



City of Madison
MINUTES - APPROVED
CCOC Subcommittee on
Police & Community Relations

City of Madison
Madison, WI 53703
www.cityofmadison.com

Monday, January 30, 2017

7:00 p.m.

**Warner Park Community
& Recreation Center
1625 Northport Drive
Community Room 1**

[Website](#) | [Handouts at Meetings](#) | [Meeting Minutes](#)

Members Present: Ald. Shiva Bidar-Sielaff (vice-chair), Ald. Sheri Carter and Ald. Rebecca Kemble

Members Absent: Ald. Marsha Rummel and Ald. Denise DeMarb (notified)

Staff Present: Capt James Wheeler, MPD Representative, Lisa Veldran, Council Administrative Assistant and Heather Allen, Council Legislative Analyst

Others Present: M Adams & Max Rameau from Freedom Inc, Molly Collins & Emilio De Torre from ACLU, Larry Kaseman, Satya Rhodes-Conway, Rita Hindin, Jamala Rogers (Organization for Black Struggle), Eric Upchurch, Thomas Rehman, Megan Roman

Call to Order

Vice-Chair, Ald. Shiva Bidar-Sielaff called the meeting to order at 7:03 p.m.

Approval of Minutes

Ald. Rebecca Kemble moved to approve the January 18, 2017 CCOC Subcommittee on Police & Community Relations minutes, seconded by Ald. Sheri Carter. Motion was approved unanimously.

Public Comment

There was no public comment.

Disclosures & Recusals

There were no disclosures or recusals from members of the subcommittee present.

Suspension of the Rules

Ald. Rebecca Kemble moved, seconded by Ald. Sheri Carter to suspend the rules to allow for public participation on agenda items of #5 (Freedom Inc Presentation) and #6 (ACLU Presentation). Motion was approved.

Presentation: Freedom, Inc.

M Adams and Max Rameau, representing Freedom, Inc., presented information on creating a community policing district and a community police control board (see brochure "Community Control Over Police" PDF) which allows "municipalities, cities or towns to organize into policing districts based on existing social cohesion of neighborhoods and communities". The district would be run by a Community Police Control Board (CBCB) and funding would go directly to the board. The board would set priorities, establish policies and practices for their policing district. M Adams and Mr. Rameau believed this model would better serve the community than the current police district by giving voice to the marginalized and a democratic voice to the community.

Ald. Carter asked about board membership were they looking at people who live in the area by address, voting rolls, etc... Mr. Rameau said they would use a variety of records; in addition to the records listed by Ald. Carter, driver's license, utility records, etc.

Ald. Kemble asked about the people who are most effected negatively by the police how would the minority in predominately white districts. Mr. Rameau said the lines could be drawn in a way where people would have the greatest opportunity to have input.

There was discussion on what types of training community members would need (literacy, how to run meetings, judicial system) and supportive systems needed (transportation, child care).

- Larry Kaseman Stoughton WI Spoke/Favor
Would like to see the Council enact this model. M Adams noted that there were state statutes that would need to be changed but that there were some action that the city could take outside of the statutes.
- Jamela Rogers, Organization for Black Struggle Madison WI Spoke/Favor
Noted that she is a Visiting Fellow from St. Louis MO where there is [Civilian Oversight Board](#) and would be willing to talk to people about this model.
- Rita Hindin Madison WI Spoke/Favor
Stated that she came from the health field and perspective and suggested that the group use the [Precautionary Principle](#) when developing the model.
- Megan Roman Monona WI Spoke/Favor
Supported community control of police
- Eric S. Upchurch II Madison WI Spoke/Favor
With Council of Communities and is supportive of any ways to empower the community to self-determine their decisions around these issues.

Ald. Bidar-Sielaff asked how Freedom Inc was looking at developing the police districts. M Adams said they would look developing districts that would represent all the voices, and then determine the form and function.

Ald. Bidar-Sielaff asked how resource allocation by district would function. Mr. Rameau stated that they would look at ways where districts would not be resource “starved” and develop a system of equitable sharing of funds.

- Satya Rhodes-Conway Madison WI Spoke/Favor
Believe Council should take this model under serious consideration and use the maps from the last redistricting exercise.

Ald. Carter asked if the group envisioned more police stations. M Adams would decide how they would want to house their community safety team, but each community would have a physical space to house that policing area.

Ald. Kemble had a question about combined protective services (police and fire) and would their model be strictly police. Mr. Remeau stated that this structure varies by state and it could encompass the fire department.

Presentation: American Civil Liberties Union (ACLU)

Molly Collins and Emilio De Torre, representing the ACLU were presenters. They reviewed the overuse of surveillance efforts that target communities and the lack of checks and balances in protecting residents’ First Amendment rights. Technology is expanding in this area, causing infringement on First Amendment rights; automated license plate readers (Madison has these), [Dirtbox](#), [Cellebrite](#), social media tracking and hacking technology, [Stingray](#) tracking technology (used by Milwaukee).

Mr. De Torre reviewed the model resolution/ordinance drafted by the ACLU that tries to address how data is collected, who has access to the data and what data is collected. The draft requires Council approval of law enforcement surveillance technology and annual data reporting. He noted that Santa Clara, Oakland, Cambridge and other cities are in the process of adopting the resolution or have adopted the resolution ([ACLU Link](#)).

Ald. Bidar-Sielaff noted that the City Attorney cautioned the subcommittee against recommending adoption of the resolution/ordinance but could only discuss the draft.

Ald. Kemble asked if the ACLU had reviewed the city's adopted ordinances on surveillance cameras/technology. Ms. Collins and Mr. De Torre indicated that they had reviewed the city's ordinances but not the MPD Standard Operating Procedures. Mr. De Torre noted that there are state statutes, but not specifically city ordinances that involve procurement of the technology.

Ald. Bidar-Sielaff asked if they could provide the subcommittee with examples of cities who have adopted the language. Mr. De Torre indicated that the following cities they have either adopted or introduced the ACLU draft: Santa Clara, Oakland, Seattle, Cambridge, St. Louis and New York.

- Larry Kaseman Stoughton WI Spoke/Favor
Mr. Kaseman asked if ordinances that have been adopted, does it have an impact on public information. Ms. Collins said no, that the model language has only been recently developed so there was no data yet but ACLU hopes that it creates a great level of transparency for the public and creates greater trust with the police department. Mr. Kaseman asked about using it in court cases. Ms. Collins said that it would depend upon individual city policies; the draft language was specifically about the technology.
- Rita Hindin Madison WI Spoke/Favor
Ms. Hindin asked if there was any federal legislation. Ms. Collins did not know the answer but doesn't think there has been any legislation on this issue or if it would pre-empt city ordinances.
- Thomas Rehman Madison WI Spoke/Favor
Mr. Rehman indicated that he works with healthcare data and he was pleased that this issue was being discussed. He noted the need to protect civil liberties and have policies that require technologies to be transparent.
- Jamela Rogers, Organization for Black Struggle Madison WI Spoke/Favor
Ms. Rogers noted that there is a need to have this type of legislation in place.

Ald. Bidar-Sielaff explained to the public that an alder would need to request creation of the resolution and ordinance.

Discussion: Upcoming Meetings

FEBRUARY MEETING DATES

Thursday, February 16, 2017 at 6:00 PM
Room 351, City-County Building
Colleen Clark, Dane County Equity
& Criminal Justice Coordinator

Monday, February 27, 2017 at 6:00 PM
Room GR27, City-County Building
No presentations scheduled.
Report and recommendation

Resolution Timeline

- Council Meeting: March 7, 2017 Introduce Resolution Accepting Final Report & Recommendations and Refer to CCOC, PSRC, EOC, Common Council Meeting 3/21/17
- Special CCOC Meeting: March 21, 2017
- Council Meeting: March 21, 2017 - Adoption of Resolution Accepting Report & Recommendations

Adjournment

Ald. Sheri Carter moved, seconded by Ald. Rebecca Kemble, to adjourn. Motion passed unanimously. Meeting adjourned at 8:35 p.m.



Community Control Over Police

In Black communities, and other communities of color, the police often act and are received as an occupying force. Instead of protecting Black people in their own communities, the police are, ultimately, in those neighborhoods in order to protect others from Black people.

As such, while the police enjoy majority support among the general white population, the same cannot be said for the Black community or many other communities of color.

Any claim to democracy is firmly grounded in the informed consent of the governed, a concept rooted in international law and theories on democracy. Due to the particular racial and social history of the United States, we assert that the police operate inside of Black communities without the consent of the governed.

Community Control over Police is a proposition for real democracy.

By centering control over police in local communities, the intents and functions of democracy will be served as the police will exercise the will of community they serve.

PROCESS

A given municipality, city or town organizes itself into **policing districts** based on the existing social cohesion of neighborhoods and communities therein. These districts can overlap exactly, substantially or not at all with existing political boundaries, such as council districts.

Following sufficient public discussion, debate and information, **an election will allow residents of each district to give informed consent** to those charged with protecting them and endowed with the government sanctioned power to detain, arrest and even commit acts of violence, up to and including killing.

The election will empower residents of each district to either retain their existing police department or to replace that department with a police force that is democratically controlled by district residents. Much like voting for council members, district residents are empowered to determine the fate of their own district, but not others.

Those districts voting to retain their police continue service as usual. Those districts voting for community control begin the process of building a new force from the ground up, reflective of the priorities of that community. The existing police department will redraw its jurisdictional maps accordingly.

Funding for the new force(s) comes from the exact same taxpayer and grant sources as the existing department. The existing police budget is divided among the partitioned districts and amounts are allocated towards each district **based on the actual police resources used** prior to the election.

That is to say, districts with high crime rates necessitating constant patrolling and more arrests, by definition utilize a greater percentage of police resources. Those resources remain in that district after the vote. Similarly, state, federal or foundation grants secured by the existing department based on the needs of a particular district, remain with that district after the vote.

For example, if a local police department secures federal grants for extra police, additional weapons, new technology and used military equipment based on the statistical profile of a low-income Black community, those resources gained for that community should remain there after the vote. Securing funds for a struggling low-income Black community and then shifting it for the benefit of the business district or a wealthy enclave is stealing from the poor.

COMMUNITY POLICE CONTROL BOARD

The new force is run by the Community Police Control Board (CPCB).

The CPCB has the power and authority to set **priorities**, establish **policy** and enforce good **practice** in the force. The board meets on a regular basis to evaluate and adjust priorities and policies, as well as deal with issues of practice and implementation, upto and including firing individual officers. As strong supporters of human, worker and civil rights, all personnel decisions are subject to due process and fair labor practices.

The CPCB is comprised of 12 adult human residents of the district. CPCB terms can be 2 years in duration, with staggered seating so that the entire board is not replaced all at once.

Members of the CPCB are seated via **random selection** or **sortition** from a combination of voter rolls, driver licenses, public utility records, public benefit (social security, etc.) records or any other records that confirm residence.

Sortition is a democratic and egalitarian governing structure that ensures all residents have an equal chance of entering office irrespective of any bias in society or preferences of corporate or other interests. For example, while just over 3% of the American population has a net worth of more than \$1 million, over 50% of the 538 members of the US Congress are millionaires. Sortition will improve the chances of ordinary people to exercise their democratic rights.

Sortition also minimizes opportunities for corruption, as political cliques and entrenched interests have difficulty forming and corporate sponsorship of officials is not possible.

Sortition is used in small scale in a number of municipalities around the world, including several Canadian cities. Sortition is also the basis for the American jury system, where unelected individuals, selected at random, determine guilt, innocence and punishments, including death, of those the government accuses of breaking the law.

In order to facilitate, and even encourage, participation, selected members can be provided with transportation, childcare, meals, personal assistants and even modest stipends among other accommodations.

POWERS

The primary powers of the CPCB is setting priorities, establishing policies and enforcing good practices of the force.

Pursuant to the faithful execution of its duties, the CPCB has the power to hire force staff, legal counsel, assistants and even a chief for day to day management.

LEGISLATIVE AUTHORITY

State legislative authority for community control over police can be derived from one of two sources:

State Statute **62.13(1)** allows cities to create police and fire boards comprised of five members appointed by the mayor. Utilization of this statute requires a two step process.

