AN ORDINANCE relating to the City of Seattle’s use of surveillance equipment; requiring City
departments to obtain City Council approval prior to acquiring certain surveillance
equipment; requiring departments to propose protocols related to proper use and
deployment of certain surveillance equipment for Council review, requiring departments
to adopt written protocols that address data retention, storage and access of any data
obtained through the use of certain surveillance equipment, and establishing a new
Chapter 14.18 in the Seattle Municipal Code. It makes little sense to propose
these protocols for review. They should be presented for review, 
proposed for use, or submitted for approval.

WHEREAS, recent incidents involving the City’s acquisition of drones and the installation of
video cameras along Seattle’s waterfront have raised concerns over privacy and the lack
of public process leading up to the decisions to use certain surveillance equipment; and

WHEREAS, while surveillance equipment may help promote public safety in some contexts,
such as red light cameras, the benefits of such technologies should be weighed against the
potential downsides, including impacts on privacy; and 1) This implies that the
benefits of surveillance equipment are known and that “downsides”
are only potential. We should weigh potential benefits against
potential detriments. 2) “Red light cameras” are not an example of a
context in which such equipment may help promote safety, but
“enforcement of traffic regulations via the use of red light cameras”
would be.

WHEREAS, while the courts have established that people generally do not have a reasonable
expectation of privacy in public settings, the City should be judicious in its use of
surveillance equipment to avoid creating a constant and pervasive surveillance presence
in public life; and 1) This is somewhat misleading. We have reasonable
expectations of privacy in public from cameras looking up our skirts,
from X-rays peering into our bags, and from parabolic microphones
listening in on our quiet conversations. 2) This bill will help avoid
creating a constant and pervasive government surveillance presence in
public life. It does not address the possibility that pervasive private
surveillance may develop. 3) Prefer, “while U.S. Courts have
established that people generally do not have reasonable expectations of privacy in public settings, it is reasonable for people to expect their government to refrain from stockpiling information about their public words and actions as they go about their lawful business, and the City should be judicious in its use of surveillance equipment to avoid creating a system of constant and pervasive government surveillance in public life.”

WHEREAS, all City departments should seek approval from the City Council prior to the acquisition and operation of certain surveillance equipment; and Those departments should receive approval, not simply seek it, prior to such.

WHEREAS, City departments should also propose specific protocols for Council review and approval that address the appropriate use of certain surveillance equipment and any data captured by such equipment; and It is unclear whether protocols should address 1) appropriate use of equipment and 2) data captured, or if they should address 1) appropriate use of equipment, and 2) appropriate use of data collected. Prefer “should also propose specific protocols for Council Review and approval that address the appropriate use of certain surveillance equipment, appropriate use of data intended to be collected by such equipment, and appropriate use of data that are unintentionally captured by such equipment.”

WHEREAS, based upon the City Auditor Office’s recommendations related to the Seattle Police Departments handling of in-car video footage, departments should also develop protocols for retaining, storing, and accessing data captured by surveillance equipment; 1) This is unclear. Do the auditor's recommendations justify that which SPD should do (i.e., based on this audit, we think SPD should...), or should that which SPD does be guided by those recommendations (i.e., we think SPD should ... based on this audit)? 2) It would be helpful to provide more specific reference to the audit (e.g., year of publication, name of audit, etc.)

Protocols that departments develop should also address:
• restriction of access to the equipment to authorized users (particularly important if the equipment is remotely-accessible)
• qualifications for authorization to use the equipment
• updates to list of authorized users and audit trail
• security of any transmission of data collected by the equipment (e.g., encryption used to prevent unauthorized interception)
• notification procedures for breach of access restrictions
• public disclosure of data collected
• public disclosure of audits of use and of list of authorized users
Add: WHEREAS, Trust in a system is better rooted in clear understanding of its internal workings than in blind faith

Add: WHEREAS, Open source software and compliance with open standards facilitate understanding of computer systems, validation through peer review, early recognition of flaws, and effective remediation of those flaws

NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

Section 1. A new Chapter 14.18 of the Seattle Municipal Code is established as follows:

Chapter 14.18 Acquisition and Use of Surveillance Equipment

SMC 14.18.10 Definitions

The following definitions apply to this Chapter 14.18

“Data management protocols” generally means procedures governing how data collected by surveillance equipment will be retained, stored, indexed and accessed. Information comprising data management protocols includes, at a minimum, the information required in Section 14.18.30.

