STAFF REPORT

DATE: July 10, 2018

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – Trail Cameras

Recommendation

Informational. The Police Department is submitting this informational staff report on consent calendar at least 30 days prior to asking the City Council to hold a public hearing to continue using trail cameras. This informational staff report has been posted on the City website with the City Council agenda (26.07.030 (c) Davis Municipal Code (DMC)).

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

A City department seeking approval to acquire/use surveillance technology as defined by 26.07.020 DMC 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 26.07.030 (a). The informational staff report shall be posted on the City website with the City Council agenda. This staff report is being is submitted to fulfill the notice requirements.

Surveillance Impact Report

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

Trail Cameras – Trail Cameras are covert, battery operated and primarily set at fixed location such as trees, buildings or other objects. Trail cameras can be set to take pictures or short videos of a pre-determined area by using a motion sensor trigger, or a time lapse mode. Trail Cameras also have an infrared (IR) mode. Cameras store data on a removable SD card. Trail cameras are commonly used by nature enthusiasts to capture pictures of wildlife, especially during nighttime hours using the IR mode.

(a) Information on the proposed purpose(s) for the surveillance technology:
Trail Cameras would be located temporarily in areas where criminal activity is suspected in order to capture images of potential suspects. Video surveillance in public areas will be conducted in a legal and ethical manner while recognizing and protecting constitutional standards of privacy.

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
Examples of situations in which Trail Cameras may be deployed are: Monitoring areas on greenbelts and city parks for hate/racist graffiti when a pattern is noticed, with consent - setting up trail cameras on property of victims of stalking and potential domestic violence in order to confirm the presence of a suspect, and assisting business owners gather images of serial shoplifters. Also used in parking lots and equipment yards to monitor against ongoing theft.

(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public
Trail Cameras are used only in areas where reasonable suspicion exists that criminal activity is occurring or may occur. Trail cameras do not surreptitiously capture or monitor conversations, and only capture images when activated by motion sensor trigger.

Trail Cameras will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Trail Cameras shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Trail Cameras shall not be used to harass, intimidate or discriminate against any individual or group.

(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
Initial Purchase Cost
$93.00 each

Personnel Costs
Nominal. These devices save considerable staff costs because human surveillance is not needed.

Ongoing Costs
Nominal. Additional SD cards and batteries are needed when used.

Potential Sources of Funding
Regular police department operational budget

(e) 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;
There is no third party data storage for images gathered by the Trail Camera. Any images not useful in a criminal investigation are deleted.

(f) **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.**
Although there are limitations, Trail Cameras can be a useful tool in monitoring locations that may be targets of ongoing criminal activity. They are temporary and provide images that can allow law enforcement to identify a suspect.

Surveillance Use Policy
Council must adopt a policy 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.
To identify suspects and/or methods of criminal activity in a specific area.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
Trail Cameras will be used at fixed location to monitor locations that may be experiencing criminal activity such as graffiti, theft or other crimes. The cameras will be used by sworn police officers and authorized for use by a supervisor.

Trail Cameras are used only in areas where reasonable suspicion exists that criminal activity is occurring or may occur. Trail cameras do not surreptitiously capture or monitor conversations, and capture images when activated by motion sensor trigger.

Trail Cameras will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Trail Cameras shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Trail Cameras shall not be used to harass, intimidate or discriminate against any individual or group.

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.
Trail Cameras are located temporarily in areas where criminal activity is suspected in order to capture images of potential suspects. The cameras capture still images, or very short video

when the camera is triggered. The cameras are generally left in an area and the camera is triggered by movement. The images or video is not 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.

The information will be accessed by law enforcement officers during an investigation and court process. If the information is included as evidence in a criminal case, the information will be accessed by the prosecuting attorney and the defense attorney through the discovery process.

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

Any recordings needed as evidence in a criminal or civil proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

(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.

Although the Trail Cameras are not password protected, if information gathered is retained for a criminal investigation, the SD cards containing the images or video are stored as evidence.

(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.

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule and for a minimum of one year. If recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is resolved.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

All recorded video images gathered by the cameras are for the official use of the Davis Police Department.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records.

Requests for recorded images from other law enforcement agencies shall be referred to the Police Chief for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

(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.

Data may be shared with other law enforcement agencies who may be involved in a joint investigation, or who are conducting their own investigations. If images gathered by a trail camera become evidence in a criminal case, they may also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney. The information may also be shared with defense attorneys through the discovery process.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

All department members authorized to operate or access public video surveillance systems shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training should also address state and federal law related to the use of video surveillance equipment and privacy.

(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.

Use of Trail Cameras can be authorized by a police sergeant, Lieutenant or other sworn administrator. They are stored at the police department or other law enforcement facility while not in use. Supervisors will monitor video surveillance access and usage to ensure members are within department policy and applicable laws. Supervisors will ensure such use and access is appropriately documented. Members are subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the use of the cameras. The review should include an analysis of the cost, benefit and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee. Any recommendations for training or policy should be promptly addressed.