First, for the members of the board, even though endowed with the power to appoint, most mayors make appointments based on recommendations from council members, staff, friends and even lobbyists. This recommendation process can be formalized with a city ordinance compelling the mayor to select board members from among sitting members of a local CPCB, or at least one from each CPCB in existence and others at the will of the mayor. Second, the board will have to agree to limit their range of directives in order to allow the CPCB their full range of prescribed powers.

State Statute **62.13(2e)** allows cities to forgo the traditional police department and accompanying board in favor of a Combined Protective Services department that can perform police and other public safety functions. State Statutes allow this department, or departments, broader latitude in terms of organizational structure and decision making process.

A number of villages in Wisconsin, such as the village of Menomonee Falls, WI, use Combined Protective Services departments in lieu of traditional police departments.

ACLU WORKING DRAFT

A Resolution to Establish Community Control Over Police Surveillance

Whereas, the Common Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology.

Whereas, no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution.

Whereas, surveillance technology has historically threatened the privacy of all citizens, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

Whereas, legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed.

Whereas, if a surveillance technology is approved, data reporting measures must be adopted that empower the Common Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

Whereas, the full cost of a surveillance technology should be considered and made publically available to analyze if its financial benefits outweigh its costs and if an expenditure on such a technology, and any contractual obligation or usage agreement is in the best interest of the City.

Whereas, the Common Council finds that regular reporting by the Madison Police Department as to the effectiveness of purchased surveillance technologies must be made to ensure transparency, understanding, and progress.

NOW, THEREFORE, BE IT RESOLVED By the Common Council of the City of Madison, a Community Control Over Police Surveillance policy, a copy of which is attached to this file, is adopted as City policy; and, be it:

Further Resolved, That the implementation of the policy shall be overseen by the Finance Committee; and, be it

Further Resolved, That the Finance Committee shall provide annual updates to the Common Council on the implementation of the Community Control Over Police Surveillance policy.

Community Control Over Police Surveillance Policy

Purpose

Decisions relating to surveillance technology should occur with strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution. Additionally, the full cost of a surveillance technology should be considered and made publically available to analyze if its financial benefits outweigh its costs and if an expenditure on such a technology, and any contractual obligation or usage agreement is in the best interest of the City.

Scope

A municipal department must obtain Common Council approval (via a Surveillance Impact Report and Surveillance Usage Policy), subsequent to a mandatory, properly-noticed, germane, public Common Council hearing at which the public is afforded a fair and adequate opportunity to provide written and oral testimony, prior to engaging in any of the following:

- (1) Seeking funds for new surveillance technology;
- (2) Acquiring or borrowing new surveillance technology;
- (3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the Common Council in accordance with this Policy; or
- (4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use surveillance technology or surveillance data.

Definitions

- (A) "Discriminatory" shall mean (1) disparate treatment of any individual(s) because of any real or perceived traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the State of Wisconsin, or any ordinance of the City of Madison, or because of their association with such individual(s), or (2) disparate impact on any such individual(s) having traits, characteristics, or status as described in subsection (1).
- (B) "Disparate impact" shall mean an adverse effect that is disproportionately experienced by individual(s) having any traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the State of Wisconsin, or any ordinance of the City of Madison than by similarly situated individual(s) not having such traits, characteristics, or status.
- (C) "Discriminatory" shall mean targeted at any community or group or its members because of their real or perceived inclusion in or association with a community or group as to which discrimination is prohibited under the constitution or any law of the United States, the constitution or any law of the State of Wisconsin, or any ordinance of the City of Madison, or having a disparate impact on any such community or group or its members.
- (D) "Disparate impact" shall mean an adverse effect that is statistically more likely to be experienced by members of a particular community or group as to which discrimination is prohibited under the constitution or any law of the United States, the constitution or any law of the State of Wisconsin, or any ordinance of the City of Madison, than similarly situated individuals outside of that community or group.
- (E) "Municipal entity" shall mean any municipal government, agency, department, bureau, division, or unit of this City.

- (F) "Surveillance data" shall mean any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.
- (G) "Surveillance technology" shall mean any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.
- (1) "Surveillance technology" includes, but is not limited to: (a) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (b) automatic license plate readers; (c) electronic toll readers; (d) closed-circuit television cameras; (e) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (f) mobile DNA capture technology; (g) gunshot detection and location hardware and services; (h) x-ray vans; (i) video and audio monitoring and/or recording technology, such as surveillance cameras and wearable body cameras; (j) surveillance enabled or capable lightbulbs or light fixtures; (k) tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; (l) social media monitoring software; (m) through-the-wall radar or similar imaging technology, (n) passive scanners of radio networks, (o) long-range Bluetooth and other wireless-scanning devices, (p) radio-frequency I.D. (RFID) scanners, and (q) software designed to integrate or analyze data from surveillance technology, including surveillance target tracking and predictive policing software. The enumeration of surveillance technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by any municipal entity.
- (2) "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 1(E): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be use surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; and (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems.
- (H) "Viewpoint-based" shall mean targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

General Policy

Section 1.

- (A) A municipal entity must obtain Common Council approval, subsequent to a mandatory, properly-noticed, germane, public Common Council hearing at which the public is afforded a fair and adequate opportunity to provide written and oral testimony, prior to engaging in any of the following:
- (1) Seeking funds for new surveillance technology, including but not limited to applying for a grant, or soliciting or accepting state or federal funds or in-kind or other donations;
 - (2) Acquiring or borrowing new surveillance technology, whether or not that acquisition is made through the exchange of monies or other consideration;

- (3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the Common Council in accordance with this Policy; or
 - (4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use surveillance technology or surveillance data.
- (B) Prior to seeking approval pursuant to Section 1(A) for the funding, acquisition, or use of surveillance technology or the entry into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the Common Council a Surveillance Impact Report and Surveillance Use Policy concerning the technology at issue at least forty-five (45) days prior to the public hearing.
- (1) The Common Council shall publicly release, in print and online, the Surveillance Impact Report and Surveillance Use Policy at least thirty (30) days prior to the public hearing.
 - (2) The Common Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 1(A).
- (C) No use of surveillance technology by a municipal entity pursuant to Section 1(A) shall be permitted without the Common Council's express approval of the related Surveillance Impact Report and Surveillance Use Policy submitted by the municipal entity pursuant to Section 1(B).
- (D) Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy, the Common Council may request revisions be made by the submitting municipal entity. Revisions should be requested where any inadequacies are perceived to exist within a Surveillance Use Policy or Surveillance Impact Report, especially with respect to the protection of civil rights and civil liberties and the avoidance of discriminatory and viewpoint-based uses, deployments, and impacts.
- (E) A Surveillance Impact Report submitted pursuant to Section 1(B) shall be a publicly-released, legally enforceable written report that includes, at a minimum, the following:
- (1) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - (2) Information on the proposed purpose(s) for the surveillance technology;
 - (3) If the surveillance technology will not be uniformly deployed or targeted throughout the city:
 - (a) What factors will be used to determine where the technology is deployed or targeted; and
 - (b) Based upon those factors enumerated pursuant to Section 1(E)(3)(a), what geographical location(s) are anticipated to receive a disproportionately high level of deployment or targeting;
 - (4) The fiscal impact of the surveillance technology, including but not limited to:
 - (a) Initial acquisition costs;
 - (b) Ongoing operational costs such as personnel, legal compliance, use auditing, data retention and security costs;
 - (c) Any cost savings that would be achieved through the use of the technology; and
 - (d) Any current or potential sources of funding; and
 - (e) The City of Madison will retain ownership and rights of usage of data, products, information, and reporting; and
 - (5) An assessment identifying with specificity:
 - (a) Any potential impacts the surveillance technology, if deployed, might have on civil liberties and civil rights, including but not limited to:
 - (i) Potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a discriminatory manner;

- (ii) Potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a viewpoint-based manner;
 - (iii) Potential disparate or adverse impacts on any communities or groups if the surveillance technology is operated using intentionally or inadvertently biased algorithms;
 - (iv) Potential adverse impacts on privacy and anonymity rights;
 - (v) Other potential adverse impacts on the civil rights and civil liberties guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution; and
 - (b) What specific, affirmative measures will be implemented to safeguard the public from each of the potential disparate and adverse impacts identified pursuant to Section 1(E)(5)(a).
- (F) A Surveillance Use Policy submitted pursuant to Section 1(B) shall be a publicly-released, legally enforceable written policy governing the municipal entity's use of the surveillance technology that, at a minimum, includes and addresses the following:
- (1) Purpose: What specific purpose(s) that the surveillance technology is intended to advance.
 - (2) Authorized Use: What specific surveillance technology uses is authorization being sought for, and:
 - (a) Whether the surveillance technology will be operated continuously or used only under specific circumstances;
 - (b) Whether the surveillance technology will be installed permanently or temporarily;
 - (c) Whether the surveillance technology will be uniformly deployed or targeted throughout the city, and, if not, what factors will be used to determine where the technology is deployed or targeted;
 - (d) What rules will govern and what processes will be required prior to each use of the surveillance technology, including but not limited to:
 - (i) For each authorized use enumerated pursuant to Section 2(F)(2):
 - a. What existing legal standard must be met before the technology is used, or, where such a standard does not currently exist, what is the proposed standard to be followed;
 - b. Whether a judicial warrant is required; and
 - c. What information must be included in any warrant or court authorization granting permission to use the device;
 - (e) What potential capabilities and uses of the surveillance technology will be prohibited, such as the warrantless surveillance of public events and gatherings;
 - (f) The extent to which, and how the surveillance technology will be used to monitor persons in real time, as data is being captured;
 - (g) Whether the surveillance technology will be used to investigate (i) violent crimes, (ii) non-violent crimes, (iii) felonies, (iv) misdemeanors, and (v) other legal violations and/or infractions not classified as felonies or misdemeanors; and
 - (h) The extent to which, how, and under what circumstances retained surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology will be analyzed or reviewed.
 - (3) Data Collection:
 - (a) What types of surveillance data are capable of being collected, captured, recorded, intercepted, or retained by the surveillance technology.

- (b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and
 - (c) How, consistent with Section 1(F)(7)(f), inadvertently collected data identified in Section 1(F)(3)(b) will be expeditiously identified and deleted.
- (4) Database Reliance: Where applicable, what databases will the technology rely upon to make subject identifications.
- (5) Data Access:
- (a) Under what circumstances will an individual will be allowed to request access to surveillance data, who will be responsible for authorizing access to the surveillance data, what rules and processes must be followed prior to accessing or interacting with the surveillance data, and what are the acceptable grounds for requesting access to the surveillance data;
 - (b) What type of viewer's log or other comparable method will be used to track viewings of any surveillance data and what information will it track;
 - (c) A description of what individuals will have the authority to obtain copies of the surveillance data and what procedures will be put in place to prevent the unauthorized distribution of the copied surveillance data.
- (6) Data Protection: What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.
- (7) Data Retention: What rules and procedures will govern the retention of surveillance data, including those governing:
- (a) For what time period, if any, surveillance data will be retained. Such information shall include a statement as to why the designated retention period is appropriate in light of the purpose(s) enumerated in the Surveillance Use Policy;
 - (b) What specific conditions must be met to retain surveillance data beyond the retention period stated in Section 1(F)(7)(a);
 - (c) By what process will surveillance data be regularly deleted after the retention period stated in Section 1(F)(7)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained beyond the retention period;
 - (d) What methods will be used to store surveillance data, including how will the surveillance data is to be labeled or indexed;
 - (e) What methods will be used to identify surveillance data that has been improperly collected and/or retained, and how will that data, including any copies thereof, be expeditiously destroyed once it is identified;
 - (f) What process will be put into place so individuals who claim surveillance data pertaining to them has been improperly collected and/or retained can petition to have their claims reviewed and how will improperly collected or retained surveillance data, including any copies thereof, be expeditiously destroyed once it is identified;
 - (g) What technological system will be used to store the surveillance data, and who will maintain custody and control over the system and its surveillance data; and
 - (h) What unit or individuals will be responsible for ensuring compliance with Section 1(F)(7), and when and how compliance audits will be conducted.
- (8) Public Access: How will surveillance data be accessible to members of the public, how does the municipal entity interpret the applicability of, and intend to comply with Wis. Stat. §§ 19.31 *et seq.*, and what steps will be taken to protect individual privacy.

