STAFF REPORT

DATE: July 10, 2018

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – GPS Tracking Device

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 GPS tracking devices in criminal investigations. 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;

(a) **Information on the proposed purpose(s) for the surveillance technology**: GPS Tracking device – A GPS Tracking device uses Global Positioning System (GPS) technology to track the devices movements. The GPS Device is placed on a vehicle, bicycle or other object in order to track that objects location by monitoring the GPS information. The GPS information can be stored within the device, or obtained remotely using a laptop computer or smartphone.

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
Locations GPS Tracking Devices are deployed include items which are at high risk for theft that may be used in "bait" type operations. These items include locked bicycles, laptop computers and delivered parcels/packages to name a few. Other location GPS Tracking Devices may be used are then they are placed on vehicles or vessels.

(c) **An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;**
GPS Tracking Devices placed in items involved in "bait" type operations are not intrusive, and are only tracked if the item is stolen and the GPS information gathered from the device is utilized to recover the property and identify the suspect. Information gathered during these operations is only retained if an arrest is made and the information is needed for a criminal prosecution.

GPS Tracking Devices may also be placed on vessels or vehicles when probable cause exists to believe that the owner or operator is involved in criminal activity. In these instances a search warrant must be obtained and signed by a judge authorizing its use or there must be a 4th amendment waiver (the person is on probation or parole).

(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
GPS Tracking device - $450.00 (already purchased)

Personnel Costs
Nominal. GPS Tracking devices save considerable personnel expenses because they can be used instead of human surveillance.

Ongoing Costs
Yearly service plan - $600.00

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;
Data gathered by the GPS Devices is stored on the vendor's secured servers. Users can access their accounts through password and generate reports, which can be printed or saved.

(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.**
Devices using GPS Tracking technology are very common. They can be found in cell phone mapping programs, automobiles and fleet management systems, court ordered ankle and DUI monitoring devices, and numerous other standalone devices available to civilians. They are

commonly used by law enforcement to surveille individuals suspected of criminal activity and for gathering evidence during "bait" type operations. The devices are used for criminal investigations, which are documented in a police report, a search warrant affidavit, and must be authorized by a search warrant signed by a judge or a 4th amendment waiver.

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.

Improve public safety by providing an effective method of investigating criminal activity.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.

GPS Tracking Devices being used during criminal investigation and 'bait" type operations. GPS Tracking Devices will be used by sworn peace officers. Use of the devices must be authorized by a supervisor or manager and warrant or waiver is required for non-bait surveillance operations.

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.

GPS Devices use Global Positioning System (GPS) technology to track the location of the device by longitude and latitude. The information gathered by the device includes geographic location (Latitude/Longitude), time, speed and direction. The information is not open source and is only accessible by the account holder and vendor.

(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.

(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.

GPS Tracking Device accounts require an account administrator be assigned by the agency using their product. The administrator assigned at the Davis PD for administrating GPS Tracking Device accounts is the Investigations Division Sergeant. The account administrator has the ability to assign "users" who have the ability to change certain setting on the device and make reports, or assign individuals the ability to "view only", which limits access to only

logging in and viewing real time data. The account administrator can also assign passwords and change passwords.

(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.**
Data gathered by GPS Tracking Devices being used for criminal investigations would be retained as evidence. The time period would then be dictated by the court process. Data saved on third party servers can be deleted at the request of the account holder.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.
Members of the public do not have access to this information when it is gathered as part of a criminal investigation.

(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. GPS Device data may also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney. Data 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.
GPS Device users are trained by other officers on how to use the device and obtain the data.

(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 GPS Devices is authorized by a police sergeant, Lieutenant or other sworn administrator. Use of these devices for criminal investigations is documented in police report, a search warrant affidavit, and must be authorized by a search warrant signed by a judge or a 4th amendment waiver. Devices are password secured to ensure that only authorized personnel have access to the data and are stored at the police department or other law enforcement facility while not in use. A member is subject to discipline for unauthorized use or misuse.