“Operational protocols” generally means procedures governing how and when surveillance equipment may be used and by whom. Information comprising operational protocols includes, at a minimum, the information required in Section 14.18.20.

”Surveillance equipment” means equipment capable of capturing and 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, regardless of whether “masking” or other technology might be used to obscure or prevent the equipment from capturing certain views. ”Surveillance equipment” includes drones or airborne vehicles and any attached equipment used to collect data. ”Surveillance equipment” does not include a handheld or body-worn device, a camera installed in or on a police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to
record traffic patterns and/or traffic violations, a camera intended to record activity inside or at
the entrances to City buildings for security purposes, or a camera installed to monitor and protect
the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.

**Regarding definition of “surveillance equipment”:**

- The exclusion of cameras “intended to record traffic patterns” from the
definition is concerning. This seems to allow for a system of high-
resolution, pan-tilt-zoom, cameras mounted on every utility pole,
recording both traffic patterns and everything else that happens on or
every public road, near every public road, and everything in line of
sight and zoom range of those cameras, without any of the restrictions
placed upon surveillance equipment applying to those cameras. As the
capability to automatically monitor and analyze the data collected by
“traffic cameras” increases, the desire to use those cameras to
perform general surveillance of the public will likely increase. In short,
if we restrict use of surveillance cameras but exempt “traffic cameras”
from those restrictions, then surveillance is likely to be performed
using traffic cameras.

- This definition includes airplanes and helicopters. Instead of “drones
or airborne vehicles,” use “drones or other unmanned vehicles” or
“drones or other unmanned, mobile, data collection devices.” Instead
of legislating the use of devices with which we are already familiar,
let's consider what it is about those vehicles that causes us to wish to
regulate them, then regulate all current and future devices that
possess those characteristics.
This definition includes infrared motion detectors such as those which trigger lights and security alarms, as those devices are “capable of capturing and recording data, including images, videos, photographs or audio.” If we mean for the definition to include only devices which are capable of capturing and recording one or more of still images, audio, and video, then this needs revision.

“Capable of capturing and recording data” causes this definition to exclude devices that capture but do not record data such as the traditional analog surveillance camera. Additionally, it's unclear just what capturing is and what recording is. It is unlikely that any digital device can capture or collect data without at least briefly recording those data (digital representations of images are recorded to internal memory before being copied to a network device, then copied in series to other network devices before being copied to a live operator's computer, then being copied to that computer's display device).

SMC 14.18.20 Council Approval for City Department Acquisition and Operations of Surveillance Equipment

Any City department intending to acquire surveillance equipment shall obtain City Council approval via ordinance prior to acquisition. Prior to deployment or installation of the surveillance equipment, City departments shall obtain Council approval via ordinance of operational protocols, unless applicable operational protocols were previously approved by ordinance. In requesting approval for acquisition of surveillance equipment, City departments shall include proposed operational protocols containing the following information for the City
Council’s consideration, along with any other information specifically requested by the City Council:

A. A clear statement describing the purpose and use of the proposed surveillance equipment. 
   Prefer “purpose and intended use.”

B. The type of surveillance equipment to be acquired and used. Should be more specific. Specifications and capabilities? Make and model?

C. The intended specific location of such surveillance equipment if affixed to a building or other structure. Require both general location of each piece of equipment (e.g., NE corner of building at 600 4th Ave.) and its specific location (latitude and longitude). Require approval of changes to location, before or after installation.

D. How and when a department proposes to use the surveillance equipment, such as whether the equipment will be operated continuously or used only under specific circumstances. 
   Operation and use can be very different things. Equipment which is operational (i.e., powered and collecting data) may not be “in use” by a human but still storing that which is collected for potential later use, or analyzing data for patterns which trigger notification.

E. How the department’s use of the equipment will be regulated to protect privacy and limit the risk of potential abuse. We don’t want to limit the risk of potential abuse, but to reduce the possibility of misuse and to limit the effect of any misuse that does occur.