- (9) Target/Defendant Access: How, to what extent, and when will surveillance data, in accordance with applicable law, be accessible to targets of criminal or civil investigations, criminal or civil defendants, and their attorneys.
- (10) Surveillance Data Sharing: If a municipal entity intends to share access to the surveillance technology or the surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, it shall detail:
 - (a) How it will require that the collection, retention, and storage of surveillance data be conducted in compliance with the principles set forth in 28 C.F.R. Part 23.
 - (b) Which governmental agencies, departments, bureaus, divisions, or units will be approved for sharing;
 - (c) How such sharing is required for the stated purpose and use of the surveillance technology;
 - (d) How it will ensure the entity receiving the surveillance data complies with the applicable Surveillance Use Policy and does not further disclose the surveillance data to unauthorized persons and entities; and
 - (e) What processes will be used to seek approval of future surveillance data sharing agreements from the municipal entity and Common Council.
- (11) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.
- (12) Training: What training, including training materials, will be required for any individual authorized to use the surveillance technology or to access surveillance data.
- (13) Maintenance: How will the security and integrity of the surveillance technology be maintained and how will the municipal entity or lead agent present any substantive changes in the surveillance technology's functionality to the Common Council for approval.
- (14) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including what internal personnel will be assigned to ensure compliance with the policy, what independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for violations of the policy.
- (15) Complaints: What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and what internal personnel will be assigned to receive, register, track, and respond to such communications.
- (16) The Surveillance Use Policy shall include a disclaimer that the Surveillance Use Policy shall be considered a draft proposal until such time as it is approved, with or without modifications, pursuant to a vote of the Common Council.

Section 3. No later than one hundred twenty (120) days following the effective date of this Policy, any municipal entity seeking to continue the use of any surveillance technology it was in use prior to the effective date of this Policy must commence a Common Council approval process in accordance with Section 2(A)(3). If the Common Council has not approved the continuing use of the surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy re submitted pursuant to Section 2(B), within one hundred eighty (180) days of their submission to the Common Council, the municipal entity shall cease its use of the surveillance technology until such time as Common Council approval is obtained in accordance with this Policy.

Section 4. If more than one municipal entity will have access to the surveillance technology or surveillance data, a lead municipal entity shall be identified. The lead municipal entity shall be responsible for maintaining the surveillance technology and ensuring compliance with all related laws,

regulations and protocols. If the lead municipal entity intends to delegate any related responsibilities to other governmental agencies, departments, bureaus, divisions, units, or personnel, these responsibilities and associated entities and/or personnel shall be clearly identified.

Section 5. The Common Council shall only approve a request to fund, acquire, or use a surveillance technology if it determines the benefits of the surveillance technology outweigh its costs, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or group. To assist the public in participating in such an analysis, all approved Surveillance Impacts Reports and Surveillance Use Policies shall be made available to the public, at a designated page on the relevant municipal entity's public website, for as long as the related surveillance technology remains in use. An approval for the funding, acquisition and/or use of a surveillance technology by the Common Council, where the risk of potential adverse impacts on civil rights or civil liberties have been identified in the Surveillance Impact Report pursuant to Section 2(D)(5)(a), shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impacts exists and must be proactively avoided.

Section 6.

(A) A municipal entity that obtains approval for the use of surveillance technology must submit to the Common Council an Annual Surveillance Report for each specific surveillance technology used by the municipal entity within twelve (12) months of Common Council approval, and annually thereafter on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

- (1) A summary of how the surveillance technology was used;
- (2) Whether and how often collected surveillance data was shared with any external persons or entities, the name(s) of any recipient person or entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
- (3) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau. For each census tract, the municipal entity shall report how many individual days the surveillance technology was deployed and what percentage of those daily-reported deployments were subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (4) Where applicable, a breakdown of how many times the surveillance technology was used to investigate potential or actual (A) violent crimes, (B) non-violent crimes, (C) felonies, (D) misdemeanors, and (E) other legal violations and/or infractions not classified as felonies or misdemeanors
- (5) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology was used to monitor Internet activity, including but not limited to social media accounts, the number of people affected, and what percentage of the reported monitoring was subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (6) Where applicable, a breakdown of what the surveillance technology was installed upon, including but not limited to on what vehicles or structures it was placed;
- (7) Where applicable, a breakdown of what hardware surveillance technology software was installed upon;
- (8) Where applicable, a breakdown of what databases the surveillance technology was applied to, including the frequency thereof;
- (9) A summary of complaints or concerns that were received about the surveillance technology;

- (10)The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
 - (11)An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public’s civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendment to the United States Constitution;
 - (12)Statistics and information about public records act requests, including response rates; and
 - (13)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.
- (B) Based upon information provided in the Annual Surveillance Report, the Common Council shall determine whether the benefits of the surveillance technology outweigh its costs and whether the public’s civil liberties and civil rights have been adequately protected and safeguarded. If the benefits do not outweigh the costs or civil rights and civil liberties have not been adequately protected and safeguarded, the Common Council shall direct the use of the surveillance technology cease or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

Section 7. Not later than April 15 of each year, the Common Council or its appointed designee shall release a public report, in paper and electronic form, containing the following information for the proceeding calendar year:

- (A) The number of requests for approval submitted to the Common Council under this Policy for the funding, acquisition, or new use of surveillance technology;
- (B) The number of times the Common Council approved requests submitted under this Policy for the funding, acquisition, or new use of surveillance technology;
- (C) The number of times the Common Council rejected requests submitted under this Policy for the funding, acquisition, or new use of surveillance technology;
- (D) The number of times the Common Council requested modifications be made to Surveillance Impact Reports and Surveillance Use Policies before approving the funding, acquisition, or new use of surveillance technology; and
- (E) All Annual Surveillance Reports submitted pursuant to Section 6.

Section 8.

- (A) Any violation of this Policy, including but not limited to funding, acquiring, or utilizing surveillance technology that has not been approved pursuant to this Policy or utilizing surveillance technology in a manner or for a purpose that has not been approved pursuant to this Policy, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, writ of mandate, or evidence suppression in any court of competent jurisdiction to enforce this Policy.
- (B) A court shall award costs and reasonable attorneys’ fees to the plaintiff who is the prevailing party in an action brought to enforce this Policy.
- (C) Municipal employees or agents, except in response to a declared municipal, state, or federal state of emergency, shall not use any surveillance technology except in a manner consistent with policies approved pursuant to the terms of this Policy, and may in no circumstances utilize surveillance technology in a manner which is discriminatory, viewpoint-based, or violates the City Ordinances, State Constitution, or United States Constitution. Any municipal employee who violates the provisions of this Policy, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For municipal employees who are represented under the terms of a collective bargaining agreement, this Policy prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the

collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

(D) Whistleblower protections.

(1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:

- (a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or Common Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Policy; or
- (b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Policy.

(2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Policy.

(3) Any employee or applicant who is injured by a violation of Section 8(D)(1) may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

(E) In addition, any person who:

- (1) Knowingly violates this Policy shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$2,500 per violation, imprisonment of not more than six months, or both.
- (2) Recklessly violates this Policy shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$1,000 per violation.

Section 9. It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Policy, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Policy shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Policy.

Section 10. It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that facilitates the receipt of surveillance data from, or provision of surveillance data to any non-governmental entity in exchange for any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts. Any contracts or agreements signed prior to the enactment of this Policy that violate this section shall be terminated as soon as is legally permissible.

Section 11. The provisions in this Policy are severable. If any part of provision of this Policy, or the application of this Policy to any person or circumstance, is held invalid, the remainder of this Policy, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. This Policy shall take effect on [DATE].

ORDINANCE NO. NS-300.897

**AN ORDINANCE OF THE BOARD OF SUPERVISORS
OF THE COUNTY OF SANTA CLARA
ADDING DIVISION A40 OF THE COUNTY OF SANTA CLARA ORDINANCE
CODE RELATING TO SURVEILLANCE-TECHNOLOGY AND COMMUNITY-
SAFETY**

Summary

This Ordinance adds Division A40 relating to the Board-approval requirement for the acquisition and operation of surveillance equipment, and for a related surveillance use policy.

**THE BOARD OF SUPERVISORS OF THE COUNTY OF SANTA CLARA
ORDAINS AS FOLLOWS:**

Title A of the Ordinance Code of the County of Santa Clara is hereby amended by adding a new Division to be numbered and titled and to read as follows:

**DIVISION A40
SURVEILLANCE-TECHNOLOGY AND COMMUNITY-SAFETY**

Sec. A40-1. Findings.

The California Constitution provides that all people have an inalienable right to privacy, which is just as explicitly described in the California Constitution as the right to enjoy and defend life and liberty; the right to acquire, possess, and protect property; and the right to pursue and obtain safety and happiness. State and federal courts, including both the California Supreme Court and the United States Supreme Court, have affirmed individuals' fundamental right to privacy, and the Board finds that protecting and safeguarding this right is a vital part of its duties. Acknowledging the significance of protecting the privacy of County citizens, the Board finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes. To balance the public's right to privacy with the need to promote and ensure community safety, the Board finds that any decision to use surveillance technology must be judiciously balanced with an assessment of the costs to the County and the protection of privacy, civil liberties and civil rights. The Board finds that proper transparency, oversight, and accountability are fundamental to minimizing the risks posed by surveillance technologies. The Board finds it essential to have an informed public

discussion before deploying surveillance technology, and that safeguards should be in place to address potential privacy, civil liberties, and civil rights issues before any new surveillance technology is deployed. The Board finds that if surveillance technology is acquired and deployed, there must be continued oversight and regular evaluation to ensure that safeguards are being followed and that the Board is assessing the surveillance technology's benefits and potential benefits in addition to its costs and potential costs.

Sec. A40-2. Board Approval Requirement for Acquisition and Operation of Surveillance Equipment, and for Related Surveillance Use Policy

- (A) County Departments Other than the Sheriff's Office and District Attorney's Office. Each County department other than the Sheriff's Office and District Attorney's Office must obtain Board approval at a properly-noticed public meeting, on the regular (non-consent) calendar, before any of the following:
- (1) Seeking funds for surveillance technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;
 - (2) Acquiring new surveillance technology, including but not limited to procuring that technology without the exchange of monies or other consideration;
 - (3) Using surveillance technology for a purpose, in a manner, or in a location not previously approved by the Board; or
 - (4) Entering into an agreement with a non-County entity to acquire, share, or otherwise use surveillance technology or the information it provides.

Those County departments must also obtain Board approval of a Surveillance Use Policy at a properly-noticed public meeting, on the regular (non-consent) calendar, before engaging in any of the activities described in subsections (A)(2), (A)(3), and (A)(4).

- (B) Sheriff's Office and District Attorney's Office. Other than with respect to surveillance technology limited to use in law enforcement investigations and prosecutions as specifically defined in Sec. A40-9 of this Division, and subject to Sec. A40-2(C) below, the Sheriff's Office and District Attorney's Office must notify the Board, and obtain Board approval, at a properly-noticed public meeting, on the regular (non-consent) calendar, before any of the following:
- (1) Seeking funds for surveillance technology, including but not limited to, applying for a grant, or accepting state or federal funds, or in-kind or other donations;

- (2) Acquiring new surveillance technology, including but not limited to procuring that technology without the exchange of monies or other consideration;
- (3) Using surveillance technology for a purpose, in a manner, or in a location not previously approved by the Board; or
- (4) Entering into an agreement with a non-County entity to acquire, share, or otherwise use surveillance technology.

The Sheriff's Office and the District Attorney's Office must also notify the Board, and obtain Board approval, of a Surveillance Use Policy at a properly-noticed public meeting, on the regular (non-consent) calendar, before engaging in any of the activities described in subsections (B)(2), (B)(3), and (B)(4).

