STAFF REPORT

DATE: March 20, 2018

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology Ordinance

Recommendation
Provide staff feedback and/or direction on Surveillance Technology Ordinance.

Fiscal Impact
There is no fiscal impact to this report. If Council provides direction, future actions could have fiscal impacts.

Council Goal(s)
Goal 7 - Ensure a Safe and Health Community. This item is not called out as a specific task.

Background and Analysis
Last April (2017), after listening to a presentation by the ACLU, the Human Relations Commission (HRC) passed a motion that Council consider adopting a local ordinance governing the acquisition and use of surveillance technology. Following additional suggestions made during the public comments portion of a regular City Council meeting, Council asked staff to come back with recommendations for a surveillance policy or ordinance.

In September (2017), staff provided the City Council with various options regarding how surveillance technology can be regulated, either by policy or ordinance. Following presentation and discussion, there was general council consensus that staff should: return with draft options for an actual ordinance; the ACLU model could be used as a basis for the ordinance, but other options could be presented based on what other entities are doing; and that the ordinance should be written so that the City Council would directly approve the use of any surveillance technology rather than a city commission.

In January, staff met with a few community members and representatives from the ACLU regarding an ordinance. Following that meeting, Brian Hofer, a member of Oakland Privacy and the Chair of the City of Oakland Privacy Advisory Commission, provided staff with and updated version for a surveillance technology ordinance. There was also general consensus from the community members that the purpose of any surveillance ordinance is really about how government uses technology in an outward looking fashion, rather than how technology is used to accomplish the day-to-day internal work of the City.

As requested, staff is returning with a draft ordinance that contains proposed language (Attachment 1). For ease in explanation, the following steps would be required for a City department that wants to use, acquire or share data involving a surveillance technology;

1. The City department would have to draft a **Surveillance Use Policy**, as defined in the ordinance, and a **Surveillance Impact Report**, as defined in the ordinance.

2. The City department would submit the two documents, along with a brief staff report, to the City Council as a consent item at a regular city council meeting. This allows the Council and the public to see the documents at least 30-days prior to Council holding a public hearing that would allow a City department to use the surveillance technology. The documents would also be viewable on the City website.

3. Following the 30-day notice period, the City Council would hold a public hearing at a regular city council meeting to determine whether the City department can acquire, use or share data from the surveillance technology item. In making a decision, the City Council would balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City before approving any use.

4. Thereafter, the City department would have to submit an **Annual Surveillance Report**, as defined in the ordinance, to the City Council and seek continuing permission to use the surveillance technology item using the same balancing test.

The following are a few highlights of the draft language:

- The City Council finds that any decision to use surveillance technology must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.

- The City Council finds that proper transparency, oversight and accountability for the acquisition and use of surveillance technology is fundamental to protecting the rights and civil liberties, including privacy and free expression, of all people.

- "Surveillance Technology" means any software, 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 or similar information specifically associated with, or capable of being associated with, any individual or group by a City department. Examples of surveillance technology includes but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality and biometric identification hardware or software.

"Surveillance technology" does not include the following devices, hardware or software:

- Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are in widespread use by City departments and used for routine City business and transactions;
- City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resource, permit, license and business records;
- City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including, payroll, accounting, or other fiscal databases;
- Information technology security systems, including firewalls and other cybersecurity systems;
- Physical access control systems, employee identification management systems, and other physical control systems;
- Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;
- Manually-operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices and email systems;
- Manually-operated, non-wearable, handheld 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;
- Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;
- Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
- Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the ordinary course of providing City services;
- Parking Ticket Devices;
- Police department interview room, holding cell and police department internal security audio/video recording systems;
- Police department computer aided dispatch (CAD), records/case management, Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems;
- Police department early warning systems.

- A City department shall obtain City Council approval following a public hearing conducted at a regular City Council meeting prior to any of the following:

- Seeking funds for 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 for the purpose of acquiring surveillance technology;
- Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
- 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
- Entering into a formal written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

- A City department may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this Article before that acquisition or use. If the City department acquires or uses a surveillance technology pursuant to this Section, the City department shall:

  - Use the surveillance technology to solely respond to the exigent circumstances;
  - Cease using the surveillance technology when the exigent circumstances ends;
  - Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation;
  - Following the end of the exigent circumstances report the acquisition or use to the City Council at a regular City Council meeting for discussion and/or possible recommendation for approval to acquire or use the surveillance technology; and
  - Any technology temporarily acquired in exigent circumstances shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 26.07.030 and is approved.