F. A description of how and when data will be collected and retained and who will have access to any data captured by the surveillance equipment. Substitute “collected” for “captured” to maintain consistency (same for other instances later in the document). Consider that unless data collected are exempt from
the PRA, they are public record and anyone who requests access to those data will, by law, have access to them.

G. The extent to which activity will be monitored in real time as data is being captured and the extent to which monitoring of historically recorded information will occur. Monitoring can mean many different things. Observation of activities by one or more humans is naturally limited, as staffing is limited and a person can only observe so much at one time. The volume of activities which can be monitored by computers, however, is virtually unlimited. “Monitoring of historically recorded information” is confusing and redundant, as monitoring implies real-time observation and all recording is historical. Prefer “review of collected data” if we are to define “collect” as synonymous with “record.”

H. A description of the nature and extent of public outreach conducted in each community in which the department intends to use the surveillance equipment. Consider also requiring counts of people in affected communities, counts of people who were reached by outreach efforts, summary of comments provided by the public as a result of these outreach efforts, count of comments received.

I. If a department is requesting to acquire or use drones or other unmanned aircraft, it shall propose the specific circumstances under which they may be deployed, along with clearly articulated authorization protocols. Why limit to unmanned aircraft? Prefer “drones or other unmanned vehicles” or “drones or other unmanned, mobile, data collection devices.” Self-driving land vehicles are improving rapidly. The state of Nevada issued the first license for a self-driving car in mid-2012.
1. If more than one department will have access to the surveillance equipment or the data captured by it, a lead department shall be identified that is responsible for maintaining the equipment and ensuring compliance with all related protocols. If the lead department intends to delegate any related responsibilities to other departments and city personnel, these responsibilities and associated departments and personnel shall be clearly identified. If a device is accessed remotely (e.g., via computer network), then anyone with sufficient credentials or the ability to circumvent access controls (e.g., someone who is given or otherwise acquires one of the correct sets of username and password) will have access to the equipment. Consider the difference between restriction of access by policy and restriction of access by design (i.e., is unauthorized access impossible, difficult, or simply forbidden by policy?)

Exemption from the requirement for approval of protocols by ordinance for protocols which were previously approved may allow for protocols appropriate for one set of equipment to be used for equipment which should have different protocols. For instance, equipment that provides real-time and remote access to data collected would likely require different protocols than equipment that records locally and does not provide a live feed. Equipment which is available via the public Internet would likely require different protocols than that which is connected only to a private network or is not at all networked.

Upon review of the information required under this Section 14.18.20, and any other information deemed relevant by the City Council, the City Council may approve the acquisition and operation of surveillance equipment, approve the acquisition of surveillance equipment and
require future Council approval for operations, deny the acquisition or use of surveillance
equipment for the purpose proposed, or take other actions.

City Council may do any of the first three options at any time. Furthermore,
that they may do any of three things or take other action is a rather brain-
dead statement. Even stating that they shall take one of three actions or
some other action is rather weak, requiring only that they not react with
complete inaction upon review of required information. Prefer “Within N
days of review of information... City Council shall do one of the following:
approve... approve and require... or deny...”

SMC 14.18.30 Data Management Protocols for Surveillance Equipment

Prior to operating surveillance equipment acquired after the effective date of this ordinance, City
departments shall submit written protocols for managing data collected by surveillance
equipment to the City Council. The City Council may require that any or all data management
protocols required under this Section 14.18.30 be approved by ordinance. These data
management protocols shall address the following:

A. The time period for which any data collected by surveillance equipment will be retained.
B. The methods for storing recorded information, including how the data is to be labeled or
indexed. Such methods must allow for the department personnel and the City Auditor’s
Office to readily search and locate specific data that is collected and determine with
certainty that data was properly deleted, consistent with applicable law. What does it
mean to delete information that has been copied to multiple locations?
What does it mean to “locate specific data”---to retrieve (and thus to
copy) those data? To simply discover that they exist?
C. How the data may be accessed, including who will be responsible for authorizing access, who will be allowed to request access, and acceptable reasons for requesting access.  

1) Restrictions on who may request access are nearly meaningless. Much more significant are restrictions on which requests will be granted.  

2) Require also the addressing of who will be responsible for unauthorized access.  