- (C) In enacting this Division, the Board is not limiting its rights under Government Code section 25303, including without limitation, its right to supervise the official conduct of all county officers, to require reports, or to exercise budgetary authority over the district attorney and sheriff.
- (D) Consistent with California Government Code section 25303, however, in receiving notification and approving or denying the actions in subsections (B)(1), (B)(2), (B)(3), and (B)(4), and approving, and/or denying any Surveillance Use Policy, the Board shall not "obstruct the investigative function of the sheriff of the county nor shall it obstruct the investigative and prosecutorial function of the district attorney."
- (E) To the extent the Board or a court of law determines that approving or denying the actions in subsections (B)(1), (B)(2), (B)(3), or (B)(4), or approving or denying the Surveillance Use Policy would unlawfully "obstruct" the applicable function of the sheriff or district attorney under Government Code section 25303, the Board shall simply receive and discuss notification from the Sheriff's Office or District Attorney's Office regarding subsections (B)(1), (B)(2), (B)(3), or B(4) and receive and discuss the applicable Surveillance Use Policy at a properly-noticed public meeting, on the regular (non-consent) calendar.

Sec. A40-3. Information Required

Unless it is not reasonably possible or feasible to do so (e.g., exigent circumstances, a natural disaster, or technological problems prevent it, etc.), the County department seeking approval under Section A40-2 of this Division must submit to the Board an Anticipated Surveillance Impact Report and a proposed Surveillance Use Policy before the public meeting. The County shall publicly release printed and online copies of

the Anticipated Surveillance Impact Report and proposed Surveillance Use Policy before the public meeting.

Sec. A40-4. Determination by Board that Benefits Outweigh Costs and Concerns

Before approving any action described in Section A40-2(A) and A40-2(B) of this Division, the Board shall assess whether the benefits to the impacted County department(s) and the community of the surveillance technology outweigh the costs—including both the financial costs and reasonable concerns about the impact on and safeguards for privacy, civil liberties, and civil rights.

Sec. A40-5. Compliance for Existing Surveillance Technologies

Each County department possessing or using surveillance technology before the effective date of this Ordinance shall submit a proposed Surveillance Use Policy for that surveillance technology no later than one-hundred eighty (180) days following the effective date of this Ordinance, for review and approval by the Board at a properly-noticed public meeting, on the regular (non-consent) calendar. If a County department is unable to meet this 180-day timeline, the Department may notify the Board in writing of the department's request to extend this period and the reasons for that request. The Board may grant County departments extensions of up to 90 days beyond the 180-day timeline to submit a proposed Surveillance Use Policy.

Consistent with California Government Code section 25303, in approving or denying a Surveillance Use Policy from the Sheriff's Office or the District Attorney's Office, the Board shall not "obstruct the investigative function of the sheriff of the county nor shall it obstruct the investigative and prosecutorial function of the district attorney." To the extent the Board or a court of law determines that approving or denying the Surveillance Use Policy would unlawfully "obstruct" under Government Code section 25303, the Board shall simply receive and discuss the applicable Surveillance Use Policy at a properly-noticed public meeting, on the regular (non-consent) calendar.

Sec. A40-6. Oversight Following Board Approval

- (A) A County department that obtained approval for the use of surveillance technology or the information it provides under Section A40-2(A)(3) or A40-2(A)(4), A40-2(B)(3), A40-2(B)(4), or A40-5 of this Division, must submit an Annual Surveillance Report within twelve (12) months of Board approval, and annually thereafter on or before November 1. Similarly, if the Board received but did not approve a Surveillance Use Policy from the Sheriff's Office or District Attorney's office because of limitations of the Board's authority under Government Code

section 25303, the Sheriff's Office or District Attorney's Office, as applicable, must still submit an Annual Surveillance Use Report within twelve (12) months of the Board's receipt of the Surveillance Use Policy, and annually thereafter on or before November 1.

- (B) Based upon information provided in the Annual Surveillance Report, the Board shall determine whether the benefits to the impacted County department(s) and the community of the surveillance technology outweigh the costs and whether reasonable safeguards exist to address reasonable concerns regarding privacy, civil liberties, and civil rights impacted by deployment of the surveillance technology. If the benefits or reasonably anticipated benefits do not outweigh the costs or civil liberties or civil rights are not reasonably safeguarded, the Board shall consider (1) directing that the use of the surveillance technology cease; (2) requiring modifications to the Surveillance Use Policy that are designed to address the Board's concerns; and/or (3) directing a report-back from the department regarding steps taken to address the Board's concerns.
- (C) No later than January 15 of each fiscal year, the Board shall hold a public meeting, with Annual Surveillance Reports agendaized on the regular (non-consent) calendar, and publicly release a report that includes the following information for the prior year:
 - (1) A summary of all requests for Board approval and all notifications and Surveillance Use Policies received by the Board pursuant to Section A40-2 or Section A40-5 of this Division, including whether the Board approved, rejected, or received the proposal or notification, and/or required changes to a proposed Surveillance Use Policy before approval; and,
 - (2) All Annual Surveillance Reports submitted.

Sec. A40-7. Definitions

The following definitions apply to this Division:

- (A) **"Annual Surveillance Report"** means a written report concerning specific surveillance technology that includes all of the following:
 - (1) A description of how the surveillance technology was used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct;

- (2) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure;
 - (3) A summary of community complaints or concerns about the surveillance technology;
 - (4) The results of any non-privileged internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
 - (5) Whether the surveillance technology has been effective at achieving its identified purpose;
 - (6) Statistics and information about public records act requests;
 - (7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.
- (B) **“County department”** means any County department with a recognized County budget unit.
- (C) **“Surveillance technology”** means any electronic device, system using an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site simulators, International Mobile Subscriber Identity (IMSI) trackers, Global Positioning System (GPS) technology, radio-frequency identification (RFID) technology, biometrics-identification technology, and facial-recognition technology.

For purposes of this Division, surveillance technology does not include standard word-processing software; information-technology-protection tools such as web-filtering; medical equipment used to diagnose, treat, or prevent disease or injury; Public Defender or District Attorney case-management databases; publicly available databases; or standard telephone-message equipment that stores the author of a document or the time a phone message was left on a County voicemail, for example.

For purposes of the acquisition and annual reporting requirements in this Division, surveillance technology also does not include County-owned cell phones with the

capacity to capture audio or video footage; or recording devices used exclusively with the express consent of everyone captured on the recording devices; but use of a County-owned cell phone or recording device for an illegal or unauthorized surveillance purpose violates this Division.

(D) “**Anticipated Surveillance Impact Report**” means a publicly-released written report including at a minimum the following:

- (1) Information describing the surveillance technology and how it works;
- (2) Information on the proposed purpose(s) for the surveillance technology;
- (3) The location(s) it may be deployed;
- (4) The potential impact(s) on civil liberties and privacy, and a description of whether there is a plan to address the impact(s); and,
- (5) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

(E) “**Surveillance Use Policy**” means a publicly-released policy for use of the surveillance technology, vetted through County Counsel and submitted to and approved by the Board at a properly-noticed public meeting on the regular (non-consent) calendar. The Surveillance Use Policy shall at a minimum specify the following:

- (1) Purpose: The specific purpose(s) for the surveillance technology.
- (2) Authorized Use: The uses that are authorized, the rules and processes required before that use, and the uses that are prohibited.
- (3) Data Collection: The information that can be collected by the surveillance technology.
- (4) Data Access: The individuals who can access or use the collected information, and the rules and processes required before access or use of the information.
- (5) Data Protection: The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms.
- (6) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason that retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the conditions that must be met to retain information beyond that period.
- (7) Public Access: If and how collected information can be accessed by members of the public, including criminal defendants.

- (8) Third-Party Data-Sharing: If and how other County or non-County entities can access or use the information, including any required justification and legal standard necessary to do so, and any obligation(s) imposed on the recipient of the information.
 - (9) Training: The training, if any, required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including whether there are training materials.
 - (10) Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including, but not limited to, identifying personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy.
- (F) **“Exigent circumstances”** means the County Sheriff’s Office or District Attorney’s Office’s good faith belief that an emergency involving danger of death or serious physical injury to any person requires use of the surveillance technology or the information it provides.

Sec. A40-8. Severability

The provisions of this Division are severable. If any section, subsection, paragraph, sentence, clause or phrase of this Division is for any reason held unconstitutional or invalid, the remaining parts of this Division shall remain fully effective. If the application of any part of this Division to any person or circumstance is held invalid, the application of that part of this Division shall not be affected regarding other persons or circumstances.

Sec. A40-9. Temporary Acquisition and Use of Surveillance Equipment Related to Law Enforcement Investigations and Prosecutions

Notwithstanding the provisions of this Division, the County Sheriff’s Office and District Attorney’s Office may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this ordinance before that acquisition or use unless a State law or federal law preempts or conflicts with this exigent-circumstances exception in any manner (e.g., Civil Code sections 1798.90.5, et seq.; and Government Code section 53166). However, if the Sheriff’s Office or District Attorney’s Office acquires or uses surveillance technology in exigent circumstances under this subdivision, that Office must (1) report that acquisition or use to the Board of Supervisors in writing within 90 days following the end of those circumstances; (2) submit a proposed Surveillance Use Policy to the Board regarding that

surveillance technology within 90 days following the end of those circumstances; and (3) include that surveillance technology in the department's next Annual Surveillance Report to the Board following the end of those circumstances. If the Sheriff's Office or District Attorney's Office is unable to meet the 90-day timeline to submit a proposed Surveillance Use Policy to the Board, that Office may notify the Board in writing of the Office's request to extend this period and the reasons for that request. The Board may grant extensions of up to 90 days beyond the original 90-day timeline to submit a proposed Surveillance Use Policy.

Sec. A40-10. Enforcement

This Division does not confer any rights upon any person or entity other than the Board of Supervisors or its designee to seek the cancellation or suspension of a County contract. This Division does not confer a private right of action upon any person or entity to seek injunctive relief against the County or any individual unless that person or entity has first provided written notice to the County Executive and the Board of Supervisors, by serving the Clerk of the Board, regarding the specific alleged violation of this Division; and has provided the County Executive and the Board with at least 90 days to investigate and achieve compliance regarding any alleged violation. If the specific alleged violation is not remedied within 90 days of that written notice, a person or entity may seek injunctive relief in a court of competent jurisdiction. If it is shown that the violation is the result of arbitrary or capricious action or conduct by the County or an officer thereof in his or her official capacity, the prevailing complainant in an action for injunctive relief may collect from the County reasonable attorney's fees—computed at one hundred dollars (\$100) per hour, but not to exceed seven thousand five hundred dollars (\$7,500)—if he or she is personally obligated to pay the fees. However, a prevailing complainant may not recover attorney's fees under this section and under Government Code section 800 for the same arbitrary or capricious action or conduct.

Sec. A40-11. Retaliation is a Ground for Discipline

It shall be a ground for disciplinary action for a County employee to retaliate against any individual who makes a good-faith complaint to the County Executive's Office that there has been a failure to comply with any part of this Division.

Sec. A40-12. Intentional Misuse of Surveillance Equipment is a Misdemeanor

It shall be a misdemeanor to intentionally use County-owned surveillance technology (1) for a purpose or in a manner that is specifically prohibited in a Board-approved Surveillance Use Policy, or (2) without complying with the terms of this Division with respect to that County-owned surveillance technology. Unless otherwise

prohibited by law, either the District Attorney or County Counsel may prosecute a violation of this Division.