- A City department or departments possessing or using surveillance technology prior to the effective date of this Article shall submit or jointly submit a proposed Surveillance Use Policy no later than one-hundred twenty (120) days following the effective date of this Article for review and approval by the City Council pursuant to Section 26.07.030. If such review and approval has not occurred within four regular meetings from when the item was initially scheduled for City Council consideration, the City department shall cease its use of the surveillance technology until such review and approval occurs.

Attachments

1. Ordinance

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF DAVIS ADDING ARTICLE 26.07 OF THE DAVIS MUNICIPAL CODE REGARDING CITY USE OF SURVEILLANCE TECHNOLOGY AND ESTABLISHING THE PENALTY FOR A VIOLATION THEREOF

WHEREAS, the City Council finds that any decision to use surveillance technology must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.

WHEREAS, the City Council finds that proper transparency, oversight and accountability for the acquisition and use of surveillance technology is fundamental to protecting the rights and civil liberties, including privacy and free expression, of all people.

WHEREAS, the City Council finds it essential to have an informed public debate as early as possible about whether to acquire and use surveillance technology.

WHEREAS, the City Council finds it necessary that safeguards be in place to protect civil liberties and civil rights before any surveillance technology is deployed.

WHEREAS, the City Council finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF DAVIS DOES HEREBY ORDAIN AS FOLLOWS:

SECTION 1. Article 26.07 is hereby added to Chapter 26 of the City of Davis Municipal Code to read as follows:

26.07.010 Purpose and Findings.

This Article shall be known as the Surveillance Technology Ordinance.

The purpose and intent of this Article is to impose safeguards to protect civil liberties and civil rights before any surveillance technology is deployed.

The City Council finds that any decision to use surveillance technology must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.

The City Council finds that proper transparency, oversight and accountability for the acquisition and use of surveillance technology is fundamental to protecting the rights and civil liberties, including privacy and free expression, of all people.

The City Council finds it essential to have an informed public debate as early as possible about whether to acquire and use surveillance technology.

The City Council finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs.

26.07.020 Definitions.

For purposes of this Article, the following words, terms and phrases shall have these definitions:

"Annual Surveillance Report" means an annual written report concerning a specific surveillance technology.

(a) The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;

(2) A general description of whether and how often data acquired through the use of the surveillance technology item 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);

(3) A summary of community complaints or concerns about the surveillance technology item;

(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

(6) Statistics and information about any related 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;

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

(b) The Annual Surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes and/or information protected, restricted and/or sealed pursuant to State and/or federal laws, including information not required to be released by the Public Records Act.

"City Department" means any City department and its officers and employees.

"Exigent Circumstances" A City department's good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires the use of the surveillance technology or the information it provides.

"Personal Communication Device" means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

"Surveillance Impact Report" means a written report including at a minimum the following:

(a) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

(b) Information on the proposed purpose(s) for the surveillance technology;

(c) If applicable, the location(s) it may be deployed and crime statistics for any location(s);

(d) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;

(e) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

(f) 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; and

(g) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.

"Surveillance Technology" means any software, 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 or similar information specifically associated with, or capable of being associated with, any individual or group by a City department. Examples of surveillance technology includes but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed. It also includes software designed to

monitor social media services or forecast criminal activity or criminality and biometric identification hardware or software.

(a) "Surveillance technology" does not include the following devices, hardware or software:

(1) Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are in widespread use by City departments and used for routine City business and transactions;

(2) City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resource, permit, license and business records;

(3) City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including, payroll, accounting, or other fiscal databases;

(4) Information technology security systems, including firewalls and other cybersecurity systems;

(5) Physical access control systems, employee identification management systems, and other physical control systems;

(6) Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

(7) Manually-operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices and email systems;

(8) Manually-operated, non-wearable, handheld 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;

(9) Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

(10) Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;

(11) Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the ordinary course of providing City services;

(12) Parking Ticket Devices;

(13) Police department interview room, holding cell and police department internal security audio/video recording systems;

(14) Police department computer aided dispatch (CAD), records/case management, Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems;

(15) Police department early warning systems.

"Surveillance Use Policy" means a policy adopted by the City Council at a regularly scheduled City Council meeting for use of the surveillance technology that at a minimum specifies the following:

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.

(b) Authorized Use: The 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, including "open source" data.

(d) Data Access: The category of individual 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 general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

(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.

(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 record keeping 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.