3) Require explicit and specific disclosure of how access will be restricted, how authorized users will be authenticated, etc. Security by obscurity is folly; let's get all this out in the open so we can identify and rectify flaws before people with nefarious intent identify and exploit those flaws. As with the common tumbler lock, access restrictions should be well-known and trusted, and key management should be performed with great caution.  

3) Require also an audit log for authorization and retraction of such.  

4) Require that the list of authorized users and accompanying audit log be published proactively so that the public is able to learn of it without cumbersome and labor-intensive records requests and to encourage any redaction necessary for public disclosure to happen at the time of creation, not simply upon demand.

D. A viewer’s log or other comparable method to track viewings of any data captured or collected by the surveillance equipment, including the date, time, the individuals involved, and the reason(s) for viewing the records.  

1) Require logging of both date/time of access and date/time that accessed data were recorded.  

2) Require this log to be electronic, not written, and that it be published on a reasonable schedule to allow for public review.  

3)
Consider the effect of the Public Records Act on viewings of captured data.

E. A description of the individuals who have authority to obtain copies of the records and how the existence and location of copies will be tracked. 1) Such information will rapidly become obsolete as people change positions. Instead, require criteria by which decisions to authorize will be made. 2) Require also the logging and publication of such decisions (who authorized, who was authorized, under what circumstances will this authorization be revoked).

F. A general description of the system that will be used to store the data. 1) When describing a system with such high potential for misuse, hand-waving on the part of City departments, contractors, and vendors is unacceptable. Require a specific description of the system. The better we understand how the data are stored, the better we will be able to make use of them and to observe the use of them. 2) Consider carefully the implications of the Public Records Act on storage. If these are public records, they should be available to the public without the requirement that proprietary hardware or software be used to review them. 3) Whether or not they are public records, require that when possible, the data will be stored using open standards (e.g., standard, non-proprietary, computer file systems like EXT4 and XFS; image formats and audio/video codecs and containers that are not patent-encumbered, like PNG, OGG, and x264; free and open source database management systems like PostgreSQL, MySQL, and SQLite; standard and well-tested encryption algorithms like AES and Twofish). If access
to the data is to be restricted, they should be encrypted to mitigate the negative effect of security breaches. 4) Digital signatures should be used to verify that data have not been modified since collection.

G. A description of the unit or individuals responsible for ensuring compliance with Section 14.18.30 and when and how compliance audits will be conducted. Again, this information is likely to become obsolete rapidly, so require descriptions of the criteria by which such responsibility will be delegated, and require publication and maintenance of the current state of responsibility.

Section 2. Unless Council previously approved operational protocols by ordinance for department surveillance equipment, each City department operating surveillance equipment prior to the effective date of this ordinance shall propose written operational protocols consistent with SMC 14.18.20 no later than thirty days following the effective date of this ordinance for Council review and approval by ordinance. It is unclear what “operating prior to a date” means (and without prefacing “was” it is likely grammatically incorrect), and “operation” of the equipment at any time is less significant than the possibility of such. Prefer “each City department that acquired surveillance equipment prior to the effective date of this ordinance, shall, unless that equipment has since been destroyed or transferred elsewhere, propose...”.

Section 3. Each department operating surveillance equipment prior to the effective date of this ordinance shall adopt written data management protocols consistent with SMC 14.18.30 no later than thirty days following the effective date of this ordinance and submit these protocols to the City Council for review and possible approval by ordinance. Similar to section 2, require such of departments that acquired the equipment prior to the ordinance unless that department no longer has the equipment.
We should require departments that acquired their equipment prior to the ordinance to disclose all information that the ordinance requires of new acquisitions, including: Current authorized users, criteria for authorization, locations of fixed-location equipment.

This ordinance shall take effect and be in force 30 days after its approval by the Mayor, but if not approved and returned by the Mayor within ten days after presentation, it shall take effect as provided by Seattle Municipal Code Section 1.04.020.
Passed by the City Council the ____ day of ________________________, 2013, and signed by me in open session in authentication of its passage this _____ day of __________________, 2013.

_________________________________
President __________of the City Council

Approved by me this ____ day of _____________________, 2013.

_________________________________
Michael McGinn, Mayor

Filed by me this ____ day of __________________________, 2013.

____________________________________
Monica Martinez Simmons, City Clerk

(Seal)