PASSED AND ADOPTED by the Board of Supervisors of the County of Santa Clara, State of California, on **JUN 21 2016** by the following vote:

AYES: **CHAVEZ, CORTESE, SIMITIAN, WASSERMAN, YEAGER**

NOES: **NONE**


ABSENT: **NONE**

ABSTAIN: **NONE**



DAVE CORTESE, President
Board of Supervisors

ATTEST:



MEGAN DOYLE
Clerk of the Board of Supervisors

APPROVED AS TO FORM AND LEGALITY:



ROBERT M. COELHO
Assistant County Counsel

1317046

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

INTRODUCED BY COUNCILMEMBER [IF APPLICABLE]

THE SURVEILLANCE AND COMMUNITY SAFETY ORDINANCE

Whereas, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology; and

Whereas, the City Council finds that, while surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

Whereas, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes, while acknowledging the significance of protecting the privacy of citizens; and

Whereas, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

Whereas, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

Whereas, the City Council finds that any and all decisions regarding if and how surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight; and

Whereas, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

Whereas, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to; now, therefore

THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. City Council Approval Requirement

- 1) A City entity shall notify the Chair of the Privacy Advisory Commission prior to the entity:
 - a) Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - b) Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

Upon notification by the entity, the Chair shall place the item on the agenda at the next meeting for discussion and possible action. At this meeting, the entity shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action the entity intends to take. The Privacy Advisory Commission may vote its approval to proceed, object to the proposal, recommend that the entity modify its proposal, or take no action. Failure by the Privacy Advisory Commission to act shall not prohibit the entity from proceeding. Opposition to the action by the Privacy Advisory Commission shall not prohibit the entity from proceeding. The City entity is still bound by subsection (2) regardless of the action taken by the Privacy Advisory Commission under this subsection.

- 2) A City entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public hearing prior to any of the following:
 - a) Accepting state or federal funds or in-kind or other donations for surveillance technology;
 - b) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
 - c) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council; or
 - d) Entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

- 3) A City entity must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (2)(a)-(d).

Section 3. Information Required

- 1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.

- a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting.
- b) The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose modifications to the City entity and/or City Council in writing.
- c) Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the City entity to proceed to the City Council for approval of the item.

- 2) After receiving the recommendation of the Privacy Advisory Commission, the City Council shall provide the public notice that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

- 3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 4. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 5. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy for each surveillance technology, in compliance with Section 3 (1) (a-c).

- a) Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, each City entity shall present to the Privacy Advisory Commission a list of surveillance technology already possessed or used by the City entity.
- b) The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
- c) Within sixty (60) days of the Privacy Advisory Commission's action in b), each City entity shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter every month until the list is exhausted.
- d) Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following City Council Approval

1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.

- a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Privacy Advisory Commission for its review.
- b) The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.

2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.

- 3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
- a) A summary of all requests for City Council approval pursuant to Section 2 or Section 5 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
 - b) All Surveillance Reports submitted.

Section 7. Definitions

The following definitions apply to this Ordinance:

- 1) “Surveillance Report” means a written report concerning a specific surveillance technology that includes all the following:
- a) A description of how the surveillance technology was used, including the quantity of data gathered or analyzed by the technology;
 - b) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau;
 - e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public’s civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
 - f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
 - g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - i) Statistics and information about public records act requests, including response rates;

- j) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
- k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2) “City entity” means any department, bureau, division, or unit of the City of Oakland.

3) “Surveillance technology” means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.

- a) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 7(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.

4) “Surveillance Impact Report” means a publicly-released written report including at a minimum the following:

- a) **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
- b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
- c) **Location:** The location(s) it may be deployed and crime statistics for any location(s);
- d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm. In addition, identify specific, affirmative

measures that will be implemented to safeguard the public from each such impacts;

- e) **Data Sources:** A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including “open source” data;
- f) **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
- g) **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
- h) **Third-Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
- i) **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
- j) **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

5) "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:

- a) **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
- b) **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;
- c) **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including “open source” data;
- d) **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
- f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

- g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
- h) **Third-Party Data Sharing:** If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;
- j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section 8. Enforcement

- 1) Any violation of Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), Resolution No. xxxxx (Cell Site Simulator Use Policy adopted xxxxxx, 2017), this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective City agency, the City of Oakland, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third-party with possession, custody, or control of data subject to this Ordinance.
- 2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars (\$1,000) or one hundred dollars (\$100) per day for each day of violation, whichever is greater) and punitive damages.
- 3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).

4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding one thousand dollars (\$1,000) per violation.

Section 9. Secrecy of Surveillance Technology

It shall be unlawful for the City of Oakland or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Ordinance shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Ordinance.

Section 10. Whistleblower Protections

- 1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:
 - a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
 - b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.
- 2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.
- 3) Any employee or applicant who is injured by a violation of Section 10 may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

Section 11. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such

part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL WASHINGTON, GALLO, GUILLÉN, KALB, KAPLAN, REID AND
PRESIDENT GIBSON MCELHANEY

NOES –

ABSENT –

ABSTENTION –

ATTEST:

LATONDA SIMMONS
City Clerk and Clerk of the Council of the
City of Oakland, California

An Act To Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology

Section 1: For the purposes of this Act:

- (A) “Discriminatory” shall mean (1) disparate treatment of any individual(s) because of any real or perceived traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the Commonwealth of Massachusetts, or the Charter or ^[A1]any law of the City of Cambridge^[A2], or because of their association with such individual(s), or (2) disparate impact on any such individual(s) having traits, characteristics, or status as described in subsection (1).
- (B) “Disparate impact” shall mean an adverse effect that is disproportionately experienced by individual(s) having any traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the Commonwealth of Massachusetts^[A3], or the Charte or any law of the City of Cambridge^[A4] than by similarly situated individual(s) not having such traits, characteristics, or status.
- (C) “Municipal entity” shall mean any municipal government, agency, department, bureau, division, or unit of this City.
- (D) “Surveillance data” shall mean any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.
- (E) “Surveillance technology” shall mean any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.
- (1) “Surveillance technology” includes, but is not limited to: (a) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (b) automatic license plate readers; (c) electronic toll readers; (d) closed-circuit television cameras; (e) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (f) mobile DNA capture technology; (g) gunshot detection and location hardware and services; (h) x-ray vans; (i) video and audio monitoring and/or recording technology, such as surveillance cameras and wearable body cameras; (j) surveillance enabled or capable lightbulbs or light fixtures; (k) tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; (l) social media monitoring software; (m) through-the-wall radar or

similar imaging technology, (n) passive scanners of radio networks, (o) long-range Bluetooth and other wireless-scanning devices, (p) radio-frequency I.D. (RFID) scanners, and (q) software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software. The enumeration of surveillance technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by any municipal entity.

- (2) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 1(E): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or surveillance-related functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) municipal agency databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; and (f) manually-operated technological devices that are used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems.

- (F) “Viewpoint-based” shall mean targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

Section 2.

(A) A municipal entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide online, written and oral testimony, prior to engaging in any of the following:

- (1) Seeking funds for new surveillance technology, including but not limited to applying for a grant, or soliciting or accepting state or federal funds or in-kind or other donations;
- (2) Acquiring or borrowing new surveillance technology, whether or not that acquisition is made through the exchange of monies or other consideration;
- (3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the City Council in accordance with this Act; or

- (4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use surveillance technology or surveillance data.
- (B) As a part of the process of seeking City Council approval, pursuant to Section 2(A), to fund, acquire, or use surveillance technology or to enter into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the City Council a Surveillance Impact Report and Surveillance Use Policy concerning the technology at issue.
- (1) Upon submitting a Surveillance Impact Report and Surveillance Use Policy to the City Council pursuant to Section 2(B), the municipal agency shall make both documents available to the public on its public website.
 - (2) Within ten (10) days of receiving a surveillance technology approval request pursuant to Section 2(A), the City Council shall make the related Surveillance Impact Report and Surveillance Use Policy publicly available, in print and on its public website.
 - (3) Within twenty-one (21) days of submitting a Surveillance Impact Report and Surveillance Use Policy pursuant to Section 2(B), the municipal agency shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the surveillance technology approval request the municipal entity submitted to the City Council.
 - (4) The public City Council hearing required pursuant to Section 2(A) may not be held until forty-five (45) days after the Surveillance Impact Report and Surveillance Use Policy are submitted pursuant to Section 2(B).
 - (5) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public online as long as the municipal entity continues to utilize the surveillance technology in accordance with a surveillance technology approval request submitted pursuant to Section 2(A).
- (C) No use of surveillance technology by a municipal entity pursuant to Section 2(A) shall be permitted without the City Council's express approval of the related Surveillance Impact Report and Surveillance Use Policy submitted by the municipal entity pursuant to Section 2(B).
- (D) Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy, the City Council may request revisions be made by the submitting municipal entity. Revisions should be requested where any inadequacies are perceived to exist within a Surveillance Use Policy or Surveillance Impact Report, especially with respect to the protection of civil rights and civil liberties and the avoidance of discriminatory and viewpoint-based uses, deployments, and impacts.

- (1) Any requested revisions to a Surveillance Impact Report or Surveillance Use Policy made by a member, employee, or committee of the City Council, and the responses thereto, shall be publicly released by the City Council, in print and on its public website, at least thirty (30) days prior to any City Council vote to approve or reject a request made by a municipal entity pursuant to Section 2(A).
 - (2) In the event revisions are made to the originally submitted Surveillance Impact Report or Surveillance Use Policy, prior to voting to approve or reject the revised Surveillance Impact Report or Surveillance Use Policy, the City Council shall hold another properly-noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide written and oral testimony on the revised Surveillance Impact Report and/or Surveillance Use Policy. A copy of the revised Surveillance Impact Report and/or Surveillance Use Policy shall be publicly released by the City Council, in print and on its public website, at least thirty (30) days prior to such a public hearing.
- (E) A Surveillance Impact Report submitted pursuant to Section 2(B) shall be a publicly-released, legally enforceable written report that includes, at a minimum, the following:
- (1) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - (2) Information on the proposed purpose(s) for the surveillance technology;
 - (3) If the surveillance technology will not be uniformly deployed or targeted throughout the city:
 - (a) What factors will be used to determine where the technology is deployed or targeted; and
 - (b) Based upon those factors enumerated pursuant to Section 2(E)(3)(a), what geographical location(s) are anticipated to receive a disproportionately high level of deployment or targeting;
 - (4) The fiscal impact of the surveillance technology, including but not limited to:
 - (a) Initial acquisition costs;
 - (b) Ongoing operational costs such as personnel, legal compliance, use auditing, data retention and security costs;
 - (c) Any cost savings that would be achieved through the use of the technology; and
 - (d) Any current or potential sources of funding; and
 - (5) An assessment identifying with specificity:
 - (a) Any potential impacts the surveillance technology, if deployed, might have on civil liberties and civil rights, including but not limited to:

- (i) Potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a discriminatory manner;
 - (ii) Potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a viewpoint-based manner;
 - (iii) Potential disparate or adverse impacts on any communities or groups if the surveillance technology is operated using intentionally or inadvertently biased algorithms;
 - (iv) Potential adverse impacts on privacy and anonymity rights;
 - (v) Other potential adverse impacts on the civil rights and civil liberties guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution; [A5] and
- (b) What specific, affirmative measures will be implemented to safeguard the public from each of the potential disparate and adverse impacts identified pursuant to Section 2(E)(5)(a).
- (6) A disclaimer that the Surveillance Impact Report shall be considered a draft proposal until such time as it is approved, with or without modifications, pursuant to a vote of the City Council.
- (F) A Surveillance Use Policy submitted pursuant to Section 2(B) shall be a publicly-released, legally enforceable written policy governing the municipal entity's use of the surveillance technology that, at a minimum, includes and addresses the following:
- (1) Purpose: What specific purpose(s) that the surveillance technology is intended to advance.
 - (2) Authorized Use: What specific surveillance technology use(s) is authorization being sought for, and:
 - (a) Whether the surveillance technology will be operated continuously or used only under specific circumstances;
 - (b) Whether the surveillance technology will be installed permanently or temporarily;
 - (c) Whether the surveillance technology will be uniformly deployed or targeted throughout the city, and, if not, what factors will be used to determine where the technology is deployed or targeted;
 - (d) What rules will govern, and what processes will be required prior to each use of the surveillance technology, including but not limited to:
 - (i) For each authorized use enumerated pursuant to Section 2(F)(2):

- a. What existing legal standard must be met before the technology is used, or, where such a standard does not currently exist, what is the proposed standard to be followed;
 - b. Whether a judicial warrant is required; and
 - c. What information must be included in any warrant or court authorization granting permission to use the device;
- (e) What potential capabilities and uses of the surveillance technology will be prohibited, such as the warrantless surveillance of public events and gatherings;
 - (f) The extent to which, and how the surveillance technology will be used to monitor persons in real time, as data is being captured;
 - (g) Whether the surveillance technology will be used to investigate (i) violent crimes, (ii) non-violent crimes, (iii) felonies, (iv) misdemeanors, and (v) other legal or code violations, infractions not classified as felonies or misdemeanors, unlawful activity, activities or patterns considered to be indicators of potential future involvement in criminal activity, or perceived or actual gang or other group affiliations; and
 - (h) The extent to which, how, and under what circumstances retained surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology will be analyzed or reviewed.