26.07.030 City Council Approval

(a) A City department shall obtain City Council approval following a public hearing conducted at a regular City Council meeting prior to any of the following:

(1) Seeking funds for 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 for the purpose of acquiring surveillance technology;

(2) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;

(3) 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

(4) Entering into a formal written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

(b) A City department shall obtain City Council approval following a public hearing conducted at a regular City Council meeting of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (a)(2)-(4).

(c) The City department seeking approval under subsection (a) shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular City Council meeting consent calendar at least thirty (30) days prior to the public hearing required under subsection (a). The informational staff report shall be posted on the City website with the City Council agenda.

(d) The City Council may approve any action described in subsection (a) or described in Section 26.07.040 after making a determination that any decision to use a surveillance technology item has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.

(e) Notwithstanding any other provision in this Article, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation.

26.07.040 Compliance for Existing Surveillance Technology

A City department or departments possessing or using surveillance technology prior to the effective date of this Article shall submit or jointly submit a proposed Surveillance Use Policy no later than one-hundred twenty (120) days following the effective date of this Article for review and approval by the City Council pursuant to Section 26.07.030. If such review and approval has not occurred within four regular meetings from when the item was initially scheduled for City Council consideration, the City department shall cease its use of the surveillance technology until such review and approval occurs.

26.07.050 Use of Unapproved Technology during Exigent Circumstances

A City department may temporarily acquire or temporarily use surveillance technology in exigent circumstances without following the provisions of this Article before that acquisition or use. If the City department acquires or uses a surveillance technology pursuant to this Section, the City department shall:

(a) Use the surveillance technology to solely respond to the exigent circumstances;

(b) Cease using the surveillance technology when the exigent circumstances ends;

(c) Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation;

(d) Following the end of the exigent circumstances report the acquisition or use to the City Council at a regular City Council meeting for discussion and/or possible recommendation for approval to acquire or use the surveillance technology; and

(e) Any technology temporarily acquired in exigent circumstances shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 26.07.030 and is approved.

26.07.060 Oversight Following Council Approval

(a) By the end of each fiscal year, a City department that uses surveillance technology must present a written Annual Surveillance Report at a regular City Council meeting for City Council review for each approved surveillance technology item. If the City department is unable to meet the deadline, the department head shall notify the City Council in writing of staff's request to extend this period, and the reasons for that request. The City Council may grant reasonable extensions to comply with this Section.

(b) Based upon information in the Annual Surveillance Report, the City Council will, at a regular City Council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

26.07.070 Enforcement

(a) Any violation of this Article 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 Article. An action instituted under this paragraph shall be brought against the City of Davis, and if necessary to effectuate compliance with this Article or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third party, except a city employee, with possession, custody, or control of data subject to this Article.

(1) Prior to the initiation of any legal proceeding under subsection (a), the City of Davis shall be given written notice of the violation(s) and an opportunity to correct such alleged violation(s) within 30 days of receipt of the notice.

(2) If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous space on the on the city's website that generally describes the corrective measure(s) taken to address the violation(s).

(b) A court shall award costs to the prevailing party in any action brought to enforce this Article and any reasonable attorney's fees as may be awarded pursuant to State law.

(c) It shall be unlawful and a misdemeanor punishable in the manner set forth in the City Municipal Code and State law, for any person to willfully and maliciously violate any provision of this Article.

(d) Nothing in this Article is intended to, or shall be interpreted to, conflict with the Constitution of the United States, the Constitution of the State of California or with any State or federal law.

26.06.080 Severability.

The provisions of this Article are declared to be separate and severable. The invalidity of any clause, phrase, sentence, paragraph, subdivision, section or portion of this Article, or the invalidity of the application thereof to any person or circumstance shall not affect the validity of the remainder of this Article, or the validity of its application to other persons or circumstances.

SECTION 2. The City Clerk shall certify to the adoption of this Ordinance and shall cause the same or a summary thereof to be published as required by law.

SECTION 3. This Ordinance shall take effect and be in full force and effect thirty (30) days from and after the date of its final passage and adoption.

INTRODUCED on the ___ day of _____, 2018, and PASSED AND ADOPTED by the City Council of the City of Davis on this _____ day of _____, 2018, by the following vote:

AYES:

NOES:

ABSTAIN:

ABSENT:

_____
Robb Davis, Mayor of the City of Davis

ATTEST:

_____
Zoe S. Mirabile, CMC,
City Clerk of the City of Davis