technology protections, then, becomes a complicated issue of not only needing to consider what the original data is and whether it contains identifiable information, but also what the data can be converted into, to what uses it will be put, who has access to it, and how good the controls are to prevent unauthorized access.

[4] IACP (Sept. 2009). Privacy impact assessment report for the utilization of license plate readers. http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf

Comparison of SMC Chapter 14.18 and CB 118930

Definition of Surveillance Technology

SMC 14.18.10 defines "surveillance equipment" as equipment capable of capturing or recording data, including images, videos, photographs or audio, operated by or at the direction of a City department, that may deliberately or inadvertently capture activities of individuals on public or private property. The SMC 14.18.10 definition of "surveillance equipment" arose in the context of concerns over drones and video cameras. There are, however, other technologies used by the City that the public might view as "surveillance" and therefore of concern, as evidenced by the Geofeedia situation.

Broader definition. CB 118930 defines surveillance technology much more broadly than SMC 14.18.10. Specifically, the definition of surveillance technology is not just about equipment, but rather includes any electronic device, software program or hosted solution, or services provided by a third party that is designed or primarily intended to be used for the purpose of surveillance.[5]

More exemptions. Because the definition of surveillance technology is broader, CB 118930 includes more exemptions. Social media sites and news alert services are exempted from the definition, to distinguish these common public sources from tools like Geofeedia. There is an exemption for technology where an individual opts-in to provide information or chooses not to opt out of providing information. Routine software updates and hardware replacements are also exempted.

Clarification of existing exemptions. CB 118930's definition also clarifies aspects of the SMC 14.18.10 definition, such as requiring as part of the definition that individuals be identifiable. When individual identities are not captured, there are not the same privacy concerns. SMC 14.18.10's exemption for City building security cameras is broadened to include installation anywhere on City property, in recognition of the fact that not all City security cameras focus on the inside or entrance to buildings and some are not on buildings at all, such as security cameras in parking lots.

Surveillance Impact Report

The Surveillance Impact Report required by CB 118930 is similar in content to the operational protocols and data management protocols of SMC Chapter 14.18. It contains a greater level of specificity on some items. The following topics are covered:

- The intended purpose and use of the surveillance information;

[5] "Surveillance" is defined in CB 118930 as observing or analyzing the movements, behavior, or actions of identifiable individuals or groups of individuals on public or private property.

- A description of the surveillance technology and its capabilities;
- How and when the technology will be used;
- Who will have access, how data will be secured, and how will use protocols be enforced;
- Retention periods and auditing processes;
- Whether the information will be shared with other government entities, and any restrictions on the sharing; and
- How privacy, first amendment, and other rights will be affected, and a mitigation plan.

SMC 14.18.20 requires operational protocols to include a public outreach plan for each community in which the department intends to use the equipment, including opportunity for public meetings and public comment. The outreach does not have to occur prior to Council approval, and the code does not contain provisions on how the results of the outreach should inform or affect any surveillance deployment. CB 118930 does not currently have a corresponding community engagement provision; how best to engage the community in CB 118930's process is a topic undergoing further discussion and development.

Third Party Sharing

The proposed legislation contains provisions regarding different uses and sharing of information -- either City information shared with a third party or third party information shared with the City.

In regards to information shared with a third party, if a City department plans to allow access to its surveillance technology or surveillance data by a third-party contract, the third party must comply with any relevant Surveillance Impact Report requirements. What requirements to place on third parties when the City shares data in the absence of a contract, such as the courtesy sharing of law enforcement information with other jurisdictions, is a subject of continuing discussion.

The department cannot circumvent the requirements of the code by entering into an agreement with a third party to have the third party acquire and collect surveillance data on the City's behalf. On the other hand, regardless of the data sharing protocols in the Surveillance Impact Report, surveillance technology or data can be shared when required by court order, subpoena, or as otherwise required by law.

In regards to information obtained from a third party, the proposed legislation exempts from the Council approval requirements any surveillance data collected by a third party when the data was collected for the third party's own use and the City is using the information for a criminal investigation supported by reasonable suspicion, under warrant, or for an administrative internal investigation. Convenience store video footage would be one example of such information. SMC Chapter 14.18 presently governs only data captured by or at the direction of a City department. It is a policy question whether the Council wishes to impose

surveillance approval requirements on the City's use of third party surveillance data that was not collected at the City's direction.

Exceptions

SMC 14.18.40 allows the temporary acquisition or use of surveillance for a criminal investigation supported by reasonable suspicion, pursuant to a warrant, or under exigent circumstances. CB 118930 replaces that exception with an exception for imminent risk of death or substantial bodily harm. While this creates a higher standard for spontaneous unapproved use of surveillance technology, its effect is to shift the focus of this exception to those surveillance technologies for which the need for their acquisition is truly unanticipated. If a department is contemplating the future use of a particular type of surveillance technology, when it seeks Council approval it can specify the intended use in its Surveillance Impact Report to include situations of reasonable suspicion.

Oversight and Enforcement

There are several mechanisms in the proposed legislation to ensure compliance. First, 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. Oversight responsibility falls primarily to the Seattle Police Department oversight entity, in consultation with the Chief Technology Officer; this recognizes that a large percentage of surveillance technology concerns, but not all, are in law enforcement. The reporting requirements are being examined for their level of detail and resource demands on departments, and how best to achieve effective oversight.

CB 118930 also 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.

Existing Technology

When SMC Chapter 14.18 was enacted, Ordinance 124142 gave each department operating surveillance equipment 30 days to propose operational and data management protocols. CB 118930 gives departments a timeline of one request for Council approval per month. This extended timeframe recognizes the fact that CB 118930 has a broader definition of surveillance technology and surveillance data that is expected to require more Council approvals. As the scope of the proposed legislation is finalized, additional analysis will occur on the expected backlog of technologies requiring Council approval.

Next Steps

As the proposed legislation is refined further, areas of focus will include:

- Strengthening community engagement;
- Refinement of third party use requirements; and
- Evaluation of resource impacts.

cc: Kirstan Arestad, Central Staff Director
Dan Eder, Central Staff Deputy Director
Ketil Freeman, Supervising Analyst