(3) Data Collection:

- (a) What types of surveillance data are capable of being collected, captured, recorded, intercepted, or retained by the surveillance technology.
- (b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and
- (c) How, consistent with Section 2(F)(7)(f), inadvertently collected data identified in Section 2(F)(3)(b) will be expeditiously identified and deleted.

(4) Database Reliance: Where applicable, what databases the technology will rely upon to make subject identifications.

(5) Data Access:

- (a) Under what circumstances an individual will be allowed to request access to surveillance data, who will be responsible for authorizing access to the surveillance data, what rules and processes must be followed prior to accessing or interacting with the surveillance data, and what the acceptable grounds are for requesting access to the surveillance data;

- (b) What type of viewer's log or other comparable method will be used to track viewings of any surveillance data and what information it will track;
 - (c) A description of what categories of personnel will have the authority to obtain copies of the surveillance data; and
 - (d) What procedures will be put in place to prevent the unauthorized distribution of the copied surveillance data.
- (6) Data Protection: What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.
- (7) Data Retention: What rules and procedures will govern the retention of surveillance data, including those governing:
- (a) For what time period, if any, surveillance data will be retained. Such information shall include a statement as to why the designated retention period is appropriate in light of the purpose(s) enumerated in the Surveillance Use Policy;
 - (b) What specific conditions must be met to retain surveillance data beyond the retention period stated in Section 2(F)(7)(a);
 - (c) By what process surveillance data will be regularly deleted after the retention period stated in Section 2(F)(7)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained beyond the retention period;
 - (d) What methods will be used to store surveillance data, including how will the surveillance data is to be labeled or indexed;
 - (e) What methods will be used to identify surveillance data that has been improperly collected and/or retained, and how that data, including any copies thereof, will be expeditiously destroyed once it is identified;
 - (f) What process will be put into place so individuals who claim surveillance data pertaining to them has been improperly collected and/or retained can petition to have their claims reviewed and how improperly collected or retained surveillance data, including any copies thereof, will be expeditiously destroyed once it is identified;
 - (g) What technological system will be used to store the surveillance data, and who will maintain custody and control over the system and its surveillance data; and
 - (h) What unit or individuals will be responsible for ensuring compliance with Section 2(F)(7), and when and how compliance audits will be conducted.
- (8) Public Access: How surveillance data will be accessible to members of the public, how the municipal entity interprets the applicability of, and intends to comply with all local

applicable public records laws with respect to surveillance data, and what steps will be taken to protect individual privacy.

- (9) Target/Defendant Access: How, to what extent, and when surveillance data, in accordance with applicable law, will be accessible to targets of criminal or civil investigations, criminal or civil defendants, and their attorneys.
- (10) Surveillance Data Sharing: If a municipal entity intends to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, it shall detail:
 - (a) How it will require that the collection, retention, and storage of surveillance data be conducted in compliance with the principles set forth in 28 C.F.R. Part 23, including but not limited to 28 C.F.R. Part 23.20(a), which states that a government entity operating a surveillance program “shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.”
 - (b) Which governmental agencies, departments, bureaus, divisions, or units will be approved for (i) surveillance technology sharing, and for (ii) surveillance data sharing;
 - (c) How such sharing is required for the stated purpose and use of the surveillance technology;
 - (d) How it will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable Surveillance Use Policy and does not further disclose the surveillance data to unauthorized persons and entities; and
 - (e) What processes will be used to seek approval of future surveillance technology or surveillance data sharing agreements from the municipal entity and City Council.
- (11) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.
- (12) Training: What training, including training materials, will be required for any individual authorized to use the surveillance technology or to access surveillance data.
- (13) Maintenance: How the security and integrity of the surveillance technology will be maintained and how the municipal entity or lead agent will present any substantive changes in the surveillance technology’s functionality to the City Council for approval.
- (14) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including what internal personnel will be assigned to ensure compliance with the policy, what independent persons or entities will be given

oversight authority, and what legally enforceable sanctions will be put in place for violations of the policy.

- (15) Complaints: What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and what internal personnel will be assigned to receive, register, track, and respond to such communications.
- (16) The Surveillance Use Policy shall include a disclaimer that the Surveillance Use Policy shall be considered a draft proposal until such time as it is approved, with or without modifications, pursuant to a vote of the City Council.

Section 3. No later than one hundred twenty (120) days following the effective date of this Act, any municipal entity seeking to continue the use of any surveillance technology that was in use prior to the effective date of this Act must commence a City Council approval process in accordance with Section 2(A)(3). If the City Council has not approved the continuing use of the surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy re submitted pursuant to Section 2(B), within one hundred eighty (180) days of their submission to the City Council, the municipal entity shall cease its use of the surveillance technology until such time as City Council approval is obtained in accordance with this Act.

Section 4. If more than one municipal entity will have access to the surveillance technology or surveillance data, a lead municipal entity shall be identified. The lead municipal entity shall be responsible for maintaining the surveillance technology and ensuring compliance with all related laws, regulations and protocols. If the lead municipal entity intends to delegate any related responsibilities to other governmental agencies, departments, bureaus, divisions, units, or personnel, these responsibilities and associated entities and/or personnel shall be clearly identified.

Section 5. The City Council shall only approve a request to fund, acquire, or use a surveillance technology if it determines the benefits of the surveillance technology outweigh its costs, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or group. To assist the public in participating in such an analysis, all approved Surveillance Impacts Reports and Surveillance Use Policies shall be made available to the public, at a designated page on the relevant municipal entity's public website, for as long as the related surveillance technology remains in use. An approval for the funding, acquisition and/or use of a surveillance technology by the City Council, where the risk of potential adverse impacts on civil rights or civil liberties has been identified in the Surveillance Impact Report pursuant to Section 2(D)(5)(a), shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impacts exists and must be proactively avoided.

Section 6.

(A) A municipal entity that obtains approval for the use of surveillance technology must submit to the City Council, and make available on its public website, an Annual Surveillance Report for each specific surveillance technology used by the municipal entity within twelve (12) months of City Council approval, and annually thereafter on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

- (1) A summary of how the surveillance technology was used;
- (2) Whether and how often collected surveillance data was shared with any external persons or entities, the name(s) of any recipient person or entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
- (3) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau. For each census tract, the municipal entity shall report how many individual days the surveillance technology was deployed and what percentage of those daily-reported deployments were subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (4) Where applicable, a breakdown of how many times the surveillance technology was used to investigate potential or actual (A) violent crimes, (B) non-violent crimes, (C) felonies, (D) misdemeanors, and (E) other legal or code violations, infractions not classified as felonies or misdemeanors, unlawful activity, activities or patterns considered to be indicators of potential future involvement in criminal activity, or perceived or actual gang or other group affiliations;
- (5) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology was used to monitor Internet activity, including but not limited to social media accounts, the number of people affected, and what percentage of the reported monitoring was subject to (A) a warrant, and (B) a non-warrant form of court authorization;
- (6) Where applicable, a breakdown of what the surveillance technology was installed upon, including but not limited to on what vehicles or structures it was placed;
- (7) Where applicable, a breakdown of what hardware surveillance technology software was installed upon;
- (8) Where applicable, a breakdown of what databases the surveillance technology was applied to, including the frequency thereof;

- (9) A summary of complaints or concerns that were received about the surveillance technology;
- (10) The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
- (11) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendment to the United States Constitution; [A6]
- (12) Statistics and information about public records act requests, including response rates; and
- (13) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

(B) Within thirty (30) days of submitting an Annual Surveillance Report pursuant to Section 6(B), the municipal agency shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the Annual Surveillance Report and the municipal agency's use of surveillance technologies.

(C) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits of the surveillance technology outweigh its costs and whether the public's civil liberties and civil rights have been adequately protected and safeguarded. If the benefits do not outweigh the costs or civil rights and civil liberties have not been adequately protected and safeguarded, the City Council shall direct the use of the surveillance technology cease or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

Section 7. Not later than April 15 of each year, the City Council or its appointed designee shall release a public report, in print and on its public website, containing the following information for the preceding calendar year:

- (A) The number of requests for approval submitted to the City Council under this Act for the funding, acquisition, or new use of surveillance technology;
- (B) The number of times the City Council approved requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;
- (C) The number of times the City Council rejected requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;

- (D) The number of times the City Council requested modifications be made to Surveillance Impact Reports and Surveillance Use Policies before approving the funding, acquisition, or new use of surveillance technology; and
- (E) All Annual Surveillance Reports submitted pursuant to Section 6. Printed copies of the public report may contain pinpoint references to online locations where the Annual Surveillance Reports are located, in lieu of reprinting the full reports.

Section 8.

- (A) Any violation of this Act, including but not limited to funding, acquiring, or utilizing surveillance technology that has not been approved pursuant to this Act or utilizing surveillance technology in a manner or for a purpose that has not been approved pursuant to this Act, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, writ of mandate, or evidence suppression in any court of competent jurisdiction to enforce this Act.
- (B) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought to enforce this Act.
- (C) Municipal employees or agents, except in response to a declared municipal, state, or federal state of emergency, shall not use any surveillance technology except in a manner consistent with policies approved pursuant to the terms of this Act, and may in no circumstances utilize surveillance technology in a manner which is discriminatory, viewpoint-based, or violates the City Charter^[A7], State Constitution, or United States Constitution. Any municipal employee who violates the provisions of this Act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For municipal employees who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.
- (D) Whistleblower protections.
 - (1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:
 - (a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council

Member, based upon a good faith belief that the disclosure evidenced a violation of this Act; or

(b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Act.

(2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Act.

(3) Any employee or applicant who is injured by a violation of Section 8(D)(1) may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

(E) In addition, any person who:

(1) Knowingly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$2,500 per violation, imprisonment of not more than six months, or both.

(2) Recklessly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$1,000 per violation.

Section 9. It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Act, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Act shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Act.

Section 10. It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that facilitates the receipt of surveillance data from, or provision of surveillance data to any non-governmental entity in exchange for any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts. Any contracts or agreements signed prior to the enactment of this Act that violate this section shall be terminated as soon as is legally permissible.

Section 11. The provisions in this Act are severable. If any part of provision of this Act, or the application of this Act to any person or circumstance, is held invalid, the remainder of this Act, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. This Act shall take effect on [DATE].

Ordinance No. 124142

Council Bill No. 117730

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.

Related Legislation File:

Date Introduced and Referred: <u>3-4-13</u>	To: (committee): <u>Public Safety, Civil Rights + Technology</u>
Date Re-referred:	To: (committee):
Date Re-referred:	To: (committee):
Date of Final Action: <u>3/18/13</u>	Date Presented to Mayor: <u>3/20/13</u>
Date Signed by Mayor: <u>3-26-13</u>	Date Returned to City Clerk: <u>3-27-13</u>
Published by Title Only <u>X</u>	Date Vetoed by Mayor:
Published in Full Text	Date Passed Over Veto:
Date Veto Published:	Date Returned Without Signature:

The City of Seattle - Legislative Department

3

Council Bill/Ordinance sponsored by:

[Signature]

Bruce A. Harrell

Committee Action:

Date	Recommendation	Vote
<u>3/6/13</u>	<u>Substitute version 8a for Version 10</u>	<u>BH, NL MO, SC</u>
<u>3/16/13</u>	<u>PASS AS AMENDED</u>	<u>BH, NL MO, SC</u>

This file is complete and ready for presentation to Full Council.

Full Council Action:

Date	Decision	Vote
<u>3/18/13</u>	<u>Passed as Amended</u>	<u>9-0</u>

CITY OF SEATTLE

ORDINANCE 124142

COUNCIL BILL 117730

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.

WHEREAS, recent incidents involving the City's acquisition of drones and the installation of video cameras along Seattle's waterfront and downtown 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 balanced with the need to protect privacy and anonymity, free speech and association, and equal protection; and

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

WHEREAS, all City departments should seek approval from the City Council prior to the acquisition and operation of certain surveillance equipment; and

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

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; NOW, THEREFORE,



1 **BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

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

3 **Chapter 14.18 Acquisition and Use of Surveillance Equipment**

4 **SMC 14.18.10 Definitions**

5 The following definitions apply to this Chapter 14.18

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

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

13 "Surveillance equipment" means equipment capable of capturing or recording data,
14 including images, videos, photographs or audio operated by or at the direction of a City
15 department that may deliberately or inadvertently capture activities of individuals on public or
16 private property, regardless of whether "masking" or other technology might be used to obscure
17 or prevent the equipment from capturing certain views. "Surveillance equipment" includes
18 drones or unmanned aircraft and any attached equipment used to collect data. "Surveillance
19 equipment" does not include a handheld or body-worn device, a camera installed in or on a
20 police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to
21 record traffic patterns and/or traffic violations, a camera intended to record activity inside or at
22 the entrances to City buildings for security purposes, or a camera installed to monitor and protect
23 the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.



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

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

- 11 A. A clear statement describing the purpose and use of the proposed surveillance equipment.
- 12 B. The type of surveillance equipment to be acquired and used.
- 13 C. The intended specific location of such surveillance equipment if affixed to a building or
14 other structure.
- 15 D. How and when a department proposes to use the surveillance equipment, such as whether
16 the equipment will be operated continuously or used only under specific circumstances,
17 and whether the equipment will be installed permanently or temporarily
- 18 E. A description of the privacy and anonymity rights affected and a mitigation plan
19 describing how the department's use of the equipment will be regulated to protect
20 privacy, anonymity, and limit the risk of potential abuse.
- 21 F. A description of how and when data will be collected and retained and who will have
22 access to any data captured by the surveillance equipment.
- 23 G. The extent to which activity will be monitored in real time as data is being captured and
24 the extent to which monitoring of historically recorded information will occur.



1 H. A public outreach plan for each community in which the department intends to use the
2 surveillance equipment that includes opportunity for public meetings, a public comment
3 period, and written agency response to these comments.

4 I. If a department is requesting to acquire or use drones or other unmanned aircraft, it shall
5 propose the specific circumstances under which they may be deployed, along with clearly
6 articulated authorization protocols.

7 J. If more than one department will have access to the surveillance equipment or the data
8 captured by it, a lead department shall be identified that is responsible for maintaining the
9 equipment and ensuring compliance with all related protocols. If the lead department
10 intends to delegate any related responsibilities to other departments and city personnel,
11 these responsibilities and associated departments and personnel shall be clearly
12 identified.

13 K. Whether a department intends to share access to the surveillance equipment or the
14 collected data with any other government entity.

15 L. A description of the training to be provided to operators or users of the surveillance
16 equipment.

17
18 Upon review of the information required under this Section 14.18.20, and any other information
19 deemed relevant by the City Council, the City Council may approve the acquisition and
20 operation of surveillance equipment, approve the acquisition of surveillance equipment and
21 require future Council approval for operations, deny the acquisition or use of surveillance
22 equipment for the purpose proposed, or take other actions.



1 **SMC 14.18.30 Data Management Protocols for Surveillance Equipment**

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

- 7
- 8 A. The time period for which any data collected by surveillance equipment will be retained.
 - 9 B. The methods for storing recorded information, including how the data is to be labeled or
10 indexed. Such methods must allow for the department personnel and the City Auditor's
11 Office to readily search and locate specific data that is collected and determine with
12 certainty that data was properly deleted, consistent with applicable law.
 - 13 C. How the data may be accessed, including who will be responsible for authorizing access,
14 who will be allowed to request access, and acceptable reasons for requesting access.
 - 15 D. A viewer's log or other comparable method to track viewings of any data captured or
16 collected by the surveillance equipment, including the date, time, the individuals
17 involved, and the reason(s) for viewing the records.
 - 18 E. A description of the individuals who have authority to obtain copies of the records and
19 how the existence and location of copies will be tracked.
 - 20 F. A general description of the system that will be used to store the data.
 - 21 G. A description of the unit or individuals responsible for ensuring compliance with Section
22 14.18.30 and when and how compliance audits will be conducted.
- 23

24 **SMC 14.18.40 Acquisition and Use of Surveillance Equipment Related to Law Enforcement**
25 **Investigations**



1 Notwithstanding the provisions of this Chapter, City departments may acquire or use
2 surveillance equipment that is used on a temporary basis for the purpose of a criminal
3 investigation supported by reasonable suspicion, or pursuant to a lawfully issued search warrant,
4 or under exigent circumstances as defined in case law. This exemption from the provisions of
5 this ordinance does not apply to surveillance cameras mounted on drones or other unmanned
6 aircraft.

7 Section 2. Unless Council previously approved operational protocols by ordinance for
8 department surveillance equipment, each City department operating surveillance equipment prior
9 to the effective date of this ordinance shall propose written operational protocols consistent with
10 SMC 14.18.20 no later than thirty days following the effective date of this ordinance for Council
11 review and approval by ordinance.


12 Section 3. Each department operating surveillance equipment prior to the effective date
13 of this ordinance shall adopt written data management protocols consistent with SMC 14.18.30
14 no later than thirty days following the effective date of this ordinance and submit these protocols
15 to the City Council for review and possible approval by ordinance.

16 Section 4. Following one year after the effective date of this ordinance, the City Council
17 will review its implementation as it applies to city department use of surveillance equipment.

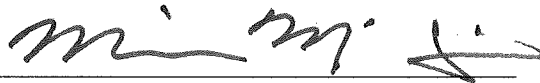
18 This ordinance shall take effect and be in force 30 days after its approval by the Mayor,
19 but if not approved and returned by the Mayor within ten days after presentation, it shall take
20 effect as provided by Seattle Municipal Code Section 1.04.020.




1 Passed by the City Council the 18th day of March, 2013, and
2 signed by me in open session in authentication of its passage this
3 18th day of March, 2013.

4
5 
6 President _____ of the City Council

7
8 Approved by me this 26th day of March, 2013.

9
10 
11 Michael McGinn, Mayor

12
13 Filed by me this 27th day of March, 2013.

14
15 
16 Monica Martinez Simmons, City Clerk

17 (Seal)



FISCAL NOTE FOR NON-CAPITAL PROJECTS

Department:	Contact Person/Phone:	CBO Analyst/Phone:
Legislative	Christa Valles/45336	

Legislation Title:

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.

Summary of the Legislation:

This legislation requires City departments to obtain Council approval before acquiring surveillance equipment. It also requires departments to develop operational and data management protocols.

Background:

This legislation is intended to create a public process and decision-making structure for the City's acquisition and use of surveillance equipment.

X

This legislation does not have any financial implications.

(Please skip to "Other Implications" section at the end of the document and answer questions a-h. Earlier sections that are left blank should be deleted. Please delete the instructions provided in parentheses at the end of each question.)



CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL 117730

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.

WHEREAS, recent incidents involving the City's acquisition of drones and the installation of video cameras along Seattle's waterfront and downtown 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 balanced with the need to protect privacy and anonymity, free speech and association, and equal protection; weighed against the potential downsides, including impacts on privacy; and

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

WHEREAS, all City departments should seek approval from the City Council prior to the acquisition and operation of certain surveillance equipment; and

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

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; NOW, THEREFORE,

THIS VERSION IS NOT ADOPTED



1 **BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:**

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

3 **Chapter 14.18 Acquisition and Use of Surveillance Equipment**

4 **SMC 14.18.10 Definitions**

5 The following definitions apply to this Chapter 14.18

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

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

13 "Surveillance equipment" means equipment capable of capturing or recording data,
14 including images, videos, photographs or audio operated by or at the direction of a City
15 department that may deliberately or inadvertently capture activities of individuals on public or
16 private property, regardless of whether "masking" or other technology might be used to obscure
17 or prevent the equipment from capturing certain views. "Surveillance equipment" includes
18 drones or unmanned aircraft and any attached equipment used to collect data. "Surveillance
19 equipment" does not include a handheld or body-worn device, a camera installed in or on a
20 police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to
21 record traffic patterns and/or traffic violations, a camera intended to record activity inside or at
22 the entrances to City buildings for security purposes, or a camera installed to monitor and protect
23 the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.

THIS VERSION IS NOT ADOPTED



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

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

- 11 A. A clear statement describing the purpose and use of the proposed surveillance equipment.
- 12 B. The type of surveillance equipment to be acquired and used.
- 13 C. The intended specific location of such surveillance equipment if affixed to a building or
14 other structure.
- 15 D. How and when a department proposes to use the surveillance equipment, such as whether
16 the equipment will be operated continuously or used only under specific circumstances,
17 and whether the equipment will be installed permanently or temporarily
- 18 E. A description of the privacy and anonymity rights affected and a mitigation plan
19 describing how the department's use of the equipment will be regulated to protect
20 privacy, anonymity, and limit the risk of potential abuse.
- 21 F. A description of how and when data will be collected and retained and who will have
22 access to any data captured by the surveillance equipment.
- 23 G. The extent to which activity will be monitored in real time as data is being captured and
24 the extent to which monitoring of historically recorded information will occur.

1 H. A public outreach plan for each community in which the department intends to use the
2 surveillance equipment that includes opportunity for public meetings, a public comment
3 period, and written agency response to these comments.

4 I. If a department is requesting to acquire or use drones or other unmanned aircraft, it shall
5 propose the specific circumstances under which they may be deployed, along with clearly
6 articulated authorization protocols.

7 J. If more than one department will have access to the surveillance equipment or the data
8 captured by it, a lead department shall be identified that is responsible for maintaining the
9 equipment and ensuring compliance with all related protocols. If the lead department
10 intends to delegate any related responsibilities to other departments and city personnel,
11 these responsibilities and associated departments and personnel shall be clearly
12 identified.

13 K. Whether a department intends to share access to the surveillance equipment or the
14 collected data with any other government entity.

15 L. A description of the training to be provided to operators or users of the surveillance
16 equipment.

17
18 Upon review of the information required under this Section 14.18.20, and any other information
19 deemed relevant by the City Council, the City Council may approve the acquisition and
20 operation of surveillance equipment, approve the acquisition of surveillance equipment and
21 require future Council approval for operations, deny the acquisition or use of surveillance
22 equipment for the purpose proposed, or take other actions.

THIS VERSION IS NOT ADOPTED



1 **SMC 14.18.30 Data Management Protocols for Surveillance Equipment**

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

- 7
- 8 A. The time period for which any data collected by surveillance equipment will be retained.
 - 9 B. The methods for storing recorded information, including how the data is to be labeled or
10 indexed. Such methods must allow for the department personnel and the City Auditor's
11 Office to readily search and locate specific data that is collected and determine with
12 certainty that data was properly deleted, consistent with applicable law.
 - 13 C. How the data may be accessed, including who will be responsible for authorizing access,
14 who will be allowed to request access, and acceptable reasons for requesting access.
 - 15 D. A viewer's log or other comparable method to track viewings of any data captured or
16 collected by the surveillance equipment, including the date, time, the individuals
17 involved, and the reason(s) for viewing the records.
 - 18 E. A description of the individuals who have authority to obtain copies of the records and
19 how the existence and location of copies will be tracked.
 - 20 F. A general description of the system that will be used to store the data.
 - 21 G. A description of the unit or individuals responsible for ensuring compliance with Section
22 14.18.30 and when and how compliance audits will be conducted.
- 23

24 **SMC 14.18.40 Acquisition and Use of Surveillance Equipment Related to Law Enforcement**

25 **Investigations**

26

27

28

1 Notwithstanding the provisions of this Chapter, City departments may acquire or use
2 surveillance equipment that will be installed or used on a temporary basis for the purpose of a
3 criminal investigation pursuant to a lawfully issued search warrant, or under exigent
4 circumstances as defined in case law. This exemption from the provisions of this ordinance does
5 not apply to surveillance cameras mounted on drones or other unmanned aircraft.

6 Section 2. Unless Council previously approved operational protocols by ordinance for
7 department surveillance equipment, each City department operating surveillance equipment prior
8 to the effective date of this ordinance shall propose written operational protocols consistent with
9 SMC 14.18.20 no later than thirty days following the effective date of this ordinance for Council
10 review and approval by ordinance.

11 Section 3. Each department operating surveillance equipment prior to the effective date
12 of this ordinance shall adopt written data management protocols consistent with SMC 14.18.30
13 no later than thirty days following the effective date of this ordinance and submit these protocols
14 to the City Council for review and possible approval by ordinance.

15 This ordinance shall take effect and be in force 30 days after its approval by the Mayor,
16 but if not approved and returned by the Mayor within ten days after presentation, it shall take
17 effect as provided by Seattle Municipal Code Section 1.04.020.

THIS VERSION IS NOT ADOPTED



1 Passed by the City Council the 18th day of March, 2013, and
2 signed by me in open session in authentication of its passage this
3 18th day of March, 2013.

4 _____
5 _____
6 President _____ of the City Council

7 _____
8 Approved by me this _____ day of _____, 2013.

9 _____
10 _____
11 Michael McGinn, Mayor

12 _____
13 Filed by me this _____ day of _____, 2013.

14 _____
15 _____
16 Monica Martinez Simmons, City Clerk

17 (Seal)
18
19
20
21
22
23
24
25
26
27
28

THIS VERSION IS NOT ADOPTED



CITY OF SEATTLE

ORDINANCE _____

COUNCIL BILL _____

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.

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

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

WHEREAS, all City departments should seek approval from the City Council prior to the acquisition and operation of certain surveillance equipment; and

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

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; NOW, THEREFORE,

BE IT ORDAINED BY THE CITY OF SEATTLE AS FOLLOWS:

DO NOT SIGN HERE
THIS VERSION IS NOT ADOPTED

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

2 **Chapter 14.18 Acquisition and Use of Surveillance Equipment**

3 **SMC 14.18.10 Definitions**

4 The following definitions apply to this Chapter 14.18

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

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

12 "Surveillance equipment" means equipment capable of capturing and recording data,
13 including images, videos, photographs or audio operated by or at the direction of a City
14 department that may deliberately or inadvertently capture activities of individuals on public or
15 private property, regardless of whether "masking" or other technology might be used to obscure
16 or prevent the equipment from capturing certain views. "Surveillance equipment" includes
17 drones or airborne vehicles and any attached equipment used to collect data. "Surveillance
18 equipment" does not include a handheld or body-worn device, a camera installed in or on a
19 police vehicle, a camera installed in or on any vehicle or along a public right-of-way intended to
20 record traffic patterns and/or traffic violations, a camera intended to record activity inside or at
21 the entrances to City buildings for security purposes, or a camera installed to monitor and protect
22 the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.

23
24 **SMC 14.18.20 Council Approval for City Department Acquisition and Operations of**
25 **Surveillance Equipment**

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

- 9 A. A clear statement describing the purpose and use of the proposed surveillance equipment.
- 10 B. The type of surveillance equipment to be acquired and used.
- 11 C. The intended specific location of such surveillance equipment if affixed to a building or
12 other structure.
- 13 D. How and when a department proposes to use the surveillance equipment, such as whether
14 the equipment will be operated continuously or used only under specific circumstances.
- 15 E. How the department's use of the equipment will be regulated to protect privacy and limit
16 the risk of potential abuse.
- 17 F. A description of how and when data will be collected and retained and who will have
18 access to any data captured by the surveillance equipment.
- 19 G. The extent to which activity will be monitored in real time as data is being captured and
20 the extent to which monitoring of historically recorded information will occur.
- 21 H. A description of the nature and extent of public outreach conducted in each community in
22 which the department intends to use the surveillance equipment.
- 23 I. If a department is requesting to acquire or use drones or other unmanned aircraft, it shall
24 propose the specific circumstances under which they may be deployed, along with clearly
25 articulated authorization protocols.

THIS VERSION IS NOT ADOPTED

1 J. If more than one department will have access to the surveillance equipment or the data
2 captured by it, a lead department shall be identified that is responsible for maintaining the
3 equipment and ensuring compliance with all related protocols. If the lead department
4 intends to delegate any related responsibilities to other departments and city personnel,
5 these responsibilities and associated departments and personnel shall be clearly
6 identified.

7
8 Upon review of the information required under this Section 14.18.20, and any other information
9 deemed relevant by the City Council, the City Council may approve the acquisition and
10 operation of surveillance equipment, approve the acquisition of surveillance equipment and
11 require future Council approval for operations, deny the acquisition or use of surveillance
12 equipment for the purpose proposed, or take other actions.

13
14 **SMC 14.18.30 Data Management Protocols for Surveillance Equipment**

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

- 20
21 A. The time period for which any data collected by surveillance equipment will be retained.
22 B. The methods for storing recorded information, including how the data is to be labeled or
23 indexed. Such methods must allow for the department personnel and the City Auditor's
24 Office to readily search and locate specific data that is collected and determine with
25 certainty that data was properly deleted, consistent with applicable law.
26

- 1 C. How the data may be accessed, including who will be responsible for authorizing access,
2 who will be allowed to request access, and acceptable reasons for requesting access.
- 3 D. A viewer's log or other comparable method to track viewings of any data captured or
4 collected by the surveillance equipment, including the date, time, the individuals
5 involved, and the reason(s) for viewing the records.
- 6 E. A description of the individuals who have authority to obtain copies of the records and
7 how the existence and location of copies will be tracked.
- 8 F. A general description of the system that will be used to store the data.
- 9 G. A description of the unit or individuals responsible for ensuring compliance with Section
10 14.18.30 and when and how compliance audits will be conducted.

11 Section 2. Unless Council previously approved operational protocols by ordinance for
12 department surveillance equipment, each City department operating surveillance equipment prior
13 to the effective date of this ordinance shall propose written operational protocols consistent with
14 SMC 14.18.20 no later than thirty days following the effective date of this ordinance for Council
15 review and approval by ordinance.

16 Section 3. Each department operating surveillance equipment prior to the effective date
17 of this ordinance shall adopt written data management protocols consistent with SMC 14.18.30
18 no later than thirty days following the effective date of this ordinance and submit these protocols
19 to the City Council for review and possible approval by ordinance.

20 This ordinance shall take effect and be in force 30 days after its approval by the Mayor,
21 but if not approved and returned by the Mayor within ten days after presentation, it shall take
22 effect as provided by Seattle Municipal Code Section 1.04.020.

1 Passed by the City Council the ____ day of _____, 2013, and
2 signed by me in open session in authentication of its passage this
3 ____ day of _____, 2013.

4 _____
5 _____
6 President _____ of the City Council

7
8 Approved by me this ____ day of _____, 2013.

9 _____
10 _____
11 Michael McGinn, Mayor

12
13 Filed by me this ____ day of _____, 2013.

14 _____
15 _____
16 Monica Martinez Simmons, City Clerk

17 (Seal)

18
19
20
21
22
23
24
25
26
27
28

THIS VERSION IS NOT ADOPTED

STATE OF WASHINGTON -- KING COUNTY

--ss.

296304
CITY OF SEATTLE, CLERKS OFFICE

No. 124140,141,142,143,144

Affidavit of Publication

The undersigned, on oath states that he is an authorized representative of The Daily Journal of Commerce, a daily newspaper, which newspaper is a legal newspaper of general circulation and it is now and has been for more than six months prior to the date of publication hereinafter referred to, published in the English language continuously as a daily newspaper in Seattle, King County, Washington, and it is now and during all of said time was printed in an office maintained at the aforesaid place of publication of this newspaper. The Daily Journal of Commerce was on the 12th day of June, 1941, approved as a legal newspaper by the Superior Court of King County.

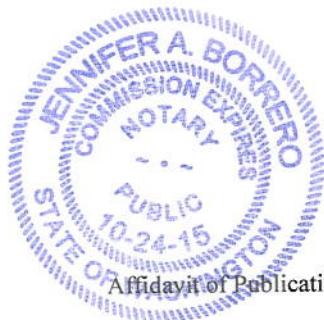
The notice in the exact form annexed, was published in regular issues of The Daily Journal of Commerce, which was regularly distributed to its subscribers during the below stated period. The annexed notice, a

CT; TITLE ONLY ORDINANCE

was published on

04/11/13

The amount of the fee charged for the foregoing publication is the sum of \$156.75 which amount has been paid in full.



Paul C. Osby

Subscribed and sworn to before me on

04/11/2013

Jennifer Borrero

Notary public for the State of Washington,
residing in Seattle

Affidavit of Publication

State of Washington, King County

City of Seattle

Title Only Ordinances

The full text of the following legislation, passed by the City Council on March 18, 2013, and published below by title only, will be mailed upon request, or can be accessed at <http://clerk.seattle.gov>. For information on upcoming meetings of the Seattle City

Council, please visit <http://www.seattle.gov/council/calendar>.

Contact: Office of the City Clerk at (206) 684-8344.

ORDINANCE NO. 124140

AN ORDINANCE relating to the City Light Department ("City Light"), declaring certain real property rights surplus and no longer required for providing public utility service or other municipal purpose; authorizing the Superintendent of City Light to execute a Real Property Exchange Agreement between the City of Seattle and Sierra Pacific Industries, Inc. (SPI) for the conveyance of said surplus property and a cash equalization payment of \$208,000 in exchange for the conveyance of SPI-owned land to the City in the South Fork of the Nooksack River watershed, Skagit County, Washington for wildlife habitat purposes; authorizing the Superintendent of City Light or his designee to execute Bargain and Sale Deeds for the properties conveyed by the City and accept a Bargain Sale Deed for the lands conveyed to the City; and placing said lands under the jurisdiction of City Light.

ORDINANCE NO. 124141

AN ORDINANCE accepting deeds for street or alley purposes; laying off, opening, widening, extending, and establishing portions of the following rights-of-way: the alley in Block 72, Gilman Park; the alley in Block 26, Woodlawn Addition to Green Lake; the alley in Block 11, D. T. Denny's Water Front Addition to the City of Seattle; the alley in Block 4, University Heights; the alley in Block 17, Heirs of Sara A. Bell's 2nd Addition to the City of Seattle; the alley in Block 18, Hill Tract Addition to the City of Seattle; the alley in Block 6, Plat of Replat of North Trunk Road Addition to the City of Seattle; the alley in Block 33, D.T. Denny's Home Addition to the City of Seattle; the alley in Block 55, Terry's First Addition to the Town of Seattle; the alley in Block 22, Hill Tract Addition to the City of Seattle; the alley in Block 4, Eastern Addition to the Town of Seattle; West Barrett Street abutting Block 20, Gilman's Addition to the City of Seattle; the alley in Block 20, Gilman's Addition to the City of Seattle; the alley in Block 11, Fairview Homestead Association for the Benefit of Mechanics and Laborers; Southwest Snoqualmie Street abutting Block 63, The Boston Co's Plat of West Seattle; the alley in Block 63, The Boston Co's Plat of West Seattle; the alley in Block 11, Bell & Denny's Addition to the City of Seattle; the alley in Block 56, Gilman Park; the alley in Block 3, Elbert Place Addition to the City of Seattle; placing the real property conveyed by said deeds under the jurisdiction of the Seattle Department of Transportation; and ratifying and confirming certain prior acts.

ORDINANCE NO. 124142

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.

ORDINANCE NO. 124143

AN ORDINANCE relating to the Traffic Code; amending section 11.23.160 of the Seattle Municipal Code to increase the number of free-floating car share permits authorized annually and ratifying and confirming certain prior acts.

ORDINANCE NO. 124144

AN ORDINANCE appropriating money to pay certain audited claims and ordering the payment thereof.

Date of publication in the Seattle Daily Journal of Commerce, April 11, 2013.

4/11